Special Committee to Review the Personal Information Protection Act (British Columbia)

Comments of

Canadian Wireless Telecommunications Association

July 30, 2021

Introduction

The Canadian Wireless Telecommunications Association (CWTA) appreciates the opportunity to provide its feedback to the Special Committee regarding its review of the Personal Information Protection Act (PIPA).

CWTA is the authority on wireless issues, developments and trends in Canada. Its membership is comprised of companies that provide services and products across the wireless industry, including wireless carriers and manufacturers of wireless equipment. The protection of personal information (PI) is a key element of our members' business practices and corporate ethos. For that reason, our members invest significant effort and resources to protect the right to privacy of customers and the security of their PI.

In keeping with the Special Committee's request for this consultation, this submission focuses on recommendations made by the Office of the Information and Privacy Commissioner for British Columbia (OIPC) in its initial[1] and supplemental[2] submissions to the Special Committee, including how they relate to provisions in the federal governments Bill C-11[3] (including the proposed *Consumer Privacy Protection Act* (CPPA)) and the European Union's *General Data Protection Regulation* (GDPR).

It is an important time for privacy legislation in Canada as the federal government and multiple provinces, including British Columbia, are considering privacy regulation reform. As pointed out in the OIPC Initial Submission, "[o]f critical importance to the Special Committee's deliberations…is that harmonization among federal and provincial laws benefits both businesses and individuals."[4]

Harmonization does not mean that PIPA must be identical to privacy regulations across Canada or internationally, but any reforms should avoid introducing measures that create significant inconsistencies and unnecessary barriers to the conduct of business across borders, and that harm the competitiveness of businesses operating in British Columbia. This includes preserving exceptions to the application of PIPA for organizations, such as telecommunication service providers, whose collection, use and disclosure of PI is already regulated by federal privacy legislation.

Any new obligations must be clearly articulated and practical, grounded in operational reality, and provide flexibility to address privacy risks as they evolve through technological

[1] https://www.oipc.bc.ca/special-reports/3465 (OIPC Initial Submission)

[2] https://www.oipc.bc.ca/special-reports/3513 (OIPC Supplemental Submission)

[3] An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts - https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

[4] OIPC Initial Submission, p2.

developments and new business models. Finally, PIPA must maintain a balance between protecting privacy and facilitating the use of data and digital technologies.

As referenced in our first recommendation below, CWTA is of the view that PIPA should not apply to organizations governed by the federal privacy legislation. Nevertheless, we have included comments to some of the other recommendations made by OIPC. We trust these recommendations will help the Special Committee in its consideration of PIPA and the goals of harmonization, flexibility, and balance referenced above.

To the extent that there is any inconsistency between CWTA's submission and that of a CWTA member in this proceeding, in regards to the position of such CWTA member, the member's submission shall prevail.

Recommendations:

1. **Section 3(2)(c) of the PIPA must be preserved**

   CWTA opposes the OIPC's recommendation that section 3(2)(c) of PIPA be repealed. Section 3(2)(c) provides that PIPA does not apply to "the collection, use or disclosure of personal information, if the federal Act applies to the collection, use or disclosure of the personal information." Repealing this section would create overlapping privacy regulations for organizations, such as telecommunication service providers (TSPs), already governed by federal privacy laws. This overlap would not only increase the cost and burden of compliance, it would introduce confusion for British Columbians regarding their rights and where to go for resolution of a privacy matter.

   British Columbians' PI is already well-protected in the context of the telecommunications services pursuant to multiple federal laws and regulations applicable to federally regulated undertakings generally and to TSPs specifically.

   Canada is known for taking a leadership role in the protection of PI. The collection, use, and disclosure of PI by TSPs is currently governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA has long been recognized as a leading piece of privacy regulation globally. With advances in technology and new ways of using PI, the federal government has proposed new legislation, Bill C-11, which will preserve the balanced, principles-based approach of PIPEDA, while creating important new individual rights and protections of PI.

   Federal privacy regulations are also subject to the oversight of the Office of the Privacy Commissioner of Canada (OPC). In addition to investigating privacy complaints and ensuring compliance with the mandatory reporting of security incidents, the OPC also develops general guidance related to the application of PIPEDA to specific issues. These

include issues arising from new business models and technical innovations, such as outsourcing, cloud computing, and obtaining meaningful consent.

