September 28, 2020

Parliamentary Committee on Institutions
Édifice Pamphile-Le May
1035, rue des Parlementaires
3e étage
Québec (Quebec) G1A 1A3

Email: ci@assnat.qc.ca

Dear Committee Members:

Re: Special consultations and public hearings on Bill 64, An Act to modernize legislative provisions as regards the protection of personal information – Proposed amendments to the *Act respecting the protection of personal information in the private sector*

1. The Canadian Wireless Telecommunications Association 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, who combine to deliver world-class wireless services, one of the key pillars on which Quebec's digital and data-driven economy is built.

2. We are writing you with respect to the Government of Quebec's consultation (Consultation) regarding Bill 64, *An act to modernize legislative provisions as regards the protection of information*, and in particular, the proposed amendments to the *Act respecting the protection of personal information in the private sector* (Act).

3. As a world-leader in the development of artificial intelligence (AI), Quebec is keenly aware that the world is undergoing a digital and data-driven revolution in which the innovative combination of data and technology will enable Quebecers to be more productive, generate economic growth, and deliver a higher quality of life. But with each new opportunity comes potential new risks, and 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.

4. It is for that reason we welcome the Government's review of the Act to ensure that it properly addresses technological and societal change and ensures consumer trust, without imposing unnecessary burdens on businesses, or inhibiting the growth and prosperity of Quebec's economy and innovation ecosystem.

5. In this submission we do not comment on every proposal contained in Bill 64. We have limited our response to those matters we consider to be of greatest importance to our members. Our decision to

not provide a response to particular proposals in Bill 64 is not an indication of CWTA's agreement with such proposals.

Creating Compatible Privacy Regulations

6. In considering changes to Quebec's private sector privacy regulations, it is important that the Government avoid contributing to the creation of a patchwork of privacy laws across the country. With the Digital Charter, released in early 2019, the federal government committed to modernizing the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). In addition, the government of British Columbia has completed consultations on reform of its privacy legislation, and Ontario is currently conducting a public consultation regarding possible new private sector privacy regulations. This patchwork of varying privacy regulations risks creating unnecessary confusion for consumers of federally-regulated businesses and an undue burden for such organizations.

7. As many Quebec-based businesses also operate elsewhere in Canada, it important that Quebec consult and coordinate with the federal and other provincial governments to avoid imposing significantly different measures on businesses that operate in Quebec. For example, having different consent rules or breach reporting requirements, including the thresholds for triggering a notification requirement, will require Quebec-based businesses that operate elsewhere in Canada to establish multiple policies and procedures for dealing with personal information. This creates an unnecessary and costly burden for businesses.

8. Harmonizing Quebec law with interprovincial and federal law will help ensure that Quebec businesses are not put at a disadvantage, while still protecting the personal information of Quebecers. In particular, we recommend that Quebec wait to see proposed changes to PIPEDA before finalizing Bill 64.

9. **Recommendation:** Consult and coordinate with other Canadian jurisdictions that have their own private sector privacy regulations to ensure that Quebec privacy law is compatible with interprovincial and federal law and does not create unnecessary burdens on businesses operating in Quebec or cause confusion for Quebec consumers. In this regard, Quebec should wait to see proposed changes to PIPEDA before finalizing Bill 64.

Cross Border Data Flows and Equivalency

10. Bill 64 proposes amendments to Section 17 of the Act that will, in part, require an entity seeking to transfer personal information outside Quebec to conduct a privacy assessment, including an assessment of the legal framework governing personal property of the state in which the information will be communicated. It further provides that the personal information cannot be transferred if the receiving state does not have a legal framework that provides protections equivalent to those afforded by the Act. A new section 17.1 provides that the Minister will publish a list of states whose legal framework is equivalent to the protections applicable in Quebec. These restrictions apply equally to transfers to persons or organizations outside Quebec who are processing personal information on behalf of the transferor.

11. While the proposed amendments to Section 17 are intended to require organizations to exercise due diligence before transferring personal information outside Quebec, as drafted the provisions create impractical and potentially harmful burdens for businesses and should be reconsidered.

12. As recently observed by Jennifer Stoddard, former Privacy Commissioner of Canada and Chair of the Access to Information Commission for Quebec, the experience of the EU with equivalency illustrates that conducting such analyses is a time-consuming and resource heavy exercise.[1] Even with its large bureaucracy, the EU has spent years analyzing the equivalency of individual countries' legal frameworks, with key issues still unresolved. It is likely that the Government of Quebec, with more limited resources, will find it to be extremely difficult to perform such assessments in a timely manner. For most businesses, conducting their own assessment of receiving state legal frameworks will be beyond their capability and resources.

