Brief to the House of Commons Standing Committee on Industry, Science and Technology on the review of Canada's Anti-Spam Legislation

October 5, 2017

ESPC
Email Sender & Provider Coalition

1. Introduction

The Email Sender and Provider Coalition ("ESPC") supports the objective of Canada's Anti-Spam Legislation ("CASL") to discourage spam, malware and other threats that undermine trust in the Internet as a medium for the modern economy. However, there are some important challenges with the legislation. As the House of Commons Standing Committee on Industry, Science and Technology conducts its review of CASL, the ESPC appreciates this opportunity to share its unique perspective on these challenges, and to provide recommendations for improvement.

2. Issues and Recommendations

2.1. Transactional and Relationship Messages

Subsection 6(6) of CASL describes several categories of messages commonly referred to as "transactional and relationship" messages, including messages that solely: provide quotes or estimates; facilitate or confirm previously agreed-to transactions; provide product warranty, safety or recall information; provide factual information about an ongoing service, membership, subscription, etc; or, provide information about an employment relationship or related benefit plan. The ESPC understands that this subsection was included in CASL in an effort to address concerns raised by some stakeholders that the law could prevent businesses from sending important transactional and relationship-type messages.[1]

The inclusion of this subsection was misguided and unnecessary, as the messages it describes are, with some limited exceptions, not commercial electronic messages ("CEMs") according to the definition of a CEM in subsection 1(2) of CASL, and therefore not subject to the Act. However, this subsection has been interpreted by Canadian Radio-television and Telecommunications Commission ("CRTC") staff to mean that CASL applies to all messages referred to in subsection 6(6) – most of which are otherwise clearly excluded. This creates significant confusion and challenges for senders. Most importantly, based on the CRTC's apparent view that subsection 6(6) messages must contain an unsubscribe mechanism, senders struggle to determine how to give effect to this requirement, given that consent for these messages is not required in the first place. Further, it is possible that the CRTC staff's interpretation of subsection 6(6) results in an unconstitutional application of CASL, as it captures messages that are not sent in the course of commercial activity, and therefore appear to fall outside of the federal trade and commerce power under section 91(2) of the *Constitution Act, 1867*.

Recommendation: Subsection 6(6) should be removed from the Act.

2.2. Cookies

Cookies are extremely important to many features of the Internet. Cookies are merely text files that record information in an Internet browser, and are not computer programs according to the definition in CASL.[2] However, a reference to cookies was included in subsection 10(8) of CASL in a misguided effort to provide greater certainty that CASL would not apply, despite assurances that this was unnecessary.[3] CRTC staff now rely

---

[1] See, for example, INDU, Evidence, 2nd Session, 40th Parliament, 16 June 2009, 1641 (Mr. Bernard Courtois, President and Chief Executive Officer, Information Technology Association of Canada). The first iteration of Bill C-27, as introduced at first reading, did not include this subsection: http://www.parl.ca/Content/Bills/402/Government/C-27/C-27_1/C-27_1.PDF.

[2] CASL references the following definition found in subs. 342.1(2) of the *Criminal Code*: "*data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.*

[3] See, for example, INDU, Evidence, 2nd Session, 40th Parliament, 11 June 2009, 1620 (Professor Michael Geist): "*The issue of cookies has come up in discussion, not so much as to whether it's spam but as to whether it's a computer program that's being inserted on someone's personal computer. I think the consensus is that it is not. If you take a look at standard definitions for what a cookie is, it is simply a text file that is inserted onto a personal computer, at the user's request; they have the ability not to have it there*"; and INDU, Evidence, 2nd Session, 40th Parliament, 30 September 2009, 1615 (Mrs.

on this subsection for the position that cookies *are, in fact* computer programs, creating significant confusion, risk, and the potential for CASL to completely disrupt how the Internet functions.[4] As a result, the CRTC, and potentially courts through the private right of action, become the arbiters of what it means for a person's conduct to be such that it is "*reasonable to believe*" that they consent to the use of a cookie. This could undermine guidance from the Privacy Commissioner of Canada, developed over years of careful consideration, on how the *Personal Information Protection and Electronic Documents Act* applies to cookies.[5] This is despite the fact that CASL was never intended to, and should not, apply to cookies.

Recommendation: The reference to cookies should be removed from subsection 10(8) of the Act. For greater certainty, CASL should also be amended to clarify that the definition of a computer program does not include a cookie.

2.3. Identification of Senders in CEMs

CASL contemplates that one person may "send" a CEM "on behalf of" another person.[6] However, there is confusion about what it means for one person to send a CEM on behalf of another person. CRTC staff have interpreted CASL to mean that some service providers, such as Email Service Providers ("ESPs"), who assist senders in creating and delivering email campaigns send "on behalf of" their clients. According to this interpretation, such service providers must be identified as the sender of a CEM. However, ESPs and other service providers are expected to assist senders in creating a seamless email experience for recipients, where advertisers are clearly identified as the sender, and accountable for the messages they send. Referring to an ESP as the sender of an advertiser's message is arbitrary and confusing for senders, service providers, and consumers, and does nothing to address problems associated with spam.

Recommendation: CASL should be amended to clarify that the person who "sends" for the purpose of CASL is the person who purports to have a consent relationship with the recipient, or, where consent is not required, the person who seeks to engage in commercial activity with the recipient. For example, the ESPC suggests a new subsection such as the following be added to section 6: *"6(9) For the purpose of subsection (2), a person who sent the message is the person who alleges that they have consent to send the message, or, if consent is not required to send the message, the person who encourages the person to whom the message is sent to participate in commercial activity."*

2.4. Administrative Monetary Penalties

At up to $10 million per violation, the maximum administrative monetary penalties under CASL are unnecessarily and disproportionally high, and the factors to be taken into account when determining the amount of

---

Nathalie Clark, General Counsel and Corporate Secretary, Canadian Bankers Association): "*We would like some clarification that tools such as "cookies" are not included in the definition of "computer program" set out in the bill.*"

[4] Canadian Radio-television and Telecommunications Commission, *Canada's Anti-Spam Legislation Requirements for Installing Computer Programs*.

