June 10, 2020

The Honorable François-Philippe Champagne
Minister of Innovation, Science and Industry
235 Queen Street
Ottawa, Ontario K1A 0H5

Sent via email: Francois-Phillipe.Champagne@parl.gc.ca

Dear Minister Champagne:

RE: Recommendations from the Canadian Wireless Telecommunications Association on Bill C-11, *An Act to Enact the Digital Charter 2020*

Please find enclosed our comments regarding the above referenced matter. Please do not hesitate to contact me if you have any questions or wish to discuss further.

Best Regards,

Robert Ghiz
President & CEO

CC: Mark Schaan, Associate Assistant Deputy Minister
Jennifer Miller, Director General
Charles Taillefer, Director
David Hurl, Policy Advisor
Brook Simpson, Director ,Parliamentary Affairs

T 613 233 4888 F 613 233 2032 www.cwta.ca
300-80 rue Elgin Street Ottawa, ON K1P 6R2

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

RECOMMENDATIONS FROM THE CANADIAN WIRELESS TELECOMMUNICATIONS ASSOCIATION ON BILL C-11, *AN ACT TO ENACT THE DIGITAL CHARTER 2020*

A. INTRODUCTION

1. The Canadian Wireless Telecommunications Association (CWTA) appreciates the opportunity to provide its recommendations on Bill C-11, *An Act to Enact the Digital Charter 2020* (Bill C-11 or the Act). 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.

2. 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 right to privacy of customers and the security of their personal information.

3. While *The Personal Information Protection and Electronic Documents Act* (PIPEDA) has served Canadians well for the last 20 years as a made-in-Canada approach to privacy, we acknowledge that it is time to update Canada's privacy framework to take into account changes in technology and new ways of using data.

4. In modernizing Canada's privacy framework, we must recognize that the world is undergoing a digital and data-driven revolution. The innovative combination of data and technology will enable Canadians to be more productive, generate economic growth, and deliver a higher quality of life. These outcomes, which are critical to the Canadian economy as recovers from the COVID-19 pandemic, require the responsible use of data and maintaining the protection of privacy.

5. These objectives are reflected in the following three key goals set forth in Part 3 of *Canada's Digital Charter in Action: A Plan by Canadians* ("Digital Charter"), which is appropriately entitled "Privacy and Trust: Making Canada a Leader in the Digital Age":

    - Clear and Responsive Marketplace Frameworks
    - Putting Data to Use for Canadians

- Security

6. It is through the framework of Part 3 of the Digital Charter and the overarching objective of "making Canada a leader in the digital age" that we analyze and make our recommendations about how to improve Bill C-11.

B. CHANGES TO BILL C-11 ARE NECESSARY TO PROTECT PRIVACY WHILE ENSURING A CLEAR AND RESPONSIVE MARKETPLACE FRAMEWORK

7. It is evident that a great deal of thought and effort was put into drafting Bill C-11. With the Digital Charter as its guide, the Act requires greater transparency from organizations regarding their collection, use and disclosure of personal information, grants individuals additional rights, and implements a new system of enforcement.

8. At the same time, the Digital Charter recognizes the need for Canada to embrace digital and data-driven technologies that will fuel economic growth, create high-value jobs, and lead to a better quality of life for all. In the commercial context, Bill C-11 acknowledges that where individuals provide personal information to an organization in exchange for goods or services, it is reasonable to allow the organization to use such information for normal business activities, and for such other reasons consented to by the individual.

9. However, despite the good faith attempt to strike an appropriate balance between the individual's right to control the use of his or her personal information and the reasonable collection and use of personal information by organizations, Bill C-11 requires some important amendments.

10. A summary of our recommendations can be found in Appendix A. They include the critical need to amend certain definitions, such as the term "de-identify" which, as currently defined, would make Canada an international outlier by subjecting non-personal information to regulation under the Act. We also recommend that certain provisions, such as sections 12 and 15 of the proposed *Consumer Privacy Protection Act* (CPPA) be made less prescriptive so as to maintain the principle-based flexibility that is one of the great strengths of PIPEDA. This flexibility allows for regulations to address privacy risks as they evolve over time and as new technologies and ways of using data are developed. Recommendations are also made that would ensure consistency between provisions, as well as changes that are necessary to ensure fairness in the enforcement of the Act.

11. Finally, and most importantly, it is critical that organizations are provided appropriate time to implement changes to their business necessitated by the Act.

Bill C-11 does not merely update existing private sector privacy legislation; it replaces existing legislation with an entirely new set of complex statutes and requirements. Implementing the changes to IT systems and business processes that will be required to comply with the Act will be costly and take considerable time for organizations of all sizes. As such, it is crucial that there be a transition period of no less than 24 months from royal assent before the CPPA comes into force. The applicability and transition periods regarding data mobility rights and the removal or suspension of the private right of action are also discussed below.

C. RECOMMENDATIONS RESPECTING COMING INTO FORCE

Provide a Transition Period of 24 Months from Royal Assent Before the *Consumer Privacy Protection Act* ("CPPA") Comes Into Force, to Enable Businesses to Effectively and Efficiently Implement New Practice

12. Before setting out our specific recommendations with respect to the provisions of Bill C-11, it is critical to emphasize the importance of affording organizations a workable and appropriate transition period (specifically, no less than 24 months following Royal Assent) to adapt and implement the ultimate requirements of Bill C-11 when it is passed by Parliament. In support of this proposal, we note that a 24-month ramp-up period preceded the coming into force of the GDPR. There is no justification for a shorter period to apply to the coming into force of Canada's new privacy law.

13. Although companies have begun to engage in detailed considerations of their current practices and potential changes that may be required pursuant to the draft language of Bill C-11, they cannot initiate implementation of changes in the absence of legal certainty regarding the final version of the bill.

14. The fact that possible extensions of Parliament's consideration of Bill C-11 may occur (due to Parliamentary and Committee schedules) is not reasonable justification for a coming into force period of less than 24 months from the date on which Bill C-11 receives Royal Assent. Organizations cannot afford to expend resources on the design of complex compliance approaches in response to draft legislative provisions that may or may not ultimately become law. Ensuring that companies can efficiently allocate their resources is even more important as we enter into a post-pandemic economy in which the national interest is focused on the strongest and swiftest possible economic recovery.

15. The work required for organizations to bring their operations and procedures into compliance with the obligations of the Act must not be underestimated. 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 in many cases renegotiated.

16. 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 Act. These IT changes will be complex, significant and costly. They also do 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. Further, organizations plan and forecast IT cycles many quarters in advance. Other IT commitments will be underway or scheduled, and human resources allocated to such commitments, when the Act is passed. These projects cannot simply be abandoned and resources shifted to the significant IT changes necessitated by the Act.