TSPs are also subject to the federal *Telecommunications Act* and the oversight of the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC's responsibility for privacy in telecommunications is explicitly set out in objective 7(i) of the *Telecommunications Act* (i.e. "to contribute to the protection of the privacy of persons"). While the investigation of complaints under PIPEDA is within the jurisdiction of the OPC, the CRTC has the power to create regulations concerning privacy with respect to telecommunications services. This power includes the ability to impose privacy standards that go beyond those found in PIPEDA and that are specific to industry use cases.

Under the powers granted in the *Telecommunications Act*, the CRTC has imposed regulatory measures and other actions to protect confidential customer information and safeguard consumer privacy. These measures include:

a. Prohibiting TSPs from disclosing confidential customer information other than the customer's name, address, and listed telephone number, without express consent of the customer, except in certain specified circumstances;
b. Prohibiting TSPs from using PI collected for the purpose of traffic management practices for other purposes or disclosing such information;
c. As part of the Wireless Code and the Internet Code, contracts and related documents, including privacy policies, "must be written and communicated in a way that is clear and easy for customer to read and understand." Permanent copies of these documents must be provided to customers after they agree to a contract and TSPs must notify customers of amendments to their privacy policies at least 30 days before the amendments take effect, also in language in that is plain, clear and easy to understand;
d. Issuance of an expectation that any TSP that charges for services will obtain express, opt-in consent before using a customer's data for the purposes of targeted advertising. The requests for consent must include a detailed explanation of the actual information that a company might use to target them for advertising purposes; and
e. Requiring TSPs to offer services that protect consumer privacy, such as unlisted number service, call display, call display blocking, prohibiting call return to a blocked number and call trace. The CRTC also established the National Do Not Call List and the Unsolicited Telecommunication Rules framework.

In addition to the above measures, the CRTC engages in ongoing research that contributes to its understanding of current and emerging privacy issues in the wireless

market. For example, in 2017, the CRTC published its *Report on the Collection and Use of Canadians' Personal Information by Wireless Service Providers and Third Party Entities.*[5]

TSPs are also subject to Canada's anti-spam legislation, commonly referred to as CASL, which has as one of its purposes, the regulation of "commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct compromises privacy and the security of confidential information." CASL – enforced by the CRTC, OPC, and Competition Bureau, establishes rules (including consent rules) pertaining to the sending of commercial electronic messages, the alteration of transmission data in electronic messages, and the installation of computer programs on another person's computer system, in the course of commercial activity. The detailed rules set out in CASL, coupled with the onerous penalty provisions under the Act, have ensured that TSPs have developed rigorous compliance programs in connection with the legislation's requirements.

As the above examples illustrate, the CRTC and the OPC have complementary roles in protecting the privacy of TSP customers across Canada, including British Columbia. Given the federal government's plan to replace PIPEDA with new legislation that addresses new ways in which PI is collected and processed, while also ensuring Canadian businesses can remain competitive and innovative in the global digital economy, there is nothing to suggest that this privacy framework is insufficient to protect the privacy of British Columbians who use federally-regulated telecommunications services.

Finally, the Government of British Columbia has previously recognized that having overlapping provincial and federal regulations regarding the provision of telecommunication services is unnecessary to protect the interests of British Columbians. During the consultations that led to the creation of the Wireless Code, Consumer Protection BC (CPBC) indicated its support for a single set of national wireless service agreement standards. CPBC suggested that a single set of standards "provides for greater consistency, more clear explanation, and lower cost," and noted that "elsewhere it is certainly the norm to have harmonized standards in place on a national basis".

The same logic applies with respect to protecting the privacy of British Columbian users of telecommunication services. As described above, multiple federal regulations and administrative oversight by the OPC and CRTC provide for a robust framework that protects the PI of telecommunication subscribers. Adding new provincial legislative or regulatory requirements – particularly those which may be inconsistent with federal requirements - would be redundant, create confusion for customers, and impose burdensome regulations on service providers that would impede the competitiveness of important federal undertakings that provide critically important services to British Columbians.

[5] https://crtc.gc.ca/eng/publications/reports/rp170106/rp170106.htm#4

2. Provide a transition period to enable organizations to effectively and efficiently implement new requirements

In considering potential changes to PIPA, the government must take into account the work required for organizations to bring their operations and procedures into compliance with any new obligations under the Act and provide for a transition period from the date of Royal Assent to the time that the new provisions come into force.

Organizations will need to undertake comprehensive reviews of their data management practices and identify necessary changes. They will have to assess and allocate human and financial resources to implement these changes and develop new policies, practices and procedures. Contracts with service providers and other third parties will have to be reviewed and may need to be renegotiated.