13. Moreover, unlike the EU's General Data Protection Regulation (GDPR), the proposed amendments of Bill 64 do not provide for an alternate mechanism that permits the transfer of personal information outside Quebec if it is determined that a jurisdiction does not have equivalent privacy laws. The absence of an alternate mechanism will hurt Quebec-based businesses, many of which rely on third-party outsourcing or who wish to expand their businesses into new markets. This will reduce the ability of Quebec businesses to compete and reduce consumer choice if businesses avoid doing business in Quebec due to their inability to transfer data beyond Quebec.

14. The proposed equivalency requirement may also violate Canada's obligations on cross-border data transfers under the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP) and the *Canada-United States-Mexico Agreement* (CUSMA). The lack of an alternative to equivalency may be in violation of CPTPP Article 14.11 and CUSMA Article 19.11 which prohibit undue restrictions on the movement of data for business. The equivalency requirement may also be a de facto requirement for companies to maintain computing facilities within Quebec as a condition of doing business and thus violate Article 14.13 of CPTPP and Article 19.12 of CUSMA.

15. It is also not clear whether the term "state" applies to other provinces and territories. Such a designation would impose significant hurdles on the transfer of information between provinces and territories, putting Quebec businesses at a distinctive disadvantage.

16. **Recommendation:** The following changes should be made to the proposed amendments to Section 17 and Section 17.1.

> *17. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct an assessment of privacy-related factors ~~must~~, in particular, ~~take into account~~*
> *(1) the sensitivity of the information;*
> *(2) the purposes for which it is to be used; and*
> *(3) the protection measures that would apply to it, including contractual measures. ~~; and~~*
> *~~(4) where appropriate, the legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principles applicable in Québec~~.*

[1] https://financialpost.com/opinion/jennifer-stoddart-quebec-takes-the-lead-in-privacy-law-but-overreaches#:~:text=from%20our%20team.-,Jennifer%20Stoddart%3A%20Quebec%20takes%20the%20lead%20in%20privacy%20law%20but,inter%2Dprovincial%20and%20international%20trade.

The information may be communicated if the assessment establishes that it would receive a comparable level of protection through legislative, contractual or other measures ~~equivalent~~ to that afforded under this Act. ~~The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.~~

The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on its behalf.

This section does not apply to a communication of information under subparagraph 7 of the first paragraph of section 18.

~~17.1. The Minister shall publish in the Gazette officielle du Québec a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec.~~

17. If, despite the recommendation above, the equivalency requirement is maintained, alternative mechanisms for transferring personal information to non-equivalent jurisdictions should be introduced.

Consent

18. Bill 64 is confusing with respect to the forms of consent required. For example, while proposed sections 12 and 13 suggest that express consent may not be required in all instances, Section 14 states that consent must be "given for specific purposes" and "*must be requested for each such purpose*, in clear and simple language and *separately from any other information provided to the person concerned*"(emphasis added). The broad scope of Section 14 does not consider the important role played by implied consent in most privacy legal frameworks, where express consent is not required in circumstances where personal information is voluntarily provided, the information is not sensitive information, and the purpose of collection and use is within the reasonable expectations of the data subject. The limited alternatives or common exceptions to consent imposes a heavy burden on businesses and, together with the requirement that consent be requested for each purpose and separately from any other information provided to the data subject, risks creating consent fatigue for consumers.

19. **Recommendation:** The following changes should be made to the proposed Section 14:

14. When explicit consent is appropriate under this Act, such consent must be clear, free and informed ~~and be given for specific purposes~~. It must be requested ~~for each such purpose,~~ in clear and simple language ~~and separately from any other information provided to the person concerned~~. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.

The consent of a minor under 14 years of age is given by the person having parental authority.

.

The consent of a minor 14 years of age or over is given by the minor or by the person having parental authority.

~~*Consent is valid only for the time necessary to achieve the purposes for which it was requested. Consent not given in accordance with this Act is without effect.*~~

Employee Personal Information

20. Bill 64 does not provide for an exception to the consent requirement for employee personal information. It is generally accepted that an employee cannot "freely" consent to the collection or use of their personal information by their employer given the imbalance in the employee/employer relationship. As a result, employee consent exceptions are found in the privacy laws of other jurisdictions.

21. Under privacy regulations in B.C. and Alberta, consent is not required for employers to collect, use and disclose employee personal information that is necessary for establishing, managing or terminating an employment relationship.[2] Similar exceptions have been proposed as part of the legislative review of the federal PIPEDA, which currently only contains limited exceptions regarding "federal works".

