Coalition of Business Associations
Association of International Automobile Manufacturers of Canada
Canadian Chamber of Commerce
Canadian Federation of Independent Business
Canadian Life and Health Insurance Association
Canadian Marketing Association
Canadian Wireless Telecommunications Association
Entertainment Software Association of Canada
Global Automakers
Interactive Advertising Bureau of Canada
Magazines Canada

February 11, 2015, 2014

Industry, Science and Technology Committee
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6
Canada

RE: Submission to the Standing Committee on Industry Science and Technology with respect to Bill S-4

Attn. Roger Préfontaine**,** Clerk of the Committee

Dear Mr. Préfontaine,

The Canadian Chamber of Commerce is pleased to make the following submission on behalf of a coalition of businesses and business organizations that addresses certain provisions of Bill S-4 which is currently before the Standing Committee on Industry Science and Technology. The associations listed above would like to thank the Committee for this opportunity to provide their perspectives on Bill S-4, the *Digital Privacy Act*.

The coalition is comprised of a broad cross section of Canadian industry that is directly impacted by the government's proposed changes. In general, business is supportive of this effort from the government to refine Canada's privacy legislation. The purpose of this submission is to draw the Committee's attention to specific provisions of the government's proposal that might benefit from targeted revisions that would align the changes to current industry practices, while still meeting the government's objectives.

To begin, we wish to express that with the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada has achieved the perfect balance between the over regulation and prescriptive nature of typical EU privacy laws and the perceived under-regulation and sectorally based rules of the US. In fact, we would argue that Canada is the envy of other countries who are just now waking up to the principle of "accountability" that has been the cornerstone of PIPEDA for over a decade. Jurisdictions like the EU and the US are catching up to Canada and our decade long emphasis on a business' accountability when it comes to the personal information of consumers. We have also seen a new trend of countries such as Singapore adopting Canada's principles-based model rather than the more prescriptive EU model.

As principles-based regulation, PIPEDA provides guidance to business regarding their privacy obligations, avoiding overly prescriptive rules while at the same time permitting the necessary level of flexibility that leads to innovation. PIPEDA's technology neutral and flexible framework has proven capable of keeping up with changes to technology, the marketplace and evolving consumer expectations.

Generally speaking, we support the objectives of Bill S-4 and the various proposed changes to PIPEDA which will bring some additional certainty and improvements to the overall PIPEDA framework, such as new provisions regarding disclosure of personal information in the course of business transactions, use of personal information in the context of employment relationships and the introduction of an explicit breach notification obligation. However, in our view, some fairly minor and yet important changes are required to S-4 to meet the Government's stated objectives and to ensure the continued balance encompassed in PIPEDA that has served Canada well for over a decade.

The purpose of this submission is three-fold:

1. Outline the rationale as to why changes are encouraged.
2. Provide specific alternatives that the Committee can consider.
3. Bring focus to the suggested changes that have broad consensus across industry.

While individual associations may be providing additional comments, we have come together to propose in the attached document very targeted changes in four specific areas: i) valid consent, ii) breach notification thresholds and record keeping, iii) public disclosures and iv) network security.

We look forward to the opportunity to discuss these changes before the Committee.

Thank you for your consideration.

Sincerely,

Scott Smith
Director, Intellectual Property and Innovation Policy
Canadian Chamber of Commerce

cc: Hon. James Moore, Industry Minister, Industry Canada
John Knubley, Deputy Minister, Industry Canada
Daniel Therien, Privacy Commissioner
Chris Padfield, Director General, Digital Policy Branch, Industry Canada

Coalition of Business Associations Proposed amendments to Bill S-4

1. A new form of "valid consent" is not needed (clause 5 of S-4)

The Government has stated that this amendment is aimed at protecting children and other vulnerable groups of individuals; an objective we all share.

Simply put, however, the proposed valid consent provision is unnecessary. PIPEDA already clearly requires knowledge and consent, and it requires that consent be reasonably understandable by the individual. Current Industry best practices already reflect the government's objective in this regard. The Office of the Privacy Commissioner (OPC) has not been hampered in its efforts to protect children and ensure appropriate consent is obtained given the various findings and guidance provided over the years (see for example the OPC's recent *Guidelines for Online Consent* which address specifically children and youth).