Depending on the changes, it is also likely that software and complex IT systems will have to be updated to account for processes, record keeping, and the administration of requests from data subjects that were not required prior to the enactment of the amendments. These IT changes may be complex, significant and costly. They also will not exist in isolation and will be part of a larger group of information technology projects that have to be budgeted for and prioritized by the organization.

A definitive recommendation regarding the length of the transition period can only be made once the scope of the proposed changes is known. However, as an example, with respect to the changes proposed under the federal Bill C-11, we have recommended a minimum general 24-month transition period, with longer transition periods for specific provisions such as those dealing with data portability.

3. Mandatory Data Breach Notifications

If PIPA is amended to include mandatory data breach notification requirements, CWTA agrees with the OIPC that such provisions should be harmonized as much as possible with similar provisions under the federal privacy law.

Of note, with respect to OIPC's recommendation that the notification provisions include requirements regarding the timing of providing notice, it is important that any timing requirements do not prescribe a specific number of days or other time period. The time required by an organization to determine the facts surrounding a potential breach will differ depending on the circumstances. Section 10.1(6) of PIPEDA reflects this need for flexibility as follows: "The notification shall be given as soon as feasible after the organization determines that the breach has occurred."

In addition, CWTA does not agree with OIPC's recommendation that OPIC be given the power to require an organization to notify an individual of a data breach. Under PIPEDA, the organization is required to notify the commissioner and affected individuals if the organization believes that the breach creates a real risk of significant harm to an individual. The commissioner is not entitled to substitute its opinion regarding the risk of harm for that of the organization. Any data breach notification provisions added to PIPA should similarly make the assessment of harm the responsibility of the organization.

4. Transfers to Service Providers

CWTA does not oppose OIPC's recommendation that PIPA be amended to expressly state that organizations are responsible for the PI transferred to a third party for processing. We agree with OIPC that "the rules need not be overly prescriptive" and that "[o]rganizations should simply be required to use contractual or other means to ensure their service providers comply with the law."[6] PIPEDA (and the proposed CPPA) contain similar provisions.

5. Modernizing Consent Requirements

As noted in the OIPC Supplemental Submission, the federal government's CPPA proposes changes to the federal approach to consent and its exceptions. The OIPC has voiced concerns with some of these changes, and in particular, as they relate to exceptions to consent. CWTA also has concerns with some of the consent provisions under the CPPA, but for different reasons.

The proposed CPPA's approach to consent and its exceptions does not correspond to the mechanisms for lawfully collecting and using personal informed employed by Canada's trading partners, nor to the context of consumer relationships across industries. It is also much more restrictive than the GDPR (which has multiple bases for legally processing PI, only one of which is consent[7]) and the California Consumer Privacy Act (CCPA).

The proposed CPPA's focus on consent, its rigid and prescriptive rules for valid consent, and its limited exceptions to consent, mean that organizations governed by the federal law, including those operating in British Columbia, will face the cost and burden of managing a consent regime that is distinct to Canada.

With respect to exceptions to consent, in contrast to California's CCPA and the GDPR, the proposed CPPA makes, with few exceptions, express consent the default basis for the collection, use and disclosure of PI. This would not only put Canada out of step with its trading partners, it would abandon both the flexible approach of PIPEDA that has served

[6] OIPC Supplemental Submission, p11.

[7] GDPR has six bases for legally processing PI, only one of which is consent. The others are performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest.

Canada so well and the rational approach that grounds implied consent in the circumstances that surround it.

The CPPA's approach could disadvantage Canadian organizations by imposing a narrow, rules-based approach to consent. In contrast to the realistic approach adopted in the GDPR and the CCPA, if passed in its present form, the CPPA would require Canadian businesses to disproportionately rely on express consent, with no gain for the individual's privacy. The proposed CPPA's onerous and unique approach to consent means organizations operating in Canada will face the cost and administrative burden of managing a distinct consent regime that is likely to put them at a competitive disadvantage.

Instead, the British Columbia government should consider bases for legal processing information other than consent, such as: business activities that a reasonable person would expect to involve the collection, use or disclosure of their information for those activities; the collection, use and disclosure of information necessary for the performance of a contract with the individual; and for the legitimate interests of the organization where they are not overridden by the data subject's interests as demonstrated by a rigorous and documented analysis of the risks and benefits.