17. It follows that proper implementation of the Act calls for a minimum general 24-month transition period, following the Bill's receiving Royal Assent, before entry into force. We note that the first draft of the EU's General Data Protection Regulation (GDPR) was published by the European Commission in January 2012, was adopted by the European Parliament in April 2016, and was subject to a 24-month grace period with the provisions of the GDPR not being enforceable until May 2018.

18. Despite this timeline, surveys of organizations taken after the GDPR enforcement date show that the challenges of compliance were greater than many anticipated. For example, a September 2019 survey by consultancy firm Capgemini revealed that just 28% of those organizations surveyed believed they were fully GDPR compliant.[1] The most commonly cited obstacles to becoming compliant were legacy IT systems, the complexity of the GDPR, and prohibitive financial costs.

19. The need for a sufficient transition period is all the more necessary since, unlike other jurisdictions that have reformed their privacy legislation, the Act will be fundamentally transforming Canada's privacy regime from an ombudsman model to an enforcement model, with order-making powers and new administrative penalties. Moreover, this significant effort will unfold without the benefit of interpretation of the new requirements and the risk of very significant financial penalties for non-compliance.

[1] https://www.zdnet.com/article/gdpr-only-one-in-three-businesses-are-compliant-heres-what-is-holding-them-back/

20. **Recommendation**: There should be a minimum general transition period of 24 months, following Royal Assent, before Bill C-11's entry into force.

Exception and General Deferral of Coming into Force of Data Mobility Provisions (Section 72) To Three Years After Applicable Regulations are Adapted

21. Data mobility rights 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 the CPPA, the CPPA should defer the entry into force of the data mobility provisions to three years after the applicable data mobility regulations are enacted.

22. Referring the details to regulations, Section 72 of the 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*."

23. 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 will be extremely challenging. 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.

24. 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, will be arduous and take time.

25. 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 wireless services subscriber would receive from the right to data mobility.

26. 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.

27. It is also unclear what personal information a wireless 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. It is telling that the Canadian Radio-television and Telecommunications Commission (CRTC), which routinely examines the competitiveness of the telecommunications industry, has not identified a need for a data mobility right in order to enhance competition. 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.

28. While we do not think that the data mobility right should apply to mobile wireless service providers, if such a right is implemented it must be narrowly focused and apply only to specific types of personal information that are considered necessary to enable an individual to switch service providers. In addition, considering the amount of time and resources required to implement data mobility, an appropriate transition period must be in place.

29. Taking into account the unique challenges of implementing the right to mobility, Québec Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64), specifically excludes, at section 165, 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]".

30. **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). For industry sectors where data mobility rights are merited, in order to allow for successful implementation, the CPPA should defer the entry into force of the data mobility provisions to three years after the applicable regulations are enacted.

Remove or Suspend the Private Right of Action (Section 106)

31. The proposed private right of action at Section 106 of the CPPA should be suspended indefinitely, or at minimum until a sufficient period of time has passed to enable a data-based review of the new law's impact. Such a review should not be conducted until at least five years from the date that the CPPA comes into

force. Only if such a review demonstrates that a private right of action is necessary to ensure compliance with the CPPA should the suspension of that right be lifted.

32. CWTA's position on the private right of action proposed in Bill C-11 is informed by the experience of the private right of action in Canada's Anti-Spam Law (CASL), where it has been suspended indefinitely notwithstanding that the law came into force in 2014. Initially, CASL's private right of action (found at Section 47 of that statue) was suspended for 3 years, to July 1, 2017. Yet even that transition period proved insufficient. In June 2017, the *Order in Council Repealing the Coming into Force of the Private Right of Action of Canada Anti-Spam Law* was adopted to indefinitely delay the coming into force of the PRA *"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."* The PRA under CASL is still not in force.

33. The grounds for suspending the private right of action in the CPPA are even stronger than those that led to its suspension in CASL. The CPPA proposes to introduce legal reforms far broader than CASL, which will necessitate changes to data system and business practices that are complex and will require integration deep within the operations of Canadian businesses.

34. Moreover, not only is the proposed new law far-reaching in its operational impacts on business, it is rife with many unanswered questions regarding its interpretation. Many of these challenges are set out below in significant detail.

35. Finally, the CPPA introduces other mechanisms for enforcement that expose organizations to broad order making, as well as administrative monetary penalties that are the toughest in the G7. The risk of imposition of these measures, combined with the reputational damage that would result from a contravention of the CPPA, stand as an extremely strong incentive for compliance. Accordingly, adding a private right of action to the CPPA, especially before understanding how the legislation is working to achieve its goals, would be premature and unnecessary. It could also incent the emergence of a speculative class action business.

36. **Recommendation:** Given the significant mechanisms for enforcement that exist in the Act, and the real risk of encouraging speculative class actions, the private right of action should be removed from the Act. If it is not removed, the proposed private right of action in the CPPA should, as shown with the experience of CASL, be suspended indefinitely or, at minimum, should not be brought into force until a period of at least five years following Royal Assent. Prior to this period, the impact

of the CPPA can be assessed and data gathered on the value, if any, of introducing a private right of action.

D. ENSURING CLEAR AND RESPONSIVE MARKETPLACE FRAMEWORKS

37. The Digital Charter states that, while PIPEDA requires modernization and streamlining, "the Government must ensure that updates both support innovation and protect Canadians." To this end, the Digital Charter notes that rules must be clear in order to determine their applicability and to implement them. Further, while appropriate enforcement measures are necessary, they must "include ease of understanding and compliance" and "a commitment to due process in order to not add undue burden and cost to firms."

38. The Digital Charter also acknowledges that Canada's privacy framework must not be considered in isolation, and that to achieve the goal of fostering legitimate and responsible use of data, it must take into consideration the privacy frameworks of Canada's trading partners. This does not mean that Canada's privacy regulations must be identical to those of our international peers, but they 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 in Canada.

39. Finally, the Digital Charter stipulates that any new privacy framework must be flexible and responsive to the accelerated pace of technological innovation.

40. To be consistent with these principles and, most importantly, to be successful, Canada's new privacy framework must articulate clear requirements, grounded in socio-economic and operational reality, and provide the flexibility to address privacy risks as they evolve through technological developments and new business models. In reforming Canada's privacy legislation, we must preserve the balance that has made PIPEDA one of the most effective privacy protection laws in the world,[2] while concurrently facilitating economic growth and innovation; both of which are fundamentally important to Canadians.

Analysis and Recommendations

(a) Definitions (section 2)

41. Achieving a clear marketplace framework starts with clear definitions. The following definitions require modification to meet that goal.

[2] Notably, Canada, under PIPEDA, has been one of only twelve countries recognized by the European Commission as having a private sector privacy law equivalent to that of Europe.

