May 31, 2016

Data Breach Consultations
Privacy and Data Protection Policy Directorate
Innovation, Science and Economic Development Canada
235 Queen Street
Ottawa ON K1A 0H5

Via email: ic.ised.breach-atteinte.isde.ic@canada.ca

Re: CWTA Comments, *Data Breach Notification and Reporting Regulations*

1. The Canadian Wireless Telecommunications Association (CWTA) is the authority on wireless issues, developments and trends in Canada. It represents wireless service providers as well as companies that develop and produce products and services for the industry, including handset and equipment manufacturers, content and application creators and business-to-business service providers. CWTA is pleased to file its comments with respect to the above-noted consultation.

2. CWTA and its members are committed to protecting the privacy of all Canadians, including safeguarding the personal information provided by consumers and partners that enjoy our products, programs and services. In addition to fully complying with legislated obligations in PIPEDA, protecting personal information is a business imperative and a matter of corporate social responsibility. The Office of the Privacy Commissioner's voluntary guidelines on data breach reporting have worked well and many organizations have developed processes that comply with the voluntary guidelines. Consequently, mandatory reporting should have minimal impact on organizations that already maintain strict privacy safeguards. However, data breach recording obligations are new, and may require technical investments, process changes and new employee training, even for organizations that already maintain strict privacy safeguards.

3. For breach recording, reporting and notification obligations it is important to maintain practical and principles-based requirements that have a proven track record. Overly-prescriptive measures can unintentionally and unnecessarily burden responsible companies without delivering greater privacy protection to individuals. Over notifying individuals and third parties where there is minimal risk of harm can cause undue inconvenience, worry, and ultimately notice fatigue, whereby important notifications become less meaningful. Similarly, any mandated publication of that breach reports made to the OPC could unintentionally provide a "how-to" resources for malicious parties to conduct breaches more effectively in the future.

4. CWTA therefore proposes an overall approach to Data Breach Notification and Reporting Regulations that: closely follows the Office of the Privacy Commissioner of Canada's existing voluntary data breach reporting program; continues allowing organizations to reasonably exercise discretion in dealing with the variety of data breaches that may occur (e.g. context matters); and recognizes existing safeguards in place by organizations that minimize the potential for harm in the case of a data breach. We are pleased to describe, through the

remainder of this submission, how these principles can be applied to the questions asked in the Department's discussion paper.

Determining real risk of significant harm

5. CWTA submits that the risk-assessment factors listed in the legislation clearly outline the most important criteria for assessing risk – namely, the sensitivity of the information involved and the probability that it will be misused. As the Department's discussion paper appropriately points out, "it is not practical to list specific types of personal information or to identify a defined list of circumstances that trigger the reporting and notification requirements" because "one of the fundamental principles in privacy protection is that context matters." It would be difficult to exhaustively identify criteria to categorically gauge the sensitivity of personal information in the absence of context.

6. Regulations or interpretive guidance from the OPC should encourage organizations to implement the latest and most effective safeguards and processes. CWTA submits there are two ways additional clarity provided in a guidance document could promote reducing the probability that data involved in a breach situation will be misused. The first is by creating a presumption that there is no risk of significant harm where the personal information involved is protected by robust technical safeguards. Guidance referring to robust technical safeguards should be technology neutral – to account for change over time – by specifying that any measure that renders personal information unusable, unreadable or indecipherable based on generally accepted industry standards can be presumed to lower the risk to individuals. Encryption alone should not be singled out as the only form of technical safeguard.

7. The second way to promote effective data safeguards and processes is creating a presumption that strong mitigation and containment measures taken by the organization after a breach has occurred can also reduce or eliminate the risk of significant harm. For example, an organization's ability to remotely delete personal information with a high level of confidence immediately following a data breach (e.g. before the personal information has been accessed) should factor into the risk assessment under 10.1(8)(b) of the legislation.

8. The presumption that there is a low risk of harm due to technological safeguards or mitigation and containment measure could always be rebutted by the OPC if there was evidence that the measures had been circumvented or had failed in a specific breach. But creating such presumptions in regulatory guidance documents would encourage organizations to implement processes and safeguards that would benefit the privacy of Canadians.