While we acknowledge that the valid consent provision in S-4 has been improved upon from its predecessor in Bill C-12 by shifting from a subjective standard which was quite problematic to an objective standard, as drafted, new section 6.1 would still apply to all requests for consent and could have the unintended effect of casting doubt on the established standards and hence on the validity of consents that have been gathered by organizations since the law went into effect over a decade ago. The concern remains that organizations would have to engage in a costly revision of policies, procedures, forms and training for general customer interactions. In our view, the proposed provision will undoubtedly add unnecessary costs and uncertainty into what is a generally well-functioning private sector privacy protection regime that already protects all Canadians, including children and vulnerable groups of individuals.

We are also concerned about the ambiguity of using the expression "reasonable to expect." At minimum, we ask that the wording be changed such that: "Consent is only valid if it is reasonable to expect or if the organization reasonably expects..."

We support the recommendation of both the Canadian Bar Association and the Public Interest Advocacy Centre that this clause be deleted.

Recommendation:

Delete clause 5 of S-4.

2. Breach notification regime needs fine-tuning (clause 10 of S-4)

While there is overall support for the new mandatory breach regime, a handful of very targeted amendments to Bill S-4 are needed to ensure the new regime meets its stated policy objectives while not unnecessarily imposing unreasonable administrative burdens and risks on organizations with no material enhancement to the protection of personal information and the privacy of individuals.

a) Notification and reporting thresholds

It has long been recognized that the objective of reporting breaches to the OPC (to permit the OPC to track the volume and types of breaches, to provide guidance to organizations as required) is quite different from the objective of notifying individuals (to permit impacted individuals to mitigate harm), requiring slightly different thresholds or triggers to meet those differing objectives. That is why guidelines developed by the OPC in 2007, as well as the proposed breach notification regimes in earlier bills (Bill C-29 and Bill C-12), included two different thresholds: i) a real risk of significant harm for notifying individuals, and ii) material breaches for reporting to the OPC. This approach has been widely accepted and implemented by businesses across the country over the last few years.

Therefore, we recommend that the Government revert back to widely supported language that was included in Bill C-12 that provided for two distinct obligations – one for notifying individuals, and one for reporting to the OPC (copied below for convenience).

In the alternative, we would recommend preserving the proposed threshold in S-4 for notification to individuals as being "a real risk of significant harm", but slightly revise the threshold for reporting to the Privacy Commissioner to limit reporting to "material" breaches only. Over the last few years the Government, the Parliamentary Committee that reviewed PIPEDA, the OPC and numerous stakeholders have for the most part agreed that the OPC should not be overburdened with breach reporting.

Bill S-4 could also introduce factors to assist organizations in determining which breaches are "material". The original factors included in former Bill C-12 are reflected as a new proposed ss. 10.1(2), or such guidance could be left to the OPC as is the case today with guidelines issued in 2007 entitled *Key Steps for Organizations in Responding to Privacy Breaches*.

In either case, both recommendations would be consistent with the Treasury Board Secretariat's revised *Directive on Privacy Practices* that makes mandatory the reporting of any "material" data breach to both the TBS and the OPC (and the OPC and TBS worked together to define what constitutes a material breach).

Recommendation:

> Delete that part of clause 10 of S-4 that was new section 10.1 of PIPEDA, and replace it with the following parts of clause 11 from Bill C-12:
>
> **10.1** (1) An organization shall report to the Commissioner any material breach of security safeguards involving personal information under its control.
>
> (2) The factors that are relevant to determining whether a breach of security safeguards is material include
>
> (*a*) the sensitivity of the personal information;
> (*b*) the number of individuals whose personal information was involved; and
> (*c*) an assessment by the organization that the cause of the breach or a pattern of breaches indicates a systemic problem.
>
> (3) The report must contain the prescribed information and be made in the prescribed form and manner as soon as feasible after the organization determines that a material breach of its security safeguards has occurred.

10.2 (1) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

(2) For the purpose of subsection (1), "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(3) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include the following:

(*a*) the sensitivity of the personal information involved in the breach; and

(*b*) the probability that the personal information has been, is being or will be misused.

(4) The notification must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of the harm that could result from it or to mitigate that harm, as well as any other prescribed information.

(5) The notification must be given as soon as feasible after the organization confirms that the breach has occurred and concludes that it is required to give the notification under subsection (1).

(6) The notification must be conspicuous and given directly to the individual in the prescribed form and manner, except in the prescribed circumstances where it is not feasible to do so, in which case it must be given indirectly in the prescribed form and manner.