22. In the European Union, an employer may process their employees' personal data without consent where the processing is necessary for the performance of the employment contract or to comply with the employer's legal obligations, or in the context of "legitimate interests".[3]

23. **Recommendation:** The following exception to the requirement for consent should be added to Bill 64:

Any person may collect, use and disclose personal information without the consent of the individual if:

> (a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the person, enterprise or business and the individual; and
> (b) the person, enterprise or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

Monetary Penalties and Private Right of Action

24. Bill-64 creates new penalties that are not proportionate and lack appropriate procedural safeguards. Potential fines of up to the greater of $25,000,000 or 4% of worldwide turnover for the preceding fiscal year (s.91) - which fines would double for a subsequent offence – and administrative monetary penalties (AMPs) of up to the greater of $10,000,000 or 2% of worldwide turnover for the preceding fiscal year (s.90.12) are excessive and pose a significant risk of fines and AMPs that are not proportionate to the circumstances of specific cases.

25. The threat of excessive fines and AMPs risks negatively impacting innovation and economic growth in Quebec. Where the Quebec market represents a small portion of their customer base, businesses may be reluctant to conduct business in the province, or may withhold their latest innovative products or services for fear that, despite exercising reasonable due diligence, they could become the subject of a privacy complaint. This is especially the case given that Bill 64 does not provide for robust procedural safeguards with respect to the AMP process.

---

[2] *PIPEDA*, sect. 7.3; PIPA (BC) sects. 13, 16 and 19; PIPA (Alberta), sects. 15, 18, 21

[3] GDPR, art. 6.

26. Bill 64 also introduces a private right of action that exposes businesses to liability even if they acted reasonably and responsibly, or could otherwise establish they were not at fault. This strict liability for privacy offences creates an unreasonable burden for businesses operating in Quebec.

27. **Recommendation:** The following changes should be made to the provisions dealing with fines, AMPs and the private right of action:

    a. The maximum fixed dollar amounts for fines and AMPs should be reduced;
    b. The use of worldwide turnover to calculate fines and AMPs should be eliminated;
    c. The private right of action should not be implemented unless, and until such time, it has been clearly determined that fines and AMPs have not been a meaningful deterrent and the benefit of imposing such private right action outweighs the potential negative impacts on businesses;
    d. If a private right of action is implemented, it should allow for appropriate defences, including the exercise of due diligence.

Data Portability

28. CWTA has concerns with introducing a portability right and applying the corresponding obligations to all industry sectors.

29. Data portability is typically regarded as a potential solution to situations where the inability to transfer personal information from one service provider to another presents a potential barrier to competition. As such, it is not a privacy matter, but rather one that is better dealt with under competition law.

30. Moreover, 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.

31. 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.[4] 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.

32. Notwithstanding the above, should a right of portability be implemented it should include several restrictions. First, in order to protect against fraud, the request for a data transfer should have to come from the data subject, not the organization to whom the data is to be transferred. Data portability should also not cover all personal data, as portability is different than a right to access. Portability should only apply to information that was provided by the data subject as well as observed data that is indirectly provided by the data subject when using the service (e.g. location data, activity logs, etc.). In

[4] 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.

addition, it should not include data and information that is derived from such information. Derived information is the work product of the organization and in many cases will comprise of intellectual property rights or commercially sensitive or confidential information of the organizations.

33. Exceptions should also include instances in which transferring information would: be contrary to law; prejudice an investigation; reveal proprietary processes or technologies; or be technically unfeasible. In addition, where an individual has provided information that includes third-party information (e.g. photos uploaded to cloud storage or a social media account) it is not reasonable to expect transferring organizations to separate third-party information from that which pertains solely to the customer. Transferring organizations should also be permitted to decline to transfer such information if the individual refuses to first provide reasonable assurances that he or she has the right to provide such information, including third-party information, to the transferee organization. Organizations should also be shielded from liability for transferring such information where they receive such assurances.

34. **Recommendation:**

a. The implementation of a data portability right should be postponed until the scope and mechanics of such right can be fully explored by Government, including considering the potential introduction of a data portability right by the federal government; and
b. Data portability obligations should only apply to industry sectors where the potential benefit to consumers outweighs the burdens imposed on businesses. If introduced, the right should be implemented in a staged, sector by sector approach, and only after engaging with impacted industry sectors to develop the sector-appropriate framework

Security/Confidentiality by Default

35. Bill 64 requires organizations to "protect personal information held by person" (s.3.1) and establish and implement policies and practices that "ensure" the protection of such information (s.3.2). These unqualified obligations are inconsistent with the requirements of Section 10 of the Act which states that organizations must take security measures that "are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of information and the medium on which it is stored."

