Canadian Telecommunications Association | Association canadienne des télécommunications

November 7, 2023

Mr. Joël Lightbound
Chair
Standing Committee on Industry, Science and Technology (INDU)
Sixth Floor, 131 Queen Street
House of Commons
Ottawa, ON K1A 0A6

VIA Email: INDU@parl.gc.ca

Re: Committee study of Bill C-27, Digital Charter Implementation Act, 2022

Dear Chair,

On behalf of the Canadian Telecommunications Association, I am pleased to submit the enclosed recommendations regarding the INDU Committee's study of Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.*

For ease of reference, I also enclose a summary of our recommendations.

Sincerely,

Eric Smith
Senior Vice President
Canadian Telecommunications Association

CC: The Honourable François-Philippe Champagne
Minister of ISED
ministerofisi-ministredeisi@ised-isde.gc.ca

CC: Mark Schaan
Senior Assistant Deputy Minister, ISED
Mark.Schaan@ised-isde.gc.ca

CC: Samir Chhabra-
Director General, Marketplace Framework Policy Branch, ISED
Samir.Chhabra@ised-isde.gc.ca

IMPLEMENTING CANADA'S DIGITAL CHARTER TO PROTECT PRIVACY AND FOSTER INNOVATION

RECOMMENDATIONS TO THE STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY FROM THE CANADIAN TELECOMMUNICATIONS ASSOCIATION ON BILL C-27, *AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT, THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND THE ARTIFICIAL INTELLIGENCE AND DATA ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS*

A. INTRODUCTION

1. The Canadian Telecommunications Association appreciates the opportunity to provide its recommendations on Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* (Bill C-27 or the Act).

2. We represent companies that provide services and products across the wired and wireless communications sector in Canada. Our primary role is to advocate on behalf of the sector and to inform Canadians about the contributions that the telecommunications sector makes to Canada, including innovation, economic growth, social well-being, and sustainability. We also facilitate industry initiatives, such as enhancing accessibility, charitable giving, and consumer protection. The protection of personal information 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 privacy of customers and the security of their personal information.

3. We had the opportunity to submit comments on Bill C-27's predecessor, Bill C-11, *An Act to enact the Consumer Privacy Protection Act* (Bill C-11) and are pleased to note that many of its comments on the *Consumer Privacy Protection Act* (CPPA), as proposed by Bill C-11, were addressed in Bill C-27. CPPA under Bill C-27 provides strong protections for personal information while allowing for the responsible use of personal information for purposes that are in the public interest, such as facilitating economic growth and innovation, which are both fundamentally important to Canadians.

4. While we support the proposed legislation and consider it to be an important step forward to protecting the privacy interests of Canadians, we have a few targeted recommendations, based on our members' experience, to help CPPA achieve the objectives set forth in the Digital Charter. A summary of our recommendations is provided as a companion this document.

B. RECOMMENDATIONS RESPECTING COMING INTO FORCE

Provide a transition period of at least 24 months from Royal Assent before provisions of CPPA come into force.

5. Although organizations already have processes in place to comply with CPPA obligations that are transposed from PIPEDA, CPPA introduces significant changes to the Canadian privacy landscape and creates new enforcement mechanisms that can lead to large penalties for organizations failing to comply. The effort required for organizations to bring their business into compliance is substantial and will take time, especially for large and complex companies, such as telecom operators.

6. Organizations will require time to analyze the changes introduced by CPPA against their current practices and to establish and implement a compliance plan. Creating a compliance plan is a complicated legal and operational task. Organizations will only be able to dedicate significant resources to this task after the text of Bill C-27 is finalized and receives Royal Assent, as any changes made to the current draft of CPPA during the amendment process could easily alter the design of complex compliance plans and lead to more cost and delay.

7. Once compliance plans have been created, implementing them will also require significant organization time and resources. For large organizations in particular, preparing for compliance with CPPA will include, without limitation, some or all of the following activities:

    a. conducting an inventory of databases that contain personal information and analyzing how current practices of collection, use, disclosure, and destruction of such data must be altered;

    b. reviewing and negotiating amendments to applicable third party agreements;

    c. procuring and onboarding new technology solutions or updating existing IT systems (for example, to receive and respond to new right of disposal requests and for data inventory and classification);

    d. adapting consent management processes;

    e. developing and implementing new employee training; and

    f. updating customer-facing documentation and providing adequate notice of changes to privacy policies to customers.

8. These activities are particularly complex and resource-intensive for organizations that have legacy and multi-layered IT systems. IT resources are limited and changes to privacy-related IT systems must be budgeted for, scheduled and prioritized in relation to the many other IT requirements of the organization, including critical service-impacting IT systems. Organizations in highly regulated industries also must respond to concurrent regulatory requirements and changes which compete for resources and capital.