"<u>Automated decision system</u>"

42. "Automated decision system" is defined in Bill C-11 as "technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets." (section 2)

43. As the above non-exhaustive list of types of automated decision systems illustrates, the breadth of current and future types of such systems is wide. Not all systems are the same, and the degree in which they aid human decision-making will vary. The focus of legislation should be on those systems that could materially impact human decision-making.

44. As currently defined, and as used in Sections 62 and 63 of the CPPA, organizations would be required to describe and, if requested, explain the use of all systems, including those that have minimal impact on the decision-making process. This could include innocuous systems such as those that automate routine tasks, like routing phone calls to the customer service centre that has the lowest call volume or that has the required expertise to assist a customer with a specific issue. Accordingly, limiting the definition of automated decision systems to include only those systems that materially assist decision-making would lessen this burden, without negatively impacting the rights of individuals.

45. **<u>Recommendation</u>: Revise the definition of "automated decision system" as follows:**

"automated decision system" means any technology that <u>materially</u> assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets."

"<u>De-identify</u>"

(i) The Definition of "De-Identify" Is out of step with International Privacy Norms

46. The definition of "de-identify" is one of the most concerning aspects of the proposed CPPA and requires amendment to avoid putting Canadian companies at a serious disadvantage with respect to their competitiveness and ability to innovate.

47. Bill C-11 defines "de-identify" as follows:

> "*to modify personal information – or create information from personal information – by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify the individual*."

48. As defined in Bill C-11, to de-identify refers to the act of turning personal information into non-personal information. Logic dictates that, once depersonalized, such information would fall outside of the scope of the CPPA. Indeed, that is how Canada's trading partners treat information that, in the proposed CPPA vernacular, has been de-identified.

49. The European Union's General Data Protection Regulation (GDPR) establishes three categories of data and information based on the risk of harm to the individual that would occur if such information were illegally accessed or processed.

a) "Personal data" relates to an identifiable individual and receives the highest protection in view of the harm that may result from a breach or unlawful processing;

b) "Pseudonymized data" results from the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[3] Pseudonymized data can be more freely processed than personal data because the risk of harm to an individual is significantly lowered; and

[3] GDPR Article 4

c) “Anonymous information” is “information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”[4] The risk of harm is considered so low and the use of such information so critical for all types of research and development, that the GDPR expressly excludes it from its scope.

50. Similarly, the California Consumer Privacy Act (CCPA) uses the term “de-identified” to mean “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer”.[5] Like the GDPR, the CCPA excludes de-identified information, which is the CCPA equivalent to the GDPR’s anonymous information, from its scope.[6]

51. Under current Canadian private sector privacy regulations, anonymized information is regarded in the same way as erased or destroyed information and, therefore, falls outside the scope of PIPEDA.[7]

52. While Canada’s trading partners and current Canadian law exclude non-personal information from the scope of their privacy laws, the proposed definition of “de-identify” and its use within the CPPA, would limit the ability of an organization to transform personal information into non-personal information, and to use or disclose such non-personal for purposes other than the limited circumstances set out in the Act. In so doing, the proposed definition of “de-identify” would put Canada out of step with the privacy law of its major trading partners.

53. The disadvantage for Canadian organizations in relation to competitiveness and innovation cannot be overstated. In conjunction with restrictions on use and disclosure, the definition of “de-identify” cuts off organizations governed by the CPPA from access to information available to organizations governed by the laws of some of Canada’s most important trading partners. These other organizations will be able to use this information for innovative purposes, gain important insights, and foster economic growth, while organizations governed by the CPPA will not. Moreover, such organizations could, as a result of the definitions and provisions with respect to de-identified information, decide not to conduct operations in, or invest in, Canada.

[4] GDPR Recital 26

[5] CCPA s. 1798.140 (h)

[6] Ibid s. 1798.146 (4) (A)

[7] clause 4.5.3 of Schedule 1

54. In addition, adopting a definition of “de-identify” that maintains non-personal information within the scope of the CPPA, and restricts its use, creates significant hurdles in the ability to use service providers outside of Canada. Many service providers require, as a contractual term, the ability to use “de-personalized” information. Canadian organizations could no longer meet their contractual terms and, in most cases, would be unable to renegotiate those terms, finding themselves in an untenable situation.

55. The effect of bringing “de-identified” information within the scope of CPPA is to make data that has been effectively rendered non-personal subject to rigid consent requirements that will often be impractical, if not impossible, to fulfill. In the rest of the world, the use of such information for beneficial and innovative purposes would be unfettered by such restrictions.

(ii) The Definition and Governing Provisions Respecting “De-Identified” Information Creates a Logical Paradox

56. The definition and governing provisions of “de-identified” information also directly contradict the provisions that define the scope of the proposed CPPA. Section 5 describes the purpose of the CPPA as to establish “*rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances*.” (Our emphasis).

57. Section 6 states its scope of application as “*in respect of personal information*”. Section 2 maintains the definition of “*personal information*” under PIPEDA as “*information about an identifiable individual*.” Bringing de-identified information within the scope of the CPPA is therefore a contradiction of its own terms.

58. In addition, the proposed regulation of de-identified information in Canada stands in contradiction with Canadian courts’ definition of personal information and of the right to privacy.

59. The Federal Court of Canada in *Gordon v. Canada (Health), 2008 FC 258* defines personal information under the federal *Privacy Act,* which uses the same test as PIPEDA, and now the proposed CPPA, to define “*personal information*”. The Court states that information is “*personal*” where it creates “*a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information”.* It is therefore established in Canadian law that where there in not “*a serious possibility that an individual be identified*”, there is no personal information.

60. If there is no “serious possibility” of an individual being identified through such information, then it is unclear why there would be a need to regulate the use of such information. In the Supreme Court of Canada decision, *R. v. Duarte*, [1990] 1 SCR 30, the Court defines the right to privacy as “*the right of the individual to determine when, how, and to what extent he or she will release personal information*” (Our emphasis).

61. It is clear that the right to privacy in Canada attaches only to information from which there is a serious possibility that an individual could be identified. The definition of “de-identified” information, and its use in related provisions of the proposed CPPA, is in direct contradiction of Canadian privacy law. It obstructs innovation in Canada without furthering any privacy rights.

(iii) Managing the Risk of Re-identification

62. We understand there may be concern about the risk of re-identification, given the amount of personal data on the internet and unprecedented data mining capacity. The test, however, even for “*anonymous information*”, has never been the complete removal of any risk of re-identification. The definition of personal information in Canadian law, as mentioned above, limits such information to that which creates a “*serious possibility*” of identification.

63. Moreover, the proposed CPPA includes additional safeguards and penalties that help mitigate any risk of re-identification. These include:

    a) proposed section 74 requires that “an organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information”;

    b) proposed section 75 provides that “an organization must not use de-identified information alone or in combination with other information to identify an individual”; and

    c) proposed section 125 criminalizes the effort to re-identify de-identified information in violation of section 75. It is an indictable offence subject to a fine of up to $25,000 and five (5) percent of the organization’s gross global revenue, or an offence punishable on summary conviction and liable for a fine of up to $20 million or four (4) percent of gross global revenue.