36. PIPEDA, PIPA AB and PIPA BC qualify the information security safeguarding obligations on organizations by obligating organizations to implement safeguarding measures that are "reasonable" and "appropriate" in the circumstances. (PIPEDA, Principle 4.1; PIPA AB s. 34; PIPA BC, s. 34). Similarly, the GDPR's standard for safeguarding requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Art.5(1)).

37. Such qualifications recognize that there is not a "one size fits all" approach to security, and that the level of security measures required should be proportionate to the circumstances, including the sensitivity level of the information involved. Bill 64 should adopt a similar approach.

38. The proposed Section 9.1 of the Act requires "technological product[s] or services[s]" be set to the "highest level of confidentiality by default, without any intervention by the person concerned" (s.9.1). This requirement imposes a standard that is much higher and less practical than the "privacy by design" concept under the EU's GDPR. The GDPR requires the data controller to implement

"appropriate technical and organizational measures" for implementing data protection principles in an effective manner, taking into account the nature, scope, context, risks and purposes of processing. (Art. 25(1)). Similarly, the GDPR requires data controllers to implement "appropriate" technical and organizational measures to ensure that by default, "only personal data which are necessary for each specific purpose of the processing are processed" (Art. 25(2)).

39. Consumers expect the products and services they use to protect their personal information, but also to operate in the manner which they expect. A requirement to implement the highest level of confidentiality by default may negatively impact the individual's use of the product or service and require the individual to spend considerable time programing the product or service to operate as intended. This could lead to an increase in customer complaints and calls to technical or customer support centres, all of which will result in an increase in the cost of doing business in Quebec.

40. **Recommendation:** Bill 64 should apply a flexible approach to the security and confidentiality requirements under proposed Sections 3.1, 3.2 and 9.1 of the Act. As is the case in other jurisdictions, such requirements should be commensurate with the sensitivity of the information and context of the relationship.

Policies and Practices

41. Bill 64 creates and obligation to "establish and implement governance policies and practices regarding personal information that ensure the protection of such information" (s.3.2). It also requires that these policies be published on the organization's website, or if it does not have a website, make them available through other means.

42. CWTA is concerned that this obligation does not distinguish between policies and practices that are published on an organization's website as part of its transparency obligations, and internal privacy policies and procedures where often contain confidential information and trade secrets. Publishing such information could also assist malicious actors gain unauthorized access to customer data.

43. **Recommendation:** The requirement to publish governance policies and practices regarding personal information (s.3.2) should be deleted.

Privacy Impact Assessments

44. Under Bill 64 the proposed Section 3.3 creates an obligation to "conduct an assessment of the privacy-related factors of any information system project or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information." This is similar to the data protection impact assessment required under Article 35 of the GDPR. However, unlike the proposed Section 3.3 of the Act, Article 35 of the GDPR includes a threshold at which an impact assessment must be conducted. Such threshold is where "taking into account the nature, scope, context and purposes of the processing", the processing "is likely to result in a high risk to the rights and freedoms of the natural persons".

45. By requiring an impact assessment for all information systems projects or electronic service delivery projects involving personal information, Bill 64 fails to recognize that not all such projects involve significant risks to data subjects. Applying the same standard and requirement to all projects involving

personal information creates unnecessary burdens on Quebec-based businesses and increases the cost of doing business.

46. **Recommendation:** Privacy-impact assessments should only be a requirement for projects where there is a high risk of material harm to individual's whose personal information is being collected and processed.

Transition Period

47. The amendments to the Act proposed by Bill 64 will have significant impacts on the Quebec-based businesses. While Bill 64 proposes that its amendments will come into effect one year following the date of the bill's assent (and three years with respect to the provision on data portability rights), such time period is likely insufficient to permit businesses to assess the impact of such changes on their current policies and procedures, develop new policies and procedures, make necessary changes to their internal computer systems, amend contracts with third-party contractors and data processes, and train personnel. Such activities are time consuming and require significant resources. Additional time to make these changes is required.

48. **Recommendation:** The amendments made to the Act by Bill 64 should come into effect two years following the date of the bill's assent, except for the provision on data portability which, if enacted, should be postponed in accordance with the recommendation made in paragraph 34a above.

CWTA appreciates the opportunity to provide its comments in relation to Bill 64. The modernization of private sector privacy regulations is an import matter to all individuals and businesses in Quebec. We commend the Government of Quebec for consulting with stakeholders on this issue and recognizing the importance of balancing the legitimate and responsible use of data with the protection of individual privacy.

*** End of Document ***