[5] See, for example, Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, December 2015. Similar guidance has existed as far back as June, 2012.

[6] For example, subsection 6(2) states as follows: "*The message must be in a form that conforms to the prescribed requirements and must…..set out prescribed information that identifies the person who sent the message* ***and the person — if different — on whose behalf it is sent****…*[and] *set out information enabling the person to whom the message is sent to readily contact one of the persons referred to in paragraph (a)* [emphasis added]".

a penalty provide the CRTC with no meaningful guidance. This creates an inordinate amount of risk for senders, particularly given the many areas that lack clarity under CASL.

The context for the enforcement of anti-spam legislation has changed significantly since CASL was first conceived in 2005. The amount of spam that reaches inboxes has been dramatically reduced with improved filtering technology, industry best practices, blacklists and market forces. Organizations engaging in legitimate business have very little incentive to send spam, even in the absence of laws such as CASL.

To put CASL in perspective, the *Telecommunications Act* provides maximum penalties of $15,000 for a violation of the Unsolicited Telecommunications Rules ("UTR").[7] It is nonsensical that the penalties for spam and related activities should be so much higher than for telemarketing.

Recommendation: The ESPC recommends that CASL be revised as follows:

- **Maximum penalties should be brought in line with the penalties for violations of the UTR under the *Telecommunications Act*; i.e., a maximum penalty of $15,000 for corporations.**
- **Maximum penalties should be more explicitly linked to a person's history of violations. Specifically, the ESPC recommends that the maximum penalty should be $5,000 for a first violation, $10,000 for a second violation, and $15,000 for a third and any subsequent violation.**
- **For violations of section 6, penalties should be applied on a campaign level, and not for each individual email sent within a given campaign.**
- **The intent of a person should be an explicit factor in determining whether penalty should be applied. An unintentional violation (e.g., a mistake), should result in a warning, and not a penalty. A penalty should only be imposed if a violation is repeated after a formal warning is received.**

2.5. Private Right of Action

The private right of action in CASL allows any person affected by an alleged violation to sue for actual damages, as well as authorizing a court to award statutory damages, in some cases up to $1 million per violation, with no requirement to demonstrate harm. If the private right of action were to come into effect, this would strongly encourage plaintiffs to seek out defendants who have substantial assets that are accessible through Canadian courts. This would likely include businesses who are found to have inadvertently violated CASL, either by committing a technical error, or due to a lack of clarity found in many provisions of the law.

To date, there is no evidence to suggest that a private right of action is necessary. The CRTC's extensive enforcement powers and the ability to impose administrative monetary penalties create very strong incentives for businesses to comply with the legislation (incentives which would continue to exist even if the ESPC's recommendations for reducing maximum penalties are implemented). Further, the very limited amount of spam-related enforcement action over the past three years demonstrates that the CRTC is far from overwhelmed with attempting to enforce CASL against spammers.

Recommendation: The ESPC recommends that the private right of action be removed from CASL. Alternatively, if the government believes that a private right of action in CASL is necessary, the authority to award statutory damages should be removed so that an award cannot be made without proof of tangible harm.

[7] *Telecommunications Act*, SC 1993, c 38, s. 72.01.

Summary of Recommendations

1. **Subsection 6(6) should be removed from the Act.**

2. **The reference to cookies should be removed from subsection 10(8) of the Act. For greater certainty, CASL should also be amended to clarify that the definition of a computer program does not include a cookie.**

3. **CASL should be amended to clarify that the person who "sends" for the purpose of CASL is the person who purports to have a consent relationship with the recipient, or, where consent is not required, the person who seeks to engage in commercial activity with the recipient. For example, the ESPC suggests a new subsection such as the following be added to section 6: "*6(9) For the purpose of subsection (2), a person who sent the message is the person who alleges that they have consent to send the message, or, if consent is not required to send the message, the person who encourages the person to whom the message is sent to participate in commercial activity.*"**

4. **The ESPC recommends that CASL be revised as follows:**
   - **Maximum penalties should be brought in line with the penalties for violations of the UTR under the *Telecommunications Act*; i.e., a maximum penalty of $15,000 for corporations.**
   - **Maximum penalties should be more explicitly linked to a person's history of violations. Specifically, the ESPC recommends that the maximum penalty should be $5,000 for a first violation, $10,000 for a second violation, and $15,000 for a third and any subsequent violation.**
   - **For violations of section 6, penalties should be applied on a campaign level, and not for each individual email sent within a given campaign.**
   - **The intent of a person should be an explicit factor in determining whether penalty should be applied. An unintentional violation (e.g., a mistake), should result in a warning, and not a penalty. A penalty should only be imposed if a violation is repeated after a formal warning is received.**

5. **The ESPC recommends that the private right of action be removed from CASL. Alternatively, if the government believes that a private right of action in CASL is necessary, the authority to award statutory damages should be removed so that an award cannot be made without proof of tangible harm.**

About the ESPC

Formed in 2002, the Email Sender & Provider Coalition ("ESPC") is an industry association representing many of the largest technology providers in the email industry, including Email Service Providers ("ESPs"), Mail Transfer Agents ("MTAs"), application and solution developers and deliverability solution providers. The ESPC's 42 members assist in delivering a significant proportion of