64. **Recommendation:** The CPPA should distinguish between personal information from which identifiers have been removed, but that could, with some diligence and

the use of other information, be used to identify the individual, versus information from which there is no serious possibility that an individual could be identified, whether alone or in combination with other available information. The former category would still be considered personal information and subject to the CPPA, but the CPPA should expressly state that it does not apply to the latter category of non-personal information. While there are a variety of ways to accomplish this objective, we suggest the following two steps:

a) replace the current proposed definition of "de-identify" with the following:

"de-identify" means to remove identifiers from personal information so that the information no longer allows the person concerned to be directly identified" ***(dépersonnaliser)***

b) expressly define what is *not* considered personal information and include a provision in the CPPA that expressly excludes such information from the scope of the CPPA. A suggested definition is as follows:

"non-personal information" means personal information that has been modified — or created from personal information — by using technical or other processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual." (renseignement non-personnel)

65. The above recommended amendments will require additional changes to the CPPA to reflect the difference between de-identified information and non-personal information. These additional changes are referenced in the "Putting data to use for Canadians" section below.

(b) Appropriate purposes (Section 12)

66. Subsection 12(1) of the proposed CPPA restricts the collection, use or disclosure of personal information to purposes "that a reasonable person would consider appropriate in the circumstances." The reasonableness standard recognizes the need for a balance between individual and organizational interests that is reflected in Section 5 of the proposed CPPA.

67. Rather than preserve the flexibility that the reasonableness standard affords, however, subsection 12(2) introduces a rigid set of factors that must be considered for the handling of all personal information. Most problematic are undefined

notions of the "*effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs", " whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits", and "whether the individual's loss of privacy is proportionate to the benefits in light of any measures [..] to mitigate the impacts of the loss of privacy*."

68. The vagueness of the listed factors will make subsection 12(2) nearly impossible to implement and add no value to the principle stated at subsection 12(1) that appropriate purposes are those "that a reasonable person would consider appropriate in the circumstances." They will open organizations to routine second-guessing regarding the effectiveness and choice of business practices, regardless of the nature of personal information collected or its intended purpose.

69. It is our understanding that subsection 12(2) is intended to codify the test referenced in *Turner v Telus Communications Inc.*, 2005 FC 1601, as presented in the Office of the Privacy Commissioner's (OPC) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) [of PIPEDA].[8] However, the OPC misconstrued the effect of *Turner* when creating the OPC guidelines.

70. The test that the OPC presents as the Federal Court's test for appropriateness is actually its own test. This test was previously applied by the OPC in its own investigation, but the Court refused to adopt it, despite the OPC urging it to do so.[9]

71. In fact, the kind of factors listed in subsection 12(2) have been applied by the courts only with respect to particularly sensitive personal information, such as sensitive medical information, biometric data and video surveillance of employees.

72. Codifying these factors and applying them to the collection, use and disclosure of all forms of personal information would remove judicial discretion and render the CPPA an inflexible and prescriptive set of rules that must be applied regardless of the context. It would require organizations to undertake analysis and keep detailed documentation for all activities involving personal information, even those that should not be controversial, in case they were called upon to establish that all the listed factors had been considered.

73. The most appropriate way to address the concerns listed above is to delete subsection 12(2) and rely on the flexible, context-driven reasonableness standard

[8] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

[9] Ibid, para 67, "Put another way, and more briefly, it is not for the Commissioner, however knowledgeable and informed she or he might be with respect to the issues here coming before the Court, to set the agenda of this Court where hearings such as this are in the nature of *de novo* proceedings."

set forth in subsection 12(1). If that is not acceptable to the Government, subsection 12(2) should be amended such that its application is limited only to the collection, use and disclosure of sensitive person information. This change would ensure that the scope of subsection 12(2) is not extended beyond current jurisprudence on the appropriateness of the collection, use and disclosure of personal information.

74. **Recommendation:** The preferable amendment is to delete subsection 12(2) in its entirety. Failing that, subsection 12(2) should be amended to read as follows:

> **(2)** Where an organization collects, uses or discloses sensitive personal information, t~~T~~he following factors must be taken into account in determining whether the purposes referred to in subsection (1) are appropriate:
>
> **(a)** the degree of sensitivity of the personal information; [….]

(c) Consent and Exceptions to Consent (sections 15 and 18)

75. The proposed CPPA's approach to consent and its exceptions does not correspond to the mechanisms for lawfully collecting and using personal information used by Canada's trading partners, nor to the context of consumer relationships across industries.

76. The CPPA represents a departure from PIPEDA's principles-based and balanced approach to "express" versus "implied" consent. It is also much more restrictive than the GDPR, which has multiple bases for legally processing personal information; only one of which is consent.[10]

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

78. It also raises serious concerns about the validity of previous consents obtained under PIPEDA that do not meet the more restrictive CPPA requirements.

79. If the CPPA is to retain consent as the primary basis for the lawful collection and processing of personal information, changes must be made to sections 15 and 18 of the proposed CPPA to provide greater flexibility with respect to how consent is obtained.

[10] GDPR has six bases for legally processing personal information, 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.

(i) Valid Consent (section 15)

80. As currently drafted, subsection 15(3) of the proposed CPPA departs from the principles-based approach of PIPEDA. It imposes highly prescriptive rules regarding the kind of information that must be provided to the individual, at or before the time that consent is sought. Not only does this rigid approach foreclose other reasonable methods for obtaining informed consent, it throws into doubt the validity of consents already obtained by organizations that did not follow these prescriptive requirements.

81. The unintended consequence is that Canadians could be inundated with requests to re-confirm consent for previous collections and processing of personal information. This would not only impose undue burdens on organizations, it would also result in a confusing and unwelcome inconvenience for individual Canadians, especially where the provision of services that utilize such information are interrupted as a result of the omission by the individual to re-confirm consent.

82. **Recommendation:** Subsection 15(3) of the proposed CPPA should be amended to incorporate the reasonableness standard currently found in s.6.1 of PIPEDA. It should also recast the prescriptive list of information to be provided to individuals as an exemplary list of possible, but not the only, ways by which an organization can satisfy the requirement for valid consent. Specifically, the clause should be amended as follows:

Information for consent to be valid

(3) The individual's consent is valid only if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. An organization may satisfy the validity requirement using different methods, including providing the individual, at or before the time that the organization seeks the individual's consent, ~~it provides the individual~~ with the following information in plain language: ...

83. The CPPA should also be amended to expressly state that nothing in the CPPA invalidates consents legally obtained by organizations prior to the date at which the CPPA comes into force.