While we arrive there for different reasons, we agree with OIPC's recommendation that the government should take a cautious approach to making changes to the consent provisions of PIPA and continue to monitor progress of the CPPA to see what changes may be put forward to deal with the issues cited above.

With respect to other recommendations put forward by the OIPC, we do not agree that organizations should be required to provide privacy notices separate from other legal terms, if by separate, the OIPC means a separate document and requiring a separate consent. Requiring multiple consents is a contributor to consent fatigue, which leads to individuals not reading the terms and conditions presented to them.

What is important is that the individual's attention is drawn to the most important terms and conditions, including terms related to the collection, use and disclosure of information that a reasonable person would not expect, or that pertains to sensitive PI. It does not require that they be set out in separate documents.

With respect to telecommunications services contracts, as mentioned in section 2 above, the Wireless Code and the Internet Code already require TSPs to communicate privacy policies "in a way that is clear and easy for a customer to read and understand", provide permanent copies of such polices and notify customers of any amendments at least 30

days in advance. Notably, and appropriately, it does not dictate whether such policies are presented separately or together with other legal terms. Fulfilling the "clear and easy" requirement does not depend on how many documents are presented to the customer. In fact, requiring separate documents may have the opposite effect.

Finally, section 10(1) of PIPA permits organizations to give notice of the collection of PI "verbally or in writing". CWTA does not agree with OIPC's recommendation to remove the ability to provide notice verbally. Written notification is not always possible, such as during telephone interactions. While the section 10 notice requirement does not apply to circumstances in which section 8(1) or (2) apply, it is not clear that these sections cover all instances in which written notice is not practicable.

6. Automated Decision-making

The OIPC has recommended that PIPA be amended to address the use of automated decision-making systems (ADS). While the proposed CPPA contains provisions dealing with ADS, it is questionable whether privacy legislation is the appropriate place to deal with this issue.

As leading technology law expert Barry Sookman has noted:

> The automated decision systems provisions of [Quebec] Bill 64 and the *CPPA*, like the comparable provisions in the GDPR, are not, however, truly directed at privacy-related mischief. They regulate the use of particular technologies more than the use of information – though, due to the nature of the technologies in question, the line is admittedly difficult to draw. Further, the goals are not the protection of reasonable expectations of privacy – which is what privacy laws advance – but to avoid other harms such as ensuring that decisions are not biased or inaccurate.[8]

These potential harms, Mr. Sookman argues, are already addressed under other regulatory frameworks such as competition laws, consumer protection laws, and human rights legislation:

> …the regulation of automated decision making under privacy law will likely result in privacy commissioners such as the OPC, with limited or no expertise in the

[8] https://www.barrysookman.com/2021/04/30/using-privacy-laws-to-regulate-automated-decision-making/

> other regulatory areas, becoming mixed up in areas that are better handled by the existing regulatory regimes already in place.[9]

To the extent that existing regulations do not address all of the issues arising from the use of ADS, stand-alone legislation or best-practices are more appropriate than trying to deal with the complex issue under privacy laws.

If, notwithstanding the above, the government decides to amend PIPA to address the use of ADS, such amendments should be limited in their scope. With some adjustments, sections 2, 62 and 63 of the proposed CPPA provide a useful framework for the government.

The definition of "automated decision system" in section 2 of the CPPA consists of "technology that assists or replaces the judgment of human decision-makers…". This definition is too broad. Not all systems are the same, and the degree to which they aid human decision-making will vary. The focus on any regulation of ADS should be limited to those systems that could materially impact human decision-making.

Similarly, the obligations to describe and, if requested explain, the use of ADS systems set out in section 62 and 63 of CPPA should be limited to circumstances in which the use of ADS could have a significant impact on the individual. This qualification is included in the transparency obligation of section 62, but is currently absent from the explanation obligation in section 63. If the government adopts a similar framework to that set out in CPPA, achieving the appropriate balance between protecting consumers and not imposing unnecessary burdens on organizations requires that a "significant impact" qualifier be applied to all obligations of the organization.

Finally, we agree with the OIPC that the GDPR goes too far in its regulation of ADS by giving the individual, with some exceptions, the right to veto the use of ADS. We also agree with the proposed CPPA which requires, upon request, an explanation of a use of ADS, but does not give the individual the right to challenge the decision. As referenced above, privacy legislation is not the appropriate vehicle for addressing all potential harms arising from the use of ADS.