9. Organizations such as telecom operators also have periods during the year where there are moratoriums on changes to IT systems. For example, organizations that rely heavily on digital commerce during peak buying periods such as Christmas, Black Friday, and Back to School are likely to have such restrictions in place.

10. For these reasons, organizations require a workable transition period between the Royal Assent and CPPA's entry into force. At a minimum, a 24-month transition period is necessary. Such a transition period would be consistent with the transition periods between the adoption and coming into force of European General Data Protection Regulation (GDPR) and, for most of its provisions, Québec Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Québec Bill 64).

11. **Recommendation**: There should be a minimum general transition period of 24 months, following Royal Assent, before provisions of CPPA come into force.

Remove the private right of action (Section 107).

12. Our position on the private right of action is informed by the experience of the private right of action in Canada's Anti-Spam Law (CASL), where it has been suspended indefinitely. Initially, CASL's private right of action was suspended for 3 years. Yet even that transition period proved insufficient, and the Government has indefinitely suspended the coming into force of the private right of action *"in order to promote certainty for numerous stakeholders claiming to experience difficulties in interpreting several provisions of the Act while being exposed to litigation risk."*[1] The private right of action under CASL is still not in force.

13. CPPA is a much broader piece of legislation than CASL as it affects multiple facets of organizations' operations. CPPA raises even more significant interpretation challenges than CASL as it introduces many novel concepts, for example: legitimate interest exceptions, data mobility rights, right of disposal, rights regarding automated decision-making and new rules around sensitive information.

14. In addition, CPPA introduces other mechanisms for enforcement that expose organizations to broad order making, as well as significant administrative monetary penalties, namely: penalties of up to $10,000,000 or three per cent of the organization's global gross revenues and penal fines of $25,000,000 and five per cent of the organization's gross global revenues (in both cases, whichever is greater).

15. The risk of imposition of these measures, combined with the reputational damage that would result from a contravention of CPPA, stand as an extremely strong incentive for compliance. Accordingly, adding a private right of action to CPPA, especially before understanding how the legislation is working to achieve its goals, is premature and unnecessary. It could also incent the emergence of a speculative class action business.

16. Alternatively, if the private right of action is not removed from CPPA, it should be suspended indefinitely, or at minimum until a sufficient period has passed to enable an evidence-based

[1] See *Order in Council Repealing the Coming into Force of the Private Right of Action of Canada Anti-Spam Law*.

review of the new law's impact. Such a review should not be conducted until at least five years from the date that CPPA comes into force. Only if such a review demonstrates that a private right of action is necessary to ensure compliance with CPPA should the suspension of that right be lifted. Suspending the Private Right of Action indefinitely is consistent with the Government's approach in CASL.

17. In any event, if a private right of action is retained in CPPA, it should be limited to gross and intentional fault, similar to the approach taken under Québec Bill 64.

18. **Recommendation:** The private right of action in Section 107 of CPPA should be removed. Failing removal, it should be suspended indefinitely or until a sufficient period (no less than five years) has passed to enable the Government to assess the need for a private right of action given the other strong enforcement mechanisms contained in CPPA. Any private right of action should be limited to gross and intentional fault.

Defer the entry into force of the data mobility rights (Section 72) to three years after the applicable regulations are enacted.

19. As further discussed in paragraphs 25 to 29, data mobility rights should not be applicable to industries, such as telecommunications, that are already subject to industry-specific regulatory oversight which can better assess the merits of applying such obligations to the applicable industry.

20. For industry sectors where data mobility rights will apply, organizations will need additional time to develop interoperability standards and to implement this new right. Taking into account the unique challenges of implementing the right to mobility, Québec Bill 64 specifically excludes, in section 175, the right to mobility from its general coming into force. Instead, the entry into force of the right to mobility is set to "three years after the date of assent to [Bill 64]".

21. **Recommendation:** For industry sectors where data mobility rights will be applicable, CPPA should defer the entry into force of the data mobility provisions to three years after the applicable regulations are enacted.

C. ENSURING CLEAR AND RESPONSIVE MARKETPLACE FRAMEWORKS

Amend the definition of "anonymize" to incorporate a standard of reasonable foreseeability in the anonymization threshold.

22. We welcome the changes that have been made from Bill C-11 to clearly state that CPPA does not apply in respect of personal information that has been anonymized (subsection 6(5)). CPPA defines "anonymize" as follows: "to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means" (subsection 2(1)).