(ii) Exceptions to Consent (section 18)

84. Consent fatigue is a real problem for organizations and individual Canadians. 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.

85. While section 18 of the proposed CPPA provides an exception to the requirement for knowledge or consent if the collection or use of personal information is made for a business activity that "a reasonable person would expect" and that is "not collected or used for the purpose of influencing the individual's behaviour or decisions", only business activities listed in subsection 18(2) or prescribed by regulations qualify for this exception.

86. Subsection 18(2) of the proposed CPPA introduces the artificial presumption of consent to only five sets of circumstances where collection is deemed to be necessary or legitimate for providing goods or services. Given the reasonableness standard in subsection 18(1), subsection 18(2) stands out as entirely redundant and out of line with the standards applied by Canada's trading partners.

87. By contrast, California's CCPA considers the pace of data-driven business models of the digital economy. It allows organizations to collect, use and even sell personal information without having to obtain consent (except in the case of minors), provided they must give individuals the right to opt-out of having their personal information sold.

88. For its part, the GDPR also 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.*"[11]

89. As drafted, the proposed CPPA makes, with few exceptions, express consent the default basis for the collection, use and disclosure of personal information. 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 Canada so well and the rational approach that grounds implied consent in the circumstances that surround it.

90. 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

[11] GDPR, Article 6(1)(f)

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.

91. **Recommendation:** To preserve the rational, principled and technology-neutral approach that has been the strength of the Canadian privacy regime, allowing it to protect privacy as privacy risks evolve through business models and technology, subsection 18(2) should be removed. This would allow the contextual criteria of subsection 18(1) to determine whether consent is required.

92. To address consent fatigue, keep express consent meaningful, and ensure that individuals are informed about the collection, use and disclosure of their personal information on complex technological platforms, the activities currently listed in 18(2) should be left to the obligation to state them in privacy policies.

93. In the alternative, if the Government is not willing to make the changes recommended above, the business activities listed in subsection 18(2) must be expanded. At a minimum the following two additional businesses activities should be added (each of which would remain subject to the reasonableness standard and influencing behaviour or decisions restriction set forth in subsection 18(1)):

    - an activity that is carried out to understand and analyze the interests, needs, and preferences of customers and users;

    - an activity that is carried out to assess, develop, enhance or provide products and services;

(d) Openness and transparency – Automated Decision Systems (sections 62 and 63)

94. Sections 62 and 63 of the proposed CCPA require organizations to make certain disclosures and explanations regarding the use of automated decision systems. Subsection 62(2)(c) requires the organization to make readily available a general account of its use of automated decisions systems "to make predictions, recommendations or decisions about individuals that could have significant impacts on them" (emphasis added). However, subsection 63(3) requires an organization, upon request by the individual, to provide an explanation of any prediction, recommendation or decision made using automated decision systems and how personal information was used in making same.

95. Unlike subsection 62(2)(c), subsection 63(3) is not limited to predictions, recommendations or decision that could have significant impacts on the individual. The absence of such a qualifier in subsection 63(3) means that organizations would have to develop processes and allocate resources to provide explanations regarding uses of automated decision systems, even where there is no significant impact on the individual.

96. This requirement creates an undue and unnecessary administrative burden for organizations, while it does not offer any meaningful additional protections to individuals. The obvious fix is to make subsection 63(3) subject to the same qualification as subsection 62(2)(c).

97. **Recommendation:** To address the issues raised above, subsection 63(3) should be amended to read as follows:

> 63 (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could produce significant impacts on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision that is reasonable in the circumstances and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

(e) Retention and disposal of personal information (sections 53 and 55)

98. In setting out a limitation on the period during which an organization may retain personal information, 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 the Act and other legal obligations.

99. This recognition is undermined by section 55 which requires that, upon the request of the data subject, the organization must delete the requestor's personal information. Section 55 makes no reference to section 53, and the exceptions listed in section 55 do not cover all the circumstances under which an organization may need to retain such information despite a disposal request.

100. First, section 55 must be congruent with section 53 and with section 18 "*business activities*". It must be amended to allow an organization to deny a disposal request where the information is retained in compliance with section 53, namely, "*to fulfil the reasonable purposes for which the information was collected, used or disclosed"* or to *"comply with the requirements of this Act, of federal or provincial law or of the reasonable terms of a contract."* It should also allow for the retention

of information that was collected for business activities for which section 18 does not require knowledge or consent.

101. Second, subsection 55(c) limits the organization's disposal obligation to cases where "*there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from doing so" (emphasis added).* While some laws prevent the disposal of information, there are other circumstances where it is reasonable for an organization to retain personal information in order to protect or exercise its legal rights.

102. For example, statutory limitation periods do not require an organization to retain personal information for a specified period. Rather, they set out a period during which one party may make a claim against the other. In order to defend itself against a potential claim, it is reasonable to allow an organization to retain related information for the duration of the limitation period. In fact, as there is often some uncertainty as to the exact start date of a limitation period, organizations will frequently add a reasonable buffer into their retention schedule.

103. In some cases, a statute may not provide for any limitation period, and organizations must estimate at what point in time the risk of it being subject to complaint is unlikely. For example, there is no explicit limitation period in which an individual may file a complaint with the Commissioner under the CPPA. Instead, section 83(1)(c) merely gives the Commissioner the discretion to decline to investigate if the complaint "was not filed within a reasonable period after the day on which the subject matter of the complaint arose."

104. Statutes may also require organizations to retain records containing personal information for a period that cannot be objectively measured. For example, section 54 of the proposed CPPA requires an organization to retain personal information "for a sufficient period of time to permit the individual to make a request for access under section 63." Organizations will have to make a reasonable determination of the appropriate retention period.

105. It is instructive to compare section 55 of the proposed CPPA to Article 17 of the GDPR, which provides the GDPR's version of the right to request disposal, referred to as the right to be forgotten.

106. Article 17 of the GDPR does not apply if the organization needs to process personal information 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.

107. The proposed right to disposal in the CPPA accommodates none of the legal rights of the organization. Proposed section 55 should offer a proper definition of the scope of the right to disposal to correspond with an organization's legitimate business purposes, in line with the obligations on retention in section. This entails applying the right to disposal exclusively to information that is no longer necessary to fulfill the purposes for which it was collected, or for the organization to assert its legal rights, such as the fulfilment of a contract, debt recovery and the exercise or defense of legal claims.

108. Given the application of administrative monetary penalties for a violation of sections 53 or 55, it is imperative that potential conflicts between these two provisions of the CPPA are resolved.

109. **Recommendation:** Section 53 should be amended as follows:

> An organization must not retain personal information for a period longer than reasonably necessary to…..

110. Section 55 should be amended to include exceptions similar to those listed in Article 17 of GDPR, as well as exceptions if the organization's continued retention of the information is in compliance with s.18(2) or s.53 of the proposed CPPA.

