Coalition of Business and Technology Associations:

Canadian Bankers Association
Canadian Chamber of Commerce
Canadian Federation of Independent Business
Canadian Marketing Association
Canadian Vehicle Manufacturers' Association
Electro-Federation Canada
Entertainment Software Association of Canada
Global Automakers of Canada
Information Technology Association of Canada
Interactive Advertising Bureau of Canada
Magazines Canada
News Media Canada
Retail Council of Canada
The Email Sender and Provider Coalition

INDU Committee Members
C/O Ms. Danielle Widmer
Clerk, INDU Committee
131 Queen Street, 6th Floor
Ottawa, ON
K1A 0A6

RE: Coalition of Business and Technology Associations submission to INDU with respect to the statutory review of An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)

Dear Committee Members,

We are the Coalition of Business and Technology Associations (the Coalition or the group) a group of organizations representing a broad cross-section of Canadian businesses, from sole proprietorships, to small and medium sized, businesses, to the largest Canadian and multi-national firms. Our member organizations span a wide range of industry sectors and touch almost every corner of the Canadian economy including manufacturing, retail, professional services, entertainment and business software, information, communications and telecommunications, advertising and marketing, publishing, and research and development.[1]

We continue to share the Government's goal of combating spam and malware, and are pleased to provide the following joint comments to the Industry Science and Technology (INDU) Committee with respect to the legislative review of **Canada's Anti-spam Law or CASL.** Several of our coalition members have made separate submissions to the Committee, however they also support this submission as being broadly complementary and consistent with the intent of their own proposals.

We support the Government's objective of ensuring that CASL achieves its goals of reducing spam and malware while encouraging and facilitating the use of electronic means of communication and ecommerce. We have studied CASL and have provided a series of comments both to Industry Canada and to the Canadian Radio-television and Telecommunications Commission ("CRTC" or the "Commission") in the past. Our perspective is informed by the reality of our collective members' attempts to comply with CASL.

We appreciate that Innovation Science and Economic Development Minister Navdeep Bains has taken note of some of our previously stated concerns with respect to CASL and its regulations by delaying the coming into force of the private right of action provisions and prompting a review by this Committee.

We wish to emphasize that this legislation was intended to encourage and facilitate the use of electronic means of communication and ecommerce, a key pillar of any nation's digital economy strategy. Bluntly stated, CASL lacks the balance needed to achieve these goals. The Committee has heard the compliance challenges from many of the organizations that form part of this coalition.

---

[1] The organizations represented by the groups listed above may be referred to as the "Coalition of Business and Technology Associations ("CBTA").

To follow is a list of recommendations for changes to the legislation that would help solve the complexities, unintended consequences and restore the balance that we believe Parliament originally intended.

1. **Narrow the scope of "commercial electronic message" so that CASL regulates only messages the primary purpose of which is offering, advertising or promoting a product, good, service, land, business, investment or gaming opportunity.** Doing so will provide needed to clarity as to when CASL's e-messaging rules apply and ensure that these rules don't apply to purely factual or transactional messages.

2. **Use a principles based approach to implied consent.** The Australian spam law approach to implied consent, referred to as inferred consent, is framed as a principle, rather than being limited to specific conduct, as is the case in CASL. The Australian approach provides a principle that can be applied to any context, rather than prescriptive rules that, by their nature, do not address all potential situations in which it would be reasonable for implied consent to apply. We suggest replacing the definition of implied consent arising from an existing business relationship with the definition of inferred consent from Australia's anti-spam law as follows:

    i. consent that can reasonably be implied from:
    the conduct; and

    ii. the business and other relationships;

    iii. of the individual or organization concerned."

    And further, we suggest that the approach to consent considered valid under PIPEDA or an exiting business relationship will be considered a valid implied consent under CASL.

3. **Ensure that the compliance burden for the sending of a CEM rests with the person or organization that authorized the creation and sending of the message or obtained consent.** The compliance burden should not rest with intermediaries or service providers who assist in the creation and delivery of CEMs.