Report to Commissioner – form and content

9. CWTA submits that the existing OPC voluntary data breach report form should be maintained under the regulations. The current voluntary form is practical, comprehensively covers the lifecycle of a breach while providing flexibility for organizations, and has a proven track record. The voluntary form also contains all the factual elements necessary to assess whether there is a real risk of significant harm. Indeed, the decision to submit a report is triggered by the organization's determination that a real risk of significant harm exists. As such, a specific assessment of harm is not necessary in reports to the OPC.

10. Data breach reports submitted to the OPC should be kept in confidence. Any public disclosure of breach reports received by OPC should only occur on an aggregated and anonymized basis. Reports contain

information on organizations' understanding of the breadth of data breaches, as well breach response tactics. Making public all of the contents of individual breach reports would assist malicious parties in carrying out more effective breaches in the future, and would effectively form a 'how-to' resources for malicious hackers. Breach reports can also contain confidential business and strategic information related to the company in question as well as their suppliers, which is often subject to non-disclosure arrangements.

11. Breach reports will provide the greatest benefit to OPC if organizations are able to make the full and frank disclosures that would be facilitated by confidentiality; organizations may be less forthcoming if technical and business details relating to a breach will be made public. Further, publishing all breach reports, particularly interim reports, could unnecessarily make public incomplete or inaccurate information based on the initial knowledge of a data breach.

12. CWTA submits that the requirement to make a report "as soon as feasible after the organization determines that the breach has occurred" should be maintained to allow organizations the flexibility to address the actual data breach and provide a report when meaningful facts have been confirmed. A rigid timeframe for reporting could also result in inaccurate information and repetitive updates.

13. Organizations should also be provided flexibility in how they report a data breach to account for the fluidity of breach situations. An organization should be considered to be in compliance with the regulations once a report has been completed with all of the information that will be available. However, this should not preclude organizations from initially providing semi-complete reports to alert the OPC based on what is known at the time. The regulations should allow organizations to update the OPC with any information that would materially alter an existing report.

14. Final data breach reports should be required to be submitted in writing, and a secure, electronic means of reporting data breaches to the Privacy Commissioner should be established to safeguard the integrity of such reports. However, to maintain the flexibility of informing the OPC during a breach situation, initial verbal reports submitted by telephone should still be allowed.

Notification to individuals – content

15. The principles for notifying individuals set out in the legislation is sufficiently clear for organizations to identify what information to include in notifications to individuals. Specifically, it requires the information to be sufficient and such that an individual can understand the significance of the breach and what they may be able to do to mitigate harm. The legislation is also appropriately flexible to allow organizations to craft notifications that respond to the context of a particular data breach. Additional prescribed regulations may hinder this ability.

16. The list of information to be included in notifications to individuals set out in the OPC voluntary breach guidelines has been effective to date. Through a guidance document, the list could form a non-exhaustive recommendation of what is generally considered sufficient information for a breach notification, while continuing to allow organizations the discretion to adjust the content of a notice to fit the situational context.

Notification to individuals – form and manner

Direct notification

17. The most important factor to consider in terms of the form and manner of a notification to individuals is how best to ensure the individuals are appropriately and sufficiently notified of the data breach. The regulations must allow the form and manner of notifications to be tailored to the context of the data breach situation as well as the relationship the organizations have with their customers or partners. Regulations should be technology neutral to account for future forms of communication.

18. For example, written notifications may not be the most efficient in cases of data breaches where an individual's personal information could be compromised without their immediate action because written notification requires the individual to open and read the communication. Physical written notifications can also potentially be intercepted by someone other than the intended recipient. In such situations, a direct phone call and conversation may be more timely and appropriate. Conversely, it would be unnecessary to call individuals directly for less significant data breach situations where no action from the individual is required.

19. An organization's ability to use certain methods of notification can also be limited based on what contact information an organization has for an individual. Many wireless agreements do not require contact information other than the cellphone number for the associated service. In such cases organizations should be able, under the regulations, to choose to notify individuals of a breach through a direct phone conversation, a voicemail message or a text message depending on the context of the situation. Or, as may be the case in the future, organizations may notify individuals through other messaging platforms or services that will better ensure the individual is appropriately and sufficiently notified.

20. CWTA agrees that in all cases the notification must be conspicuous and distinct from other communications to help guarantee it is noticed and considered by the individual. We submit that the principle for distinct notification should be that, regardless of manner, the notification must be the sole purpose of the communication between the organization and the individual.