(f) Penalties and Enforcement

111. The goal of achieving a "Clear and Responsive Marketplace Framework" cannot be realized without a fair system of enforcement, including the reasonable application of penalties and due process.

(i) Penalties (section 93)

112. The introduction of penalties to Canada's privacy regime transforms its nature from an ombudsman regime under PIPEDA, which provides guidance to organizations in meeting their obligations, to an enforcement regime that will punish organizations for contravening their obligations under the proposed CPPA.

113. The importance of this change cannot be underestimated. This is especially the case since the proposed CPPA is not simply an updating of PIPEDA, but a whole new statute containing many novel provisions that will be interpreted for the first time when considering whether to impose a penalty.

114. Section 93(2) seeks to protect fairness in the recommendation of a penalty with the following factors for the OPC to consider: the nature and scope of the contravention; whether the organization has voluntarily paid compensation to

affected individuals; the organization's history of compliance; and any other relevant factor.

115. For the reasons stated above, it is appropriate that the Commissioner and the newly established Personal Information and Data Protection Tribunal (Tribunal) should also consider the novelty of the facts or findings in the case.

116. The Commissioner and Tribunal should also be required to consider the organization's due diligence and good faith in attempting to comply with the Act. For example, when it comes to security, section 57(1) requires organizations to implement safeguards that are "proportionate to the sensitivity of the information", while section 57(2) lists additional factors that must be considered by the organization when determining the appropriate level of protection to be employed. In other words, organizations must apply due diligence when protecting personal information.

117. Unfortunately, despite best efforts, cyber-attacks are a constant and evolving activity. Even the most highly-protected institutions, including the military, suffer breaches of security. Fairness dictates that the application of penalties under section 93 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. This fact should be reflected in the factors to be considered in subsection 93(2).

118. Finally, the reference to "paid" in current subsection 93(2)(b) should be amended to account for the fact that forms of compensation other than the payment of money may be appropriate. For example, an organization may provide an individual with credits, additional goods or services at no additional cost, or other forms of compensation.

119. **Recommendation:** Subsection 93(2) should be amended to read as follows:

Factors to consider

(2) In making the decision, the Commissioner must take the following factors into account:

(a) the nature and scope of the contravention;

(b) the novelty of the facts or findings;

(c) the organization's due diligence and good faith efforts to comply with this Act;

~~**(b)**~~**(d)** whether the organization has voluntarily compensated a person affected by the contravention;

~~**(c)**~~**(e)** the organization's history of compliance with this Act; and

~~**(d)**~~**(f)** any other relevant factor.

(ii) Lack of Recourse to the Federal Court

120. A significant weakness of PIPEDA is that the right to appeal to the Federal Court of Canada belongs exclusively to the OPC. A similar weakness exists in the proposed CPPA which gives rise to even more significant potential consequences as a result of the new enforcement powers granted to the OPC and the risk of significant financial penalties. No "*responsive marketplace*" can exist with a built-in bias against organizations in the enforcement regime, and certainly not with impactful penalties at stake.

121. The Privacy Commissioner, however well-intentioned, is a single decision-maker, fallible as any other. The Commissioner may also not have the necessary business experience to properly assess the balance between the individual's right to privacy and the legitimate need of organizations to collect and process personal information as stated in section 5 of the proposed CPPA. For these reasons, enforcement powers must be accompanied by corresponding rights of recourse for organizations.

122. Based on case law and experience regarding the OPC findings, a preliminary recourse to the Federal Court of Canada must be available during an investigation to allow a respondent organization to seek remediation of an erroneous position of the OPC in a timely manner.

123. A recent and compelling illustration of the need for such preliminary recourse arose in 2019 when the OPC erroneously interpreted PIPEDA to require consent for cross-border transfers of personal information. Such an interpretation would have had significant detrimental impacts on the global competitiveness of Canadian organizations, making routine data transfers that are essential to their operations impractical, and in many cases operationally impossible to implement. The OPC's new requirements also risked contravening Canada's commitments under several international trade and other agreements, and would have made Canada an outlier when compared to its trading partners around the world. Fortunately, the OPC reversed its position after launching a public consultation that overwhelmingly demonstrated its legal mistake.

124. The incident underscores the need for a preliminary recourse to the Federal Court where a respondent organization can properly defend its good faith interpretation of the law, in a timely fashion, and before the Commissioner issues a finding. In that case, had such a right been provided in PIPEDA, the affected organization could have turned to the Federal Court as the investigation was ongoing to seek clarification on the legality of the position taken by the OPC.

125. While section 100 of the CPPA creates a right to appeal findings and certain orders of the Commissioner to the Tribunal, there is no mechanism for seeking legal recourse during the course of an investigation. Furthermore, section 6(4) of the proposed Personal Information and Data Protection Tribunal Act provides that only "one of the members of the Tribunal must have experience in the field of information and privacy law." Even then, it is not a requirement to be a jurist. Consequently, recourse to the Federal Court should be created for organizations to obtain clarification of law during an OPC investigation.

126. **Recommendation:** The proposed CPPA should be amended to give organizations the right to seek clarification of law from the Federal Court during an OPC investigation.

(iii) Disposition of Appeals (section 102)

127. Subsection 102(2) provides that the standard of review for a decision of the Commissioner is "correctness for questions of law and palpable and overriding error for questions of fact or questions of mixed law and fact".

128. As referenced above, the Commissioner is a single decision-maker whose decisions will have long-lasting, formative influence on the interpretation of CPPA, as well as a direct impact on individuals and organizations. It is therefore important that the decisions of the Commissioner be subject to rigorous review. The standard of "palpable and overriding error" is not an adequate standard of review.

129. **Recommendation:** Subsection 102(2) should be amended as follows:

> **(2)** The standard of review for an appeal is correctness for questions of law and ~~palpable and overriding error~~ reasonableness for questions of fact and for questions of mixed law and fact.

(iv) *Interim Orders (section 98)*

130. Subsection 98(1)(d) gives the Commissioner the power to make "any interim order that the Commissioner considers appropriate". Interim orders can have long-lasting impacts and impose costs that cannot be recovered. They are also made with an incomplete factual record.

131. Despite the potentially serious implications of an interim order, subsection 98(1)(d) does not impose any legal standard that the Commissioner must follow in making interim orders. A fair system of enforcement requires that interim orders not be made lightly and that they must meet an appropriate threshold.