[9] Ibid

7. Right to be Forgotten/Request Disposal

As noted by the OIPC, PIPA already contains protection from the use of outdated and inaccurate PI. Where PIPA and the proposed CPPA differ is that CPPA introduces a right, subject to some exceptions, for individual data subjects to request an organization to dispose of the requestor's personal information.[10]

While we do not oppose a right to request the disposal of PI, we have concerns with the way that the current draft CPPA does so. Section 53 of the proposed CPPA recognizes that organizations should be able to retain such information as long as is necessary to fulfil the purpose of the collection and to comply with CPPA and other legal obligations. However, this recognition is undermined by Section 55 (the section that implements the right to request disposal of PI) as the exceptions listed in that section do not cover all of the circumstances under which an organization may need to retain such information despite a disposal request.

We expect that these deficiencies will be addressed during the review process of CPPA, and we agree with the OIPC's recommendation that the government, "rather than amend PIPA to implement a form of the "right to be forgotten"….should continue to monitor developments…"[11]

Notwithstanding the foregoing, should the government introduce a right for data subjects to request the disposal of their PI, the exceptions to such right must be broader than those in the draft CPPA. For example, Article 17 of the GDPR, which provides the GDPR's version of the right to request disposal, does not apply if the organization needs to process PI to exercise the right of freedom of expression and information, to comply with a legal obligation, or for reasons of public health, archiving in the public interest or the establishment, exercise or defense of legal claims as the organization may choose to exercise.

With respect to the right to be forgotten (or deindexing), we agree with OIPC's recommendation that the provincial government should continue to monitor developments in this area before putting forward any amendments to PIPA. If, in the future, amendments are proposed, they should be carefully calibrated to address the risk of individual harm without negating other rights of organizations. For example, while it may be appropriate to require an organization to remove public access to information

[10] Section 55 of CPPA

[11] OIPC Supplemental Submission, p16

about an individual, requiring disposal of that information by the organization is a separate issue and should recognize that, as discussed above, there may be legitimate reasons to allow the organization to retain that information.

8. Data Portability

In its initial and supplemental recommendations to the government, the OIPC recommends that PIPA be amended to require organizations, upon request of the data subject, to transfer the data subject's PI to an organization that the data subject designates if it is technically feasible to do so without undue cost to the organization.[12] The reason cited by the OIPC is that "this right could have economic benefits because it can sharpen competition among businesses and may help prevent PI monopolies from forming."[13]

While we recognize that the concept of data portability is useful in the context of voluntary participation in data trusts and other data management schemes, CWTA has concerns with introducing a portability right within PIPA and applying the corresponding obligations to all industry sectors.

First, while the inability to easily transfer PI to an alternate service, such as some social media platforms or online data storage services, may present a barrier to switching service providers, such is not the case with every industry, including mobile wireless services. Wireless subscribers can easily switch to another wireless service provider, including being able to use the same phone number with the new service provider. This process is overseen by the CRTC which, given its expertise, is best-placed to determine whether there are any barriers to switching providers, and if so, how to address them.

Requiring the mobile wireless industry, and similarly situated sectors, to engineer technical solutions and procedures to enable personal data transfers that will provide little, if any, benefit to consumers is an unnecessary burden that will only make the provision of services more costly. It also gives rise to potential security risks as fraudsters could attempt to impersonate consumers and use the portability right to illegally obtain consumer's PI.[14] In fact, it may require organizations to collect even more PI from individuals for the sole purpose of being able to verify the individual's identity in case a data transfer request is made.

[12] Ibid, p17
[13] Ibid, p17-18
[14] See https://www.theregister.co.uk/2019/08/09/gdpr_identity_thief/ for examples of how fraudsters have used new individual rights under the GDPR to illegally obtain information.

Secondly, in sectors where the inability to easily transfer PI presents a potential barrier to competition, the matter is better dealt with under competition law.

The federal government is appropriately taking a cautious approach to introducing data portability rights. While section 72 of the draft CPPA includes such a right, it is qualified by the requirement that both organizations must be subject to data portability framework that is to be provided under future regulations.

Rather than amending PIPA to include a data portability right, the government should continue to monitor developments regarding data portability in CPPA. As the OIPC acknowledges, "the provincial government will likely need to work closely with the federal government to seek harmonization between the CPPA regulations for a data portability framework and PIPA's provisions on this issue."[15]

If data portability requirements are introduced, they should not be applicable to industries, such as telecommunications, which are already subject to industry-specific regulatory oversight which can better assess the merits of applying such obligations to the applicable industry.

