August 20, 2021

Hon. Nate Glubish
Minister of Service Alberta
Office of the Minister
Service Alberta
103 Legislature Building
10800-97 Avenue
Edmonton, AB
T5K 2B6

Sent via email: modernizingprivacy@gov.ab.ca; ministersa@gov.ab.ca

Dear Minister Glubish:

Re: Public Consultation – Modernizing Privacy Protection in Alberta

1. We are writing you with respect to the Service Alberta's request for feedback regarding *Modernizing Privacy Protection in Alberta* (Consultation).[1]

2. The Canadian Wireless Telecommunications Association (CWTA) is the recognized 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.

3. The following comments focus on potential amendments to Alberta's Personal Information Protection Act (PIPA) and related topics raised in the Consultation's online survey. Failure to address an item mentioned in the survey should not be construed as agreement with a government proposal. In addition, to the extent there is any inconsistency between CWTA's submission and that of a CWTA member, in regards to the position of such CWTA member, the member's submission shall prevail.

[1] https://www.alberta.ca/privacy-protection-engagement.aspx

Balancing privacy protection and the legitimate use of data

4. CWTA and its members recognize that the protection of personal information and customer trust are important to ensuring Albertans' confidence in digital services. That is why our members have made the protection of personal information a key element of their business practices and corporate values, and continue to invest significant resources into their privacy-related processes and security.

5. The world is undergoing a digital and data-driven revolution in which the innovative combination of data and technology will enable Albertans to be more productive, generate economic growth, and deliver a higher quality of life. That is why it is important to balance the legitimate and responsible use of data, including innovative uses of personal information, with the protection of privacy.

6. This balance is recognized in section 3 of PIPA which states that the Act "recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable."

7. As privacy legislation in other jurisdictions in Canada is undergoing review, some commentators argue that the privacy right should be elevated above all other rights and legal interests, including an organization's right to use data for purposes that are reasonable. Yet even some supporters of the European Union's General Data Protection Regulation (GDPR) now recognize the undesirable consequences that this can cause.

8. Alex Voss, Member of the European Parliament, and other author of the report '*Comprehensive approach on personal data protection in the EU',* which resulted in the subsequent GDPR, now laments the disproportionality between privacy and other fundamental rights in the GDPR and the resulting negative impacts on innovation in the EU. By elevating the right to privacy above all other fundamental rights and legal interests, "the GDPR is seriously hampering the EU's capacity to develop new technology and desperately needed digital solutions, for instance in the realm of e-governance and health."[2]

9. PIPA demonstrates that it is possible to protect the rights of individuals without the need to abandon the appropriate balance between privacy and commerce. The Alberta

[2] https://www.politico.eu/article/gdpr-reform-digital-innovation/. See also - https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf

government should steadfastly ensure that this balance is preserved in any amendments to PIPA.

10. **Recommendation:** As its stated purpose, PIPA should maintain the balance between the protection of privacy and the legitimate and responsible use of data. The current section 3 of PIPA should be retained.

PIPA should not apply to federal undertakings

11. Similar to section 3(2)(c) of British Columbia's *Personal Information Protection* Act, PIPA should be amended to expressly state that it 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." The absence of such a provision creates uncertainty and confusion in areas, such as the telecommunication sector, that are already governed by federal privacy laws. This uncertainty creates confusion for Albertans regarding their rights and where to go for resolution of a privacy matter.

12. As part of the British Columbia government's consultation regarding its privacy regulations, the British Columbia Information and Privacy Commissioner described the impact of overlapping federal and provincial privacy regulations:

> From the individual complainant's perspective, this regulatory morass tends to create unnecessary confusion as to which law applies and to which oversight body one should complain. For organizations, this can lead to duplicative investigative processes and potentially conflicting outcomes. From the taxpayers' standpoint, this can be perceived as needless bureaucracy and a waste of valuable resources. For policy-makers, it risks impeding innovation and dissuading global investors, setting back the government's economic objectives.[3]

13. Albertans' personal information is already well-protected in the context of the telecommunications services that they receive pursuant to multiple federal laws and regulations applicable to federally-regulated undertakings generally and to TSPs specifically.