132. **Recommendation:** Subsection 98(1)(d) should be amended as follows:

> **98 (1)** In carrying out an investigation of a complaint, conducting an inquiry or carrying out an audit, the Commissioner may
>
> […]
>
> **(d)** ~~make any interim order that the Commissioner considers appropriate~~ after notifying any affected parties and providing them with an opportunity to make submissions, make any interim order where the Commissioner determines that:
>
> (i) the order is necessary to prevent significant irreparable harm to individuals;
>
> (ii) such harm outweighs any harm likely to be suffered, as a result of the order, by a party to whom the order is directed; and
>
> (iii) the order is otherwise appropriate.
>
> […]

E. Putting Data to Use for Canadians

133. The Digital Charter recognizes the need for Canada to embrace digital and data-driven-technologies that will "create new business opportunities, foster new, high-value jobs, improve the collective ability to be leaders of change, and create a better quality of life for all." It further champions the need for "a cohesive vision for [Canada's] digital future that builds on the country's strengths, is flexible and nimble in reducing barriers to innovation, encourages a thriving and secure innovation-based marketplace, and ushers in a new era of Canadian global competitiveness."

134. This vision is echoed in Section 5 of the proposed CPPA, which recognizes that we live "in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information." Section 5 further states that the purpose of the CPPA is to strike a balance between the "right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." The proposed CPPA falls short of this objective in several areas.

(a) The Use of De-identified Information

135. As referenced above, the current definition of "de-identify" in section 2 of the proposed CPPA is problematic and gives rise to unintended consequences. For the reasons explained above, we recommended that the term "de-identify" be used to reference the process of removing personal identifiers from personal information

so that the de-identified information no longer directly identifies an individual. We also recommended a new definition, “non-personal information”, to reference information that “does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.” Information that is de-identified but falls short of being non-personal information would remain subject to the CPPA. Non-personal information would not be subject to the CPPA.

136. Implementation of the proposed definitions of “de-identify” and “non-personal information” requires a review of the provisions of the proposed CPPA where the term “de-identify” is currently used.

Section 20 – De-identification of personal information

137. While the current wording of Section 20 states that consent is not required to de-identify personal information, it also implies that de-identifying personal information is a use. This suggests that other non-substantive transformations of personal information, such as truncating, destroying, or encrypting, could be considered a use for which consent would be required. This unintended consequence can be avoided by revising Section 20 to confirm that neither knowledge nor consent is required to de-identify information. Any subsequent use of de-identified information that continues to be personal information would require consent, subject to any of the statutory exceptions.

138. **Recommendation:** Section 20 should be revised as follows:

For greater certainty, a~~A~~n organization does not need ~~may use~~ an individual’s ~~personal information without their~~ knowledge or consent to de-identify their personal information, including to create non-personal information.

Section 21 – Research and Development

139. As section 21 deals with an organization’s use of personal information for its own research and development, the continued use of “de-identified” (as newly defined herein) is appropriate. The safeguards introduced by sections 74 and 75 provide adequate protections against improper re-identification of information.

140. As discussed above, “non-personal information” should fall outside the scope of the Act, and the permission granted under section 21 is not needed in order to use such information for research and development purposes.

Section 22 – Prospective Business Transactions

141. The CPPA proposes to add the condition that information be de-identified before it is used or disclosed in context of a business transaction (as defined) and remains so until the transaction is completed. This requirement does not reflect the reality of business transactions.

142. As part of the due diligence process, it is common that a prospective purchaser of assets or the company needs to review information pertaining to key employees, as well as client lists. This information is required for the acquiring party to assess the level of risk and the value of the transaction.

143. Current PIPEDA provisions in this regard properly reflect the reality of exchanges of information that is necessary to determine whether to proceed with a transaction and, if so, under what terms. Privacy is protected through the requirement for an agreement that governs the exchange of personal information, limiting it to what is necessary and specifying that it can only be used for the purposes related to the transaction. Appropriate security safeguards must be applied and the receiving organization must be obligated to return this information should the transaction not proceed.

144. There is no indication that the above-mentioned provisions of PIPEDA are not working, and Section 22 of the CPPA contains similar safeguards. It is not clear what problem the additional requirement to de-identify information prior to being disclosed is trying to solve. Rather, it is an unnecessary requirement and makes the proper exercise of due diligence impossible.

145. **Recommendation:** Subsection 21(1)(a) should be removed.

Section 39 – Socially beneficial purposes

146. Section 39 permits disclosure of an individual's personal information without their knowledge or consent provided it is first "de-identified" and is only disclosed to a limited set of entities and only for a "socially beneficial purpose". Due to the problems identified above with the current definition of "de-identify" in the proposed CPPA, the purpose of section 39 is unclear.

147. If the intent is that personal information must first be anonymized or transformed into "non-personal information" (as defined herein) then the section 39 is problematic.

148. Not only should non-personal information fall outside the scope of the CPPA, the concept of using data for good, or for socially beneficial purposes, recognizes that

there is a balance that must be struck between using data to benefit society and the risk of re-identification. Requiring information to be rendered non-personal information (as defined herein) before it can be shared risks making the information less useful for the intended socially beneficial purpose. Placing restrictions on the use of non-personal information would result in restrictions that are not imposed on organizations by Canada's key trading partners.

149. The CPPA manages the risk of re-identification by imposing safeguards such as those in section 74, which states that "an organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information."

150. Section 39 only makes sense if its application is limited to information that, despite the removal of personal identifiers, remains personal information. As such, if the new definition of de-identify that we have recommended above is implemented, then the continued use of the term "de-identified" in section 39 is appropriate. If the current definition of "de-identify" is maintained, the utility of section 39 should be questioned and the ability of organizations in Canada to innovate and use data for good would be severely impacted.

F. Security

151. The Digital Charter also pursues the third goal of "Security". As mentioned at the outset, the protection of personal information is of the utmost importance to our members. After reviewing the security-related provisions of the proposed CPPA, we have the following recommendations:

(a) Accountability of service providers for breaches (section 61)

152. Section 61 of the proposed CPPA creates the obligation for a service provider to notify, as soon as feasible, the "*organization that controls the personal information"* of any breach of security safeguards.

153. Subsection 7(2) provides that "*Personal information is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure […] by the organization itself or by a service provider on behalf of the organization*."

154. The combined effect of sections 61 and 7(2) is to place the responsibility of addressing a security breach entirely upon the organization that hired the service provider. Organizations have a responsibility to provide appropriate notification to

impacted individuals when a security breach creates a real risk of significant harm. The organization, however, may not have full visibility into the nature or extent of the breach, the existence of real risk of significant harm, as well as the identity of which individuals to notify, as the case may be, without the cooperation of its service provider.

155. Despite due diligence in hiring and using contractual clauses to ensure compliance with privacy obligations, it can be difficult for originating organizations to compel the assistance of a service provider after a breach has occurred. For example, an organization may be terminating a contractual arrangement and planning to recover costs from the service provider. This creates little incentive for that service provider to continue to cooperate with the organization. As such, service providers should be accountable for more than simply notifying the organization of a breach.