Indirect notification

21. CWTA reiterates that the regulations regarding notifying individuals of a data breach should be guided by the principle of ensuring individuals are notified as effectively and efficiently as possible. Organizations should be permitted to use any manner of notification, direct or indirect, to achieve this goal. The decision to use indirect notification should be determined by the organization experiencing the data breach, not by prescriptive regulation.

22. While direct notification to individuals will be the preferred form of notice in most circumstances, organizations will determine when resorting to indirect notice is most appropriate. The factors set out in the OPC voluntary breach reporting regime for when indirect notice (e.g. direct notice may cause excessive harm or there is insufficient or outdated contact information) are instructive and should form the basis for OPC guidance on this issue. An additional factor to include may be urgency. For instance, a high-risk breach where the individuals potentially impacted are not immediately identifiable would require indirect notification.

23. CWTA supports guidelines on indirectly notifying individuals rather than prescriptive regulations that may preclude notifying individuals indirectly in circumstances where it would be most efficient and effective to do so. CWTA also does not believe identifying a cost threshold for using indirect notifications is necessary.

Customer privacy and trust is a business imperative. Responsible organizations will always use the notification methods to protect the privacy of their clients and maintain their trust, regardless of cost.

24. As with direct notification, CWTA submits that all methods of indirect communication should be permitted to allow maximum flexibility to respond to situations as efficiently as possible. No matter how well-considered, conditions or limitations to using particular indirect communication methods could potentially prohibit using the most effective method in a certain data breach circumstance.

Notification to other organizations

25. The regulations should clarify that notifying third parties is only necessary where the organization has *actual knowledge* that such notifications will materially reduce risks or mitigate harm with respect to the breach in question. We also strongly believe that required third-party notification be limited to law enforcement and similar public authorities. A broad and prescriptive requirement to notify private third parties of a breach will increase costs without meaningfully mitigating the impact of data breaches on Canadians.

Record keeping

26. As noted in the discussion paper, record keeping is an important component of long-term privacy diligence. The discussion paper also notes that "requirements should be flexible and reasonable so as to minimize the burden on organizations." CWTA supports both principles. The data breach reports should serve as meeting the record keeping requirement under the regulations for breaches that result in a real risk of significant harm. For breaches that did not need to be reported we support straightforward guidelines similar to those in the EU's *ePrivacy Directive*, which states that records must include "the facts surrounding the breach, its effects and the remedial action taken."

27. The record retention period must be sufficient to meet the goal of helping organizations identify patterns of data breaches over time. CWTA submits that two years is adequate to ensure regularly-occurring breach situations are identified and acted on. This requirement should continue to be limited to breaches of which the organization has actual knowledge.

28. The regulations should also not require the individual designated by the organization as being responsible for overseeing compliance with PIPEDA to be the same individual accountable for maintaining data breach records. These two tasks are often undertaken by different individuals within organizations and we can see no beneficial reason for that practice to be prohibited. While related, these are two very different responsibilities in practice that should be overseen by the most qualified individuals.

Other issues – transition period

29. As mentioned at the outset of this submission, while mandatory data breach reporting should have minimal impact on those organizations that already participate in the OPC's voluntary process, the obligation to record all data security breaches is a new obligation which may require database investments, process changes and broad-based employee training, even for organizations that already maintain strict privacy safeguards.

30. Such changes cannot be implemented until after the final regulations have been published; even relatively minor alterations between the draft regulations and the final regulations could trigger costly process changes. As such, we strongly submit that the Department provide an adequate transition period of no less than six months after the final regulations are published to allow organizations to comply.

Conclusion

31. The wireless industry is committed to protecting the privacy of all Canadians, including safeguarding the personal information provided by consumers and clients that enjoy our products, programs and services. Protecting personal information is a business imperative and a matter of corporate social responsibility.

32. CWTA therefore proposes an overall approach to Data Breach Notification and Reporting Regulations that:
    - Closely follows the Office of the Privacy Commissioner of Canada's existing voluntary data breach reporting program;
    - Continues allowing organizations to retain discretion in dealing with the variety of data breaches that may occur; and
    - Recognizes existing safeguards in place by organizations that minimize the potential for harm in the case of a data breach.

33. We appreciate the opportunity to participate in this important consultation.

End of Document