23. Unlike Québec Bill 64, CPPA definition does not include a "reasonably foreseeable" standard. The absolute nature of the definition of "anonymize" could make anonymization an

unrealistic standard to meet for organizations and place Canadian organization at a disadvantage with respect to their competitiveness and ability to innovate, especially in the context of the development and implementation of AI/ML solutions.

24. **Recommendation**: The definition of "anonymize" should be amended as follows:

> ***anonymize*** means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that it is, at all times, reasonably foreseeable in the circumstances that no individual can be identified from the information, whether directly or indirectly, by any means.

Define the organizations that are not subject to the data mobility rights (Section 72), such as industries that are already subject to industry-specific regulatory oversight.

25. Data mobility rights should not be applicable to industries, such as telecommunications, that are already subject to industry-specific regulatory oversight which can better assess the merits of applying such obligations to the applicable industry.

26. Referring the details to regulations, Section 72 of CPPA proposes a "right to mobility" with little more definition than stating that it applies to "*the personal information that it has collected from the individual*". The right entails that, "*on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations*."

27. While we assume there will be an opportunity to comment on data mobility regulations during a future process, developing interoperable data systems to give effect to the right to mobility would be complex, time consuming and costly, while offering little if any added-value to consumers. will be extremely challenging.

28. The mobile wireless industry's experience with creating and operationalizing standards and procedures for wireless number portability is a real-world example of how difficult and time consuming this process can be. In the case of a broader mobility right such as that proposed by CPPA, the challenge is even more daunting. Each service provider offers a variety of products and services, often different from those of their competitors, thus generating varying types of personal information. Developing and installing the mechanisms that will allow the transfer of uncoordinated, non-standardized information, and that will address the specific security risks of transfer would be complex and take significant time and resources.

29. To demand such effort from an industry such as the telecommunications industry, there must be a corresponding and proportionate benefit to consumers that would justify such an obligation. It is not clear, however, what benefits a subscriber would receive from the right to data mobility.

30. Data mobility is typically used to increase competition and remove barriers to switching from one vendor's products and services to those of another. As mentioned, there are already regulations in place that allow an individual to easily port their mobile phone number for use with another service provider's service. The porting process is seamless and millions of Canadians easily switch service providers every year.

31. It is also unclear what personal information a service provider possesses that an individual would want or need to be transferred to the new service provider that the individual did not already possess themselves.

32. It is telling that the Canadian Radio-television and Telecommunications Commission (CRTC), which routinely examines the activities of the telecommunications industry, has not identified a need for a data mobility right either to enhance competition or to protect the privacy of telecommunications services customers, which is one of the express objections of the Canadian telecommunications policy under the *Telecommunications Act*[2]. Accordingly, if a telecommunications approach to data mobility is merited, it should be left to the CRTC to make such a determination, rather than apply a law of general application to the telecommunications industry.

33. While we do not think that the data mobility right should apply to telecommunication service providers, if such a right is implemented, in consideration of the amount of time and resources required to implement data mobility, an appropriate transition period must be in place.

34. As referenced in paragraph 20 of this submission, Québec Bill 64 specifically excludes the right to mobility from its general coming into force. Instead, the entry into force of the right to mobility is set to "three years after the date of assent to [Québec Bill 64]".

35. **Recommendation:** The data mobility provisions should not apply to industries for which there is already regulatory oversight that can assess the merits of introducing data mobility rights for customers of the industry in question (e.g. the CRTC, which regulates telecommunications pursuant to the policy objectives set out in the *Telecommunications Act* and which includes an express reference to the privacy of person). For industry sectors where data mobility rights are merited, to allow for successful implementation, CPPA should defer the entry into force of the data mobility provisions until three years after the applicable regulations are enacted.

Reconsider the approach to children's privacy by focusing on organizations that have actual knowledge that they are collecting personal information of minors and by not excluding personal information of minors from exceptions to the right of disposal.

36. Though we appreciate the Government's desire to provide stronger protections for minors, we have concerns with the manner in which CPPA attempts to implement these protections.

[2] S.9(1) of the Act is "to contribute to the protection of privacy of persons."

37. Section 2(2) of CPPA provides that personal information of minors is sensitive information and Section 15(5) specifies that sensitivity is a factor to determine the appropriate form of consent. In combination, these provisions could be interpreted as requiring express consent whenever an organization is dealing with personal information of minors.

38. A blanket requirement to obtain express consent to handle minors' information would result in significant operational challenges for organizations that do not specifically target minors and have no actual knowledge that they are processing personal information of minors. This is particularly true for telecom providers.