156. **Recommendation**: To ensure proper management and mitigation of the impact of a breach, section 61 of the proposed CPPA should be modified to read:

> If a service provider determines that any breach of security safeguards has occurred that involves personal information, it must as soon as feasible notify the organization that controls the personal information and must provide the organization with all information in its possession that is requested by the organization so that the organization can comply with sections 58, 59 and 60.

(b) Prohibition on re-identification (section 75)

157. Section 75 of the proposed CPPA provides that an organization "*must not use de-identified information alone in combination with other information to identify an individual*". The one exception is to test the effectiveness of the security safeguards that the organization has put in place to protect the information.

158. This limited exception does not consider the fact that organizations will often temporarily de-identify information as part of data management and protection practices, and then re-identify it when such re-identified information is to be used for lawful purposes.

159. In addition, it is possible that an organization seeking to associate data with an identifiable person may not be aware that the data was previously de-identified. As such, the prohibition should be limited by a knowledge qualifier.

160. **Recommendation**: Section 75 should be amended to read:

> An organization must not knowingly use de-identified information alone or in combination with other information to identify an individual, except:

(a) in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information; or

(b) *where the information has been de-identified or de-personalized by the organization itself, as a security safeguard or data minimization measure*.

G. Conclusion

161. PIPEDA has proven its effectiveness and value for Canada. The OPC has caused organizations to change their internal policies and practices. Light has been shed on otherwise inscrutable uses of personal information on the internet. Canadians have enjoyed a high level of protection of their privacy.

162. These outcomes result from the fact that PIPEDA pursues the goals now set out in the Digital Charter. "Clear and Responsive Marketplace Frameworks" are secured with firm principles and flexibility in their application to address privacy risks as they evolve, while providing clarity, fairness in enforcement and avoiding undue burden and cost to organizations. "Putting Data to Use for Canadians" is served by affording the proper level of protection to information according to risk to privacy while embracing innovative uses of data that create a better quality of life for all. It also enhances Canada's competitiveness in a data-driven digital economy. Data security is ensured through the obligation to apply technical, physical and organizational measures that are appropriate to the level of sensitivity of the organization.

163. The strength of PIPEDA resides in its adaptability to context. Individual context determines the expectation of privacy, and general context allows proper responses to technological changes as they occur. The Act must update PIPEDA without losing the strengths that have served Canadians so well for decades. It must also respect the purpose set forth in section 5 of the proposed CPPA which is to recognize the right of privacy as well as the need for organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

164. Finally, while we encourage a made-in-Canada approach to privacy reform, privacy regulations cannot be made in isolation. While the Act does not need to be the same as privacy legislation in other countries, it must avoid imposing obligations that are out-of-step with Canada's key trading partners. Such measures could negatively impact Canada's competitiveness without necessarily furthering the protection of privacy.

165. The recommendations set out herein will help the Act achieve the objectives set forth in the Digital Charter.

APPENDIX A

SUMMARY OF RECOMMENDATIONS

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

1. The proper implementation of CPPA calls for a minimum general transition period of 24 months from the date of Royal Assent before the CPPA comes into force. (¶ 12-20)

2. 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 such industry (e.g. the CRTC). For industry sectors where data mobility rights are merited, in order to allow for successful implementation, the CPPA should defer the entry into force of the data mobility provisions to mobility to three years after the applicable regulations are enacted. (¶ 21-30)

3. Given the significant mechanisms for enforcement that exist in the Act, and the real risk of encouraging speculative class actions, the private right of action should be removed from the Act. If it is not removed, the proposed private right of action in the CPPA should, as shown with the experience of CASL, be suspended indefinitely or, at minimum, should not be brought into force until a period of at least five years following Royal Assent. Prior to this period ending, the impact of the CPPA can be assessed and data gathered on the value, if any, of introducing a private right of action. (¶ 31-36)

4. The definition of “automated decision systems” and “de-identify” (section 2) must be amended and CPPA should expressly state that it does not apply to “non-personal information” (as defined herein). (¶ 42-45; ¶46-64)

5. The appropriate purposes test for the collection, use or disclosure of personal information should rely on the flexible, context-driven reasonableness standard set forth in subsection 12(1). The rigid and inflexible list of factors in subsection 12(2) that are to be considered when assessing reasonableness should be removed. In the alternative, if subsection 12(1) is not removed from the CPPA, subsection 12(2) should only apply to sensitive personal information. (¶66-74)

6. The highly prescriptive rules set out in section 15(3) regarding the kind of information that must be provided to the individual, at or before the time that consent is sought, should be replaced by the reasonableness standard currently

found in s.6.1 of PIPEDA. The CPPA should also be amended to expressly state that nothing in the CPPA invalidates consents legally obtained by organizations prior to the date at which the CPPA comes into force. (¶75-83)

7. To address the issue of consent fatigue, and to make express consent meaningful, the list of business activities in subsection 18(2) should be removed, as it limits the reasonable expectations exception to knowledge and consent in subsection 18(1). Instead, organizations should be obligated to disclose business activities to which a reasonable expectation of consent attaches in their privacy policies. Failing that, the list of business activities in subsection 18(2) must be expanded as described above. (¶84-93)

8. The obligation to explain a prediction, recommendation or decision that is aided by using an automated decision system (ss. 63(3)) should be limited to predictions, recommendations or decisions that have a significant impact on the individual. (¶94-97)

9. The individual's right to request the disposal of information set forth in section 55 must be made consistent with the organization's information retention rights (s.53), as well as its other legal rights and obligations. (¶98-110)

10. To ensure fairness in the recommendation of a penalty against an organization, the factors to be considered by the Commissioner (ss. 93(2)) should be expanded to include the novelty of the facts or findings, as well as the organization's due diligence and good faith efforts to comply with the CPPA. (¶112-119)

11. Organizations should have the right to seek clarification from the Federal Court on matters of law during an investigation. (¶120-126)

12. The standard of review for the appeal of a decision by the Commissioner (ss. 102(2)) should be reasonableness for questions of fact and for questions of mixed law and fact. (¶127-129)

13. A fair system of enforcement requires that interim orders not be made lightly. They must meet an appropriate threshold. Given the potentially serious implications of an interim order by the Commissioner, subsection 98(1(d) should be amended to include a legal standard for making interim orders that considers whether there is a risk of significant irreparable harm and whether such individual harm would outweigh any harm that is likely to be suffered, as a result of the order, by the party to whom the order is directed. (¶130-132)

14. The additional requirement that personal information be de-identified prior to being disclosed in relation to a prospective business transaction (s.22) should be removed. (¶141-145)

15. In addition to the obligation to notify the organization of any breach of security safeguards (s.61), service providers should also be required to provide the organization with information in the service provider's possession that may be needed by the organization to comply with its obligations under sections 58, 59, and 60. (¶152-156)

16. Section 75 should be amended to expressly state that an organization may re-identify de-identified information if that information was de-identified by the organization as a security safeguard or data minimization measure. (¶157-160)

[End of Document]