Alternative recommendation:

Amend clause 10 of S-4 as follows:

10.1 (1) An organization shall report to the Commissioner any material breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

(2) The factors that are relevant to determining whether a breach of security safeguards is "material" include

(*a*) the sensitivity of the personal information;

(*b*) the number of individuals whose personal information was involved; and

(*c*) an assessment by the organization that the cause of the breach or a pattern of breaches indicates a systemic problem.

b) Record keeping

The record keeping provisions of the proposed breach notification scheme are highly problematic for several reasons.

These provisions pose significant practical challenges for organizations, as the provisions do not contain any clear standard of materiality. The definition of "personal information" in the Act is extremely broad, and encompasses a wide spectrum of information, from the extremely sensitive to the innocuous. Accordingly, a broad array of common – and inevitable - workplace errors and omissions could constitute technical breaches of security safeguards, even where there is no discernible impact on individual privacy interests.

The lack of a clear materiality threshold for recording breaches necessarily requires that all breaches, regardless of how trivial or inconsequential (e.g. a single misaddressed billing envelope, a temporarily unlocked filing cabinet containing employee records, a customer invoice left momentarily on a service counter), must be diligently logged in the prescribed manner just in case the OPC makes a request, a daunting task for any organization, especially large organizations with multiple locations.

However, the record keeping requirement is particularly problematic as a failure to comply would also constitute a new offence under the proposed amendments to s. 28 (see clause 24 of Bill S-4). At best, pairing such a vague and overly broad provision with a criminal offence for non-compliance will cause risk-averse organizations to over-record, documenting any incident that might conceivably be viewed as a "breach". Such compliance efforts will give rise to additional business processes, training and monitoring efforts, and recording and retention infrastructure, all of which will add significantly to the administrative burden and costs of doing business in Canada – without any material benefit to the protection of privacy. At worst, legitimate and responsible businesses that act in good faith may nevertheless face criminal prosecutions for the failure to record immaterial "breaches."

Furthermore, attaching criminal offences to the new record keeping requirement seems to be entirely disproportionate to the nature of the potential "offence" in the context of the other offence provisions and the scheme of the Act as a whole. In this regard, the only other behaviours that are, or that are proposed to be, the subject of criminal offences for non-compliance are:

- The premature destruction of personal information that is the subject of an access request for individual access, in violation of s. 8(8);
- The failure to report to the Commissioner or an affected individual of a breach of security safeguards that create a real risk of significant harm to an individual, in violation of s. 10.1;
- Taking retaliatory action against a whistleblower, in violation of s. 27.1(1); or
- Obstructing the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit (s. 28).

Each of these other offences relates to actions that materially affect the privacy rights and interests of individuals, and that include a clear element of malfeasance. This is not the case for a failure to retain records for even the most mundane technical data "breaches."

In the circumstances, we submit that the simplest way to address the foregoing concerns would be to delete the reference in s. 28 of PIPEDA (as proposed to be revised by s. 24 of Bill S-4) to subsection 10.3(1). This would allow the new record-keeping obligation to be interpreted and applied by organizations and the OPC using the same flexible approach that currently applies to the vast majority of the obligations under

PIPEDA, including such fundamental requirements as accountability, collection of consent and providing for individual access. Under this approach, following further study and consultation with industry, the OPC could issue guidelines as to what constitutes an acceptable record keeping practice for breaches of security safeguards, similar to guidance the OPC provides today on breaches and other various obligations.

An alternative option would be to amend the record keeping obligation to apply only to "material" breaches that are reported to the OPC as recommended above (recognizing that this would not impact the normal record keeping practices of organizations). If the second option is adopted, then it is critical that organizations are consulted and know as soon as possible any prescribed requirements.

Recommendation:

> Amend clause 24 of S-4 as follows:
>
> **28.** Every organization that knowingly contravenes subsection 8(8), section 10.1 or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of

Alternative recommendation:

> Amend clause 10 of S-4 as follows:
>
> 10.3 (1) An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every material breach of security safeguards involving personal information under its control.

3. Need to narrow breadth of "public disclosure of confidential information" (clause 17 of S-4)

PIPEDA, like many other regulatory statutes granting investigative powers to a regulator, contains a provision generally prohibiting the Commissioner or any person acting under his direction from publicly disclosing information that comes to their knowledge in the performance of their duties and functions under this Act. Similar clauses are found, for example, in the *Access to Information Act*, the *Competition Act*, and the *Official Languages Act*, among others.