4. **Eliminate the 2-years and 6-months existing business relationship purge date rules.** If inferred consent is valid consent, it would replace the current implied consent model in section 10(9)(a) which flows from an existing business relationship which lasts 2 years following termination of a written contract or purchase of a product or service, and 6 months following submission of an inquiry or application.

5. **Allow business to business communication.** The business to business exemption in section 3(a)(ii) of the *Electronic Commerce Protection Regulations* does not relieve obligations in many of the circumstances that are necessary for the day to day conduct of electronic commerce. The concept of inferred consent would satisfy this concern if adopted, making the business to business exemption unnecessary going forward and it could be eliminated.

6. **Permit consents to be obtained on an enterprise basis** if consistent with the expectations of the recipient – across a brand, for example – thereby reducing compliance cost and complexity.

7. **Fully exempt all transactional messages,** including those that provide safety information. Section 6 (6) exempts transactional messages from section 6 (1) (a) of the Act (requiring consent) but not from section 6 (1) (b) (the requirement for prescribed information and an unsubscribe mechanism).

8. **Include de-minimis exceptions so that CASL does not apply below a specific threshold,** as it now does, to such things as one on one communications between businesses.

9. **Exempt not-for-profit organizations, such as educational institutions, from the electronic messaging provisions of CASL.**

10. **Revise definition of "electronic address"** by deleting "any similar account" or replacing "any similar account" with "any similar account prescribed by regulation" in order to allow for a careful consideration by the government as to whether CASL should apply to additional forms of digital communication.

11. **Ensure that the "cookies" are not deemed to be computer programs** (as may be the case currently, due to the drafting of section 10(8) of CASL).

12. **Limit the scope of the computer program provisions,** so that they prohibit the installation of malicious software, by amending the sections of CASL dealing with the installation of computer programs to ensure that CASL regulates only malicious software or spyware. Malicious software would be defined as a computer program designed to result in harm, such as to:

    i. disrupt or deny operation of a computer system or other computer program;

    ii. disrupt or deny access to resources of a computer system; or

    iii. collect personal information stored on the computer system;

    iv. that, in each case, is installed without authorization.

    The concept of "without authorization" would be defined to mean "without authorization of the owner or an authorized user of the computer system, including where authorization is obtained with an intent to deceive or defraud or where a computer system is accessed in contravention of an Act of Parliament.

13. **Limit the scope or eliminate the private right of action provision.** Standing to sue under the private right of action should be restricted to those businesses who are directly impacted by spam, spyware and other online threats, including telecommunications companies, online companies and internet service providers.

14. **Broaden the exceptions to the computer program provisions to permit all organizations to counter cyber-threats to networks and software – not just telecommunications service providers.**

15. **Provide additional avenues for guidance to CRTC enforcement staff.** Amend the law to allow the CRTC (the Commission) to provide interpretive guidance and direction to the "designated persons" (CRTC staff) that investigate and enforce CASL, including allowing the CRTC to rule on preliminary questions of interpretation before staff issue a Notice of Violation. As currently written, CASL places in the hands of CRTC staff all significant decisions respecting the interpretation, application and enforcement of the law, with no role for the appointed members of the Commission unless and until an organization, having received a Notice of Violation, makes submissions to the Commission as an "appeal" pursuant to s. 25 of CASL.

16. **Amend the law to allow the Minister or the Governor in Council to issue interpretive guidance and proactive direction to the CRTC with respect to CASL**, using a mechanism similar to s. 8 of the *Telecommunications Act* and s. 7 of the *Broadcasting Act*.

17. **Recommend that regulations be made to introduce additional factors to be taken into account in determining the amount of a penalty**, pursuant to s. 20(3), such as levying heavier penalties against bad actors, and lighter penalties for minor, inadvertent non-compliance by legitimate companies with CASL compliance programs.

Thank you again for the opportunity to comment on this investigation and thank you again for undertaking the review process.

Sincerely,

Scott Smith,
Director, Intellectual Property and Innovation Policy
Canadian Chamber of Commerce
On behalf of the Coalition of Business and Technology Associations