39. Residential internet access services are typically sold on a per household basis, while mobile wireless services are often purchased by a single account holder who acquires multiple lines so that family members can use their own mobile device (often referred to as a family plan). In both such cases, the telecom provider does not know, except for the account holder, the identity or age of the persons using the internet service or mobile services. Requiring telecom providers to verify the age of each user who connects a device to the household's internet access services (whether a resident or visitor) or wireless services is impractical.

40. A more effective and practical means to achieving its goals would be to create enhanced consent obligations for organizations that offer services that are specially directed at minors or that have actual knowledge that an individual is a minor, similar to the approach taken by the California *Consumer Privacy Protection Act* (CCPA). Such organizations should be required to adopt a contextual approach to minors' consent, as the OPC outlined in the *Guidelines for obtaining meaningful consent*. [3]

41. In addition to challenges regarding consent, another issue arises with respect to minors in the context of the right of disposal. Section 55(2) of CPPA sets out exceptions to the right of disposal, including: (i) where the information is not in relation to a minor and the disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question (at subparagraph (d)); and (ii) the information is not in relation to a minor and it is scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period for which the information will be retained (at subparagraph (f)).

42. The exclusion of personal information of minors from these two provisions is not appropriate because the fact that the individual is a minor does not lessen the organization's need to retain the data to provide the services (in the case of subsection (d)) or for legitimate legal and business needs (in the case of subsection (f)).

43. **Recommendation:** Organizations should only be required to treat personal information of a minor as *de facto* sensitive information when they have actual knowledge that the applicable individual is a minor or if the personal information was collected through a service that

[3] OPC, *Guidelines for obtaining meaningful consent*

specifically targets minors. The exceptions to the right of disposal at subsections 55(2)(d) and (f) should not exclude personal information in relation to a minor.

Extend the "business activities" and "legitimate interest" exceptions to the disclosure of personal information.

44. CPPA allows organizations to collect and use personal information without the individual's knowledge and consent for a "business activity" (subsections 18(1) and (2)) or when it has a "legitimate interest" that outweighs any potential adverse effect on the individual (subsection 18(3)). These exceptions should also apply to an organization's disclosure of personal information.

45. Organizations may need to disclose personal information to another organization for one of the business activities listed in CPPA, which include, for example, activities that are necessary to provide the service or product the individual has requested. For example, organizations may need to disclose personal information to a payment processor to provide a product or service that the individual has requested from the organization (these payment providers are generally not "service providers" and would therefore not be captured by the consent exception set out in section 19). Also, it could be in the legitimate interest of an organization to voluntary disclose personal information to a government institution to participate in a governmental program.

46. It is instructive to note that under the GDPR, all legal bases for consent– including legitimate interest – apply equally to all categories of processing, including the disclosure of personal data. Like the GDPR, CPPA already provides for sufficient guardrails to ensure that individuals' privacy rights are respected should an organization rely on the "business activities" and "legitimate interest" exceptions to disclose personal information. More specifically, section 18 requires organizations to consider the reasonable expectation of the individual and exclude situations where personal information is processed for the purpose of influencing the individual's behaviour or decisions (and, in the case of the "legitimate interest" exception, organization must undertake and record a legitimate interest assessment).

47. These exceptions represent a step in the right direction to address consent fatigue and keep consent meaningful. Expanding the application of these exceptions to the disclosure of personal information would further achieve these purposes.

48. **Recommendation:** Subsections 18(1) and 18(3) should be amended as follows:

> **Business activities**
>
> 18 (1) An organization may collect, ~~or~~ use or disclose an individual's personal information without their knowledge or consent if the collection, ~~or~~ use or disclosure is made for the purpose of a business activity described in subsection (2) and
>
> (a) a reasonable person would expect the collection or use for such an activity; and
>
> (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

(…)

Legitimate interest

(3) An organization may collect, ~~or~~ use or disclose an individual's personal information without their knowledge or consent if the collection, ~~or~~ use or disclosure is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and

(a) a reasonable person would expect the collection or use for such an activity; and

(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

Allow the "legitimate interest" consent exception to coexist with implied consent.

49. Subsection 15(5) of CPPA acknowledges that under some circumstances relying on implied consent may be appropriate "taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used, or disclosed". In some cases, the business activities and legitimate interest activities described in Section 18 of CPPA would also lend themselves well to relying on implied consent (i.e., because the information is not sensitive, the activity falls within the reasonable expectations of the individual and the organization is well positioned to provide notice of the purpose of the processing of information to the individual).

50. However, subsection 15(6) of CPPA provides that it is not appropriate to rely on an individual's implied consent if their personal information is collected or used for a "business activity" (as defined in subsection 18(2)) or for an activity which is in the legitimate interest of the organization (as set out in subsection 18(3)). Furthermore, subsections 18(3) and 18(4) require organisations to conduct and record assessments of legitimate interest activites.