Such protections only make sense, as businesses share a good deal of information with the OPC that is of extreme commercial sensitivity. Moreover, in many cases this information is shared not in the context of an investigation, but on a voluntary consultative basis, where organizations are seeking to brief the OPC and receive informal feedback on proposed information management practices.

Alarmingly, the amendment to s. 20(2) of PIPEDA, as proposed by clause 17 of S-4, would provide such a broad, discretionary exception to the general prohibition on disclosure by the OPC that it would effectively eviscerate the general prohibition on disclosure, removing any protection currently offered under the law. In this regard, S-4 creates a broad exception that would allow the Commissioner to make public any information where he considers that it is in the public interest to do so. This level of discretion appears to be unprecedented in other federal and provincial regulatory statutes, and seems to ignore even the

categories of third party information whose non-disclosure is mandated under the *Access to Information Act*.

A significant result of the passage of such a broad exemption will be the reluctance of organizations to share information with the OPC, jeopardizing the cooperative relationships that the OPC has strived to create with many organizations and industrial sectors and significantly reducing, or even eliminating, voluntary consultations with the OPC that would involve the disclosure of commercially sensitive information.

We understand that the revised clause may have been introduced to remedy a perceived limitation in the previous wording, that some felt prevented the OPC from publicizing non-compliance with remedial agreements entered into by organizations, or from disclosing instances of obstruction or lack of cooperation with OPC investigations.

Accordingly, we would propose the following alternative wording, designed to preserve the essential confidentiality obligation found in PIPEDA, but allow the OPC greater latitude to make limited disclosures in the public interest.

Recommendation:

Amend clause 17 of S-4 as follows:

20. (2) The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part, where that information relates to:

a) the personal information management practices of an organization;
b) the compliance of an organization with a compliance agreement entered into pursuant to s. 17.1(1); or
c) the assistance or cooperation of an organization with respect to the acceptance of a recommendation, the investigation of a complaint or the conduct of an audit.

4. Network Security

Network and information security can often require collection, use and disclosure of personal information without the knowledge or consent of the individual. Take the example of efforts to counter a botnet being used for a denial of service attack. In this circumstance it may make sense to quarantine infected devices. This could involve use of personal identifiers, such as IP addresses, but it would be neither practical nor effective to request the consent of the individuals whose devices are being misused.

In order to effectively prepare for and mitigate security incidents, organizations need to communicate with one another and with government institutions. Networks and information systems are interdependent and vulnerabilities that can be exploited in one may be exploitable elsewhere. Security teams from the public and private sector need to work together in order to ensure the ecosystem is

protected and information sharing is a key component of such activities. Discretion can be essential during investigation or in order to get security measures in place. As such, it may not be wise to inform individuals whose information may be incidentally used.

Much as it may be necessary to collect, use and disclose personal information in order to ensure network and information security, it might be wise not to provide access to personal information if that stands to compromise the security stance. For example, an organization investigating a security incident may not want to give information relating to the investigation of the incident to the malicious actor suspected of being responsible. While subsection 9(3)(c) already provides for access refusal where such access threatens the security of another individual, not all security threats target individuals – for example, they may be targeted at a critical infrastructure. As such, a direct provision allowing for refusal on network and information security grounds would be welcomed.

Recommendation:

Amend Clause 6(3) of Bill S4 by adding the following clause as 7(1) b.3 in the Act:

b.3 it is in relation to the security of all or part of a computer system, network or information on such system or network from a current, suspected or identifiable threat to the availability, reliability, confidentiality, authenticity efficiency, or optimal use or integrity of such a system, of a computer system or network, information or other possible cyber security threat.

Amend Clause 6(5) of Bill S4 by adding the following clause as 7(2) b.3 in the Act

b.3 it is in relation to the security of all or part of a computer system, network or information on such system or network from a current, suspected or identifiable threat to the availability, reliability, confidentiality, authenticity efficiency, or optimal use or integrity of such a system, of a computer system or network, information or other possible cyber security threat.

Amend Clause 6(8) of Bill S4 by inserting the following clause as 7(3) d.3 in the Act:

b.3 it is in relation to the security of all or part of a computer system, network or information on such system or network from a current, suspected or identifiable threat to the availability, reliability, confidentiality, authenticity efficiency, or optimal use or integrity of such a system, of a computer system or network, information or other possible cyber security threat.