If such a right is implemented under PIPA, in addition to them being subject to an applicable data portability framework that provides for standard processes and safeguards, impacted organizations must be provided sufficient time to implement such frameworks. The wireless industry's experience with designing and implementing a mobile number portability framework shows that operationalizing data portability is a time consuming, costly, and often difficult task. As we have recommended to the federal government, PIPA should defer the entry into force of the data mobility provisions to three years after the applicable data mobility regulations are enacted.

Finally, organizations should only be required to transfer information provided by the data subject, and should not be required to transfer information created by the service provider, including inferred data and derived data. Exceptions where compliance would reveal a trade secret or otherwise provide the new service provider a competitive advantage should also be included.

[15] OIPC Supplemental Submission, p18.

9. Administrative Monetary Penalties

The OIPC currently has several tools at its disposal to ensure compliance with PIPA, including the power to investigate, audit, and attempt to resolve and mediate complaints. It also provides guidance to organizations regarding their business practices. This collaborative approach has been very successful with most valid complaints being resolved voluntarily. If a voluntary settlement is not reached, OIPC may hold a formal inquiry. As part of the inquiry it can compel testimony, order the production of evidence, enter premises and issue binding orders. It can also refer a matter to the Supreme Court of British Columbia for prosecution and the Court can issue fines of up to $10,000 for individuals and $100,000 for organizations. Individuals also have remedies under a private right of action as well as through privacy claims in tort and contract law.

Providing the OIPC with the power to levy administrative monetary penalties (AMPs) would undermine the collaborative model that currently exists under PIPA. Rather than seeking proactive guidance from the OIPC regarding proposed organization initiatives, many organizations would hesitate to consult with the OIPC knowing that it has the power to directly impose significant monetary penalties on them. This would harm the government's goal of fostering economic growth through the responsible use of data and digital technology.

If, notwithstanding the above, the government wishes to increase the fines that can be levied under PIPA, it should proceed cautiously and ensure that it is done in a fair and proportionate manner. Most importantly, the assessment of significant fines should be reserved for instances of egregious non-compliance with key provisions of PIPA. This point reflected in the OIPC Initial Submission: "Monetary penalties would be reserved for the most serious violations of the law, for the worst offenders and the worst offences."

Additional procedural protections should be considered. First, for the reasons discussed above, a decision to levy fines should not rest with the OIPC, but rather with the courts.

Any increase in the size of fines must be accompanied by specific factors that courts must consider when assessing penalties. Section 93(2) of the proposed CPPA seeks to protect the fairness in the recommendation of a penalty with the following factors that must be considered: the nature and scope of the contravention; whether the organization has voluntarily compensated the affected individuals; and the organization's history of compliance.

What should also be included is the novelty of the facts or findings in the case as well as the organization's due diligence and good faith in attempting to comply with PIPA. For example, cyber-attacks are a constant and evolving threat. Even the most highly-protected institutions, including the military, suffer breaches of security. Fairness dictates that the application of penalties must be limited to organizations that have not met their obligations. In the case of security obligations, the test is not whether there has been a breach, but rather whether the organization has met its due diligence obligations in implementing security safeguards.

10. Enhancing and clarifying Commissioner oversight powers

CWTA does not agree with OIPC's recommendation that the reasonable grounds threshold for initiating audits or investigations be removed. The overwhelming majority of organizations in Canada work hard to do the right thing and should not be subject to arbitrary audits or investigations if there are no reasonable grounds to believe that the organization is not complying with PIPA. Removing the reasonable grounds threshold would expose organizations to "fishing expeditions" that would be unfairly disruptive to the organization's operations and potentially tarnish the organization's reputation. It would also erode the trust and collaborative relationship between the OIPC and organizations that must remain at the centre of PIPA.

While the OIPC cites FIPPA as an example of a statute that does not contain a reasonable grounds threshold, there are plenty of other statutes where reasonable grounds or similar thresholds are required before launching an investigation.[16] Notably, despite enhancing the powers of the federal Office of the Privacy Commissioner under the proposed CPPA, Bill C-11 retains the reasonable grounds threshold for initiating an audit or investigation.[17] The OIPC should be required to continue to focus its finite resources on matters for which there are reasonable grounds to think that a contravention of PIPA has occurred.

[16] e.g. *Canadian Human Rights Act* and the *Competition Act*

[17] See sections 82 and 96 of the draft CPPA

For questions or comments regarding this submission, please contact:

Robert Ghiz
President & CEO
rghiz@cwta.ca

Eric Smith
Senior Vice President
esmith@cwta.ca