51. Requiring organizations to systematically conduct and record a legitimate interest assessment in situations where the conditions for relying on implied consent would otherwise be satisfied will result in an unnecessary burden on organizations that is not outweighed by a corresponding benefit for the protection of personal information. CPPA should allow organizations to choose between implied consent and legitimate interest when the circumstances allow for the use of either exception.

52. **Recommendation:** Subsection 15(6) should be amended to read as follows:

Business activities

(6) It is not appropriate to rely on an individual's implied consent if their personal information is collected or used for an activity described in subsection 18(2) ~~or (3)~~.

Clarify that "influencing the individual's behaviour or decision", as used in Section 18, is not intended to prohibit activities, such as direct marketing, that a reasonable person would expect in the applicable circumstances.

53. Subsection 18(3) provides that an organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the

purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and: (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

54. We are concerned that the exclusion of activities that are for the purposes of influencing the individual's behaviour or decisions is too broad as it could exclude regular marketing activities, such as providing direct offers to customers. We believe this is not the intended consequence of this exclusion, and we note that the GDPR's Recital 47 explicitly states that direct marketing may be regarded as carried out for a legitimate interest.

55. CPPA should specify that the words "influencing the behaviour and decisions" are not meant to capture regular marketing activities and are directed at behavioural advertising or political activities, e.g. tracking consumers' online activities across non-affiliated sites and platforms, over time, in order to deliver advertisements targeted to their inferred interests.

56. **Recommendation:** Amend subsection 18(3) as follows:

> (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions in ways that would not be considered by a reasonable person to be appropriate in the circumstances.

D. CONCLUSION

57. PIPEDA has proven its effectiveness and value for Canada. Bill C-27 must update PIPEDA without losing PIPEDA's strength, including its flexibility and adaptability to context, which allow privacy risks to be addressed as they evolve, while providing clarity, fairness in enforcement and avoiding undue burden and cost to organizations. These strengths are aligned with the goals set out in the Digital Charter.

58. The recommendations set out herein will help CPPA achieve the objectives set forth in the Digital Charter.

SUMMARY OF RECOMMENDATIONS

TO THE STANDING COMMITTEE ON INDUSTRY AND TECHNOLOGY FROM THE CANADIAN TELECOMMUNICATIONS ASSOCIATION ON BILL C-27, *AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT, THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND THE ARTIFICIAL INTELLIGENCE AND DATA ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS*

Reference is made to the paragraphs in the accompanying submission where the explanation and specific details of the recommendations listed below are made.

1. There should be a minimum general transition period of 24 months, following Royal Assent, before provisions of CPPA come into force. (¶ 5-11)

2. The private right of action in Section 107 of CPPA should be removed. Failing removal, it should be suspended indefinitely or until a sufficient period (no less than five years) has passed to enable the Government to assess the need for a private right of action given the other significant new enforcement mechanisms contained in CPPA. Any private right of action should be limited to gross and intentional fault. (¶ 12-18)

3. For industry sectors where data mobility rights are applicable, CPPA should defer the entry into force of the data mobility provisions until three years after the applicable regulations are enacted. (¶ 19-21)

4. Amend the definition of “anonymize” to incorporate a standard of reasonable foreseeability in the anonymization threshold. (¶ 22-24)

5. The data mobility provisions should not apply to industries for which there is already regulatory oversight that can assess the merits of introducing data mobility rights for customers of the industry in question (e.g. the CRTC). For industry sectors where data mobility rights are merited, to allow for successful implementation, CPPA should defer the entry into force of the data mobility provisions to three years after the applicable regulations are enacted. (¶ 25-35)

6. Organizations should only be required to treat personal information of a minor as *de facto* sensitive information when they have actual knowledge that the applicable individual is a minor or if the personal information was collected through a service that specifically targets minors. The exceptions to the right of disposal at subsections 55(2)(d) and (f) should not exclude personal information in relation to a minor. (¶ 36-43)

7. The “business activities” and “legitimate interest” exceptions in section 18 should be extended to apply to the disclosure of personal information. (¶ 44-48)

8. Subsection 15(6) should be amended to allow the “legitimate interest” consent exception and implied consent to coexist. (¶ 49-52)

9. Amend subsection 18(3) to allow organizations to rely on the “legitimate interest” exceptions when personal information is used for the purpose of influencing the individual’s behaviour

or decisions in ways that would be considered by a reasonable person to be appropriate in the circumstances (e.g. direct marketing). (¶ 53-56)

[End of Document]