14. Canada is known for taking a leadership role in the protection of personal information. The collection, use, and disclosure of personal information 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

[3] Information and Privacy Commissioner of Ontario, Letter to Minister Thompson re: Ontario Private Sector Privacy Reform Discussion Paper, October 16, 2020 - https://www.ipc.on.ca/wp-content/uploads/2020/10/2020-10-16-ipc-private-sector-consultation-submission.pdf (IPC Submission)

globally. With advances in technology and new ways of using personal information, the federal government proposed new legislation, which would preserve the balanced, principles-based approach of PIPEDA, while creating important new individual rights and protections of personal information. Despite the recent dissolution of Parliament and an upcoming federal election, it is expected that the new federal government will reintroduce legislation to revise PIPEDA.

15. 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 federal Office of the Privacy Commissioner (OPC), the CRTC has the power to create regulations concerning privacy with respect to telecommunications services.

16. 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 the express consent of the customer, except in certain specified circumstances;
    b. Prohibiting TSPs from using personal information 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 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 Telecommunications Rules framework.

17. 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 communications 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.*[4]

18. 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.

19. As the above examples illustrate, the CRTC and the OPC have complementary roles in protecting the privacy of TSP customers across Canada, including Alberta. Given expected changes to PIPEDA that will address new ways in which personal information 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 Albertans who use federally-regulated telecommunications services.

20. Finally, the Government of Alberta has previously recognized that having overlapping provincial and federal regulations regarding the provision of telecommunication services is unnecessary to protect the interests of Albertans. During the consultation process for the federal Wireless Code, the issue of potential conflicts between the Code and provincial consumer protection laws was a key topic of discussion. Most participants expressed the need for a national standard consistently applied across Canada. In its submissions to the CRTC as part of the proceedings which established the Code, the Government of Alberta advocated for one national standard:

> I think it's obvious that having 10 provinces with varying legislation could be a regulatory nightmare for consumers and wireless service providers. A national solution is really the only way to go on this. It will really ensure consistency across all provinces and territories and best serve consumers and service providers (…) As someone who is advocating for Alberta consumers, current and future, a national

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

Code is the most appropriate solution to address the challenges many are experiencing.[5]

21. The same logic applies with respect to protecting the privacy of Albertan 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 personal information of telecommunication subscribers. Adding provincial privacy regulations– particularly those which may be inconsistent with federal requirements - creates confusion for customers, and imposes burdensome regulations on service providers that would impede the competitiveness of important federal undertakings that provide critically important services to Albertans.

22. **Recommendation:** PIPA should be amended to expressly state that it 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.

Avoid patchwork of regulations and undue administrative burden and costs

23. Undue burdens and costs can also be created when there is a lack of harmony between privacy regulations in various provinces and at the federal level. While our recommendation above that PIPA not apply to the collection, use and disclosure of personal information that is covered by federal privacy laws would address this concern for federal undertakings, where such is not the case, it is important that organizations not be subject to different requirements in each Canadian jurisdiction. For this reason the Alberta government should monitor the privacy reforms currently underway elsewhere in Canada and work to avoid contributing to a patchwork of privacy regulations that will make Alberta a less desirable place to operate, and that make it difficult for organizations to conduct business across Canada.

24. In considering new individual rights, such as data portability, or new obligations for organizations, the government should avoid creating undue burdens on organizations, especially where the burden outweighs any corresponding benefit to individuals.

25. For example, the government survey raises the question of whether PIPA should include an individual right to request that an organization provide the individual's personal information in its possession to another organization. This is commonly referred to as data portability.

[5] Speaking notes of Service Alberta Minister Bhullar for CRTC public hearing February 14, 2013. https://services.crtc.gc.ca/pub/DocWebBroker/OpenDocument.aspx?DMID=1844949

26. 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 and applying the corresponding obligations to all industry sectors.

27. First, while the inability to easily transfer personal information 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.

28. 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 personal information.[6] In fact, it may require organizations to collect even more personal information from individuals for the sole purpose of being able to authenticate the individual in case a data request transfer is made.

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

30. The federal government is appropriately taking a cautious approach to introducing data portability rights. While section 72 of the federal government's draft Consumer Privacy Protection Act (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 yet to be drafted regulations.

31. **Recommendation:** The costs and benefits of any proposed new individual rights or obligations on organization should be carefully considered so as not to create undue burdens and costs for organizations. Any amendments to PIPA should be subject to further public consultation so that stakeholders can provide feedback regarding same. In addition, the Alberta government should closely monitor the privacy reform activities currently underway elsewhere in Canada to ensure that PIPA does not impose obligations that are inconsistent with those in other Canadian jurisdictions.

---

[6] 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.

Preserving the collaborative role of the IPC

32. The main goal of any private sector privacy regime should be to help organizations comply with the law. This is best achieved when the regulator is able to work cooperatively with organizations to provide guidance and consultation on how organizations can achieve their business objectives while respecting the privacy rights of individuals.

33. The Office of the Information and Privacy Commissioner (IPC) currently has several tools at its disposal to ensure compliance with PIPA, including the power to investigate and attempt to resolve and mediate complaints. This collaborative approach has been very successful, with most valid complaints being resolved voluntarily. If a voluntary settlement is not reached, the IPC may hold a formal inquiry and issue binding orders. It can also refer a matter 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.

34. Notwithstanding these tools and the fact that most complaints are resolved voluntarily, the IPC has called for PIPA to be amended to grant it the power to impose administrative monetary penalties (AMPs) for certain violations of the Act.[7] Providing the IPC with the power to levy AMPs would make the IPC both the enforcer and the advisor, putting at risk much of the benefits of the current collaborative approach. Many organizations would hesitate to consult with the IPC knowing it has the power to directly impose significant monetary penalties on them. At the same time, the IPC may find that it no longer has the resources to engage constructively with organizations as it devotes the bulk of its resources to enforcement actions. Both of these outcomes would harm the government's goal of fostering economic growth through the responsible use of data and digital technology.

35. If, notwithstanding the above, the government proposes 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. As the IPC (British Columbia) stated in its submission to the government of British Columbia: "Monetary penalties would be reserved for the most serious violations of the law, for the worst offenders and the worst offences."[8]

[7] See letter from IPC to Minister Glubish at https://bit.ly/3sr9Iy4
[8] https://www.oipc.bc.ca/special-reports/3465

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

37. Second, any increase in the size of the fines must be accompanied by specific factors that courts must consider when assessing penalties. In Section 93(2) of the federal government's proposed CPPA, the government sought 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.

38. 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.

39. **Recommendation:** The government should exercise caution in considering any amendments to PIPA that would negatively impact the IPC's ability to work cooperatively with organizations to resolve and mediate complaints. Any proposed increases in fines should be reserved for the most serious violations and only for those organizations that show blatant disregard for their obligations. In addition, any increases in fines or the enforcement powers of the IPC must be made in a proportionate manner that provides organizations with procedural fairness.

Consent and alternatives to consent

40. Consent fatigue is a real problem for organizations and individuals. If individuals are asked to provide express consent for nearly all collections and uses of personal information, rather than just for activities they would, under the circumstances, not expect, or for activities that require the collection and use of sensitive information, the act of seeking express consent will lose its meaning and individuals will not take consent requests seriously. We have seen this phenomenon occur with website cookie notices under the GDPR.

41. To address this issue, the government should consider alternate grounds for the lawful collection, use, and disclosure of personal information. For example, the GDPR takes a much more flexible approach to consent collection, fully recognizing the contextual nature of the requirement for express or implied consent by allowing processing without express consent where "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are*

overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[9]

42. Singapore has also recently clarified its consent requirements and added two new exceptions to the consent requirement: legitimate interests and business improvement.[10] In addition, while CWTA has concerns with the overly prescriptive nature of some of its proposed provisions, the federal government included several alternatives to consent in its draft CPPA.

43. **Recommendation:** To ensure that consent is meaningful and reduce consent fatigue, the government should consider exceptions or alternatives to consent.

44. CWTA appreciates the opportunity to provide its comments regarding this matter. We trust that any proposed amendments to PIPA will be subject to further consultation with stakeholders and we look forward to participating in same.

For questions or comments regarding this submission, please contact:

Robert Ghiz
President & CEO
rghiz@cwta.ca

Eric Smith
Senior Vice President
esmith@cwta.ca

[9] GDPR, Article 6(1)(f)
[10] https://www.jonesday.com/en/insights/2021/02/singapores-personal-data-protection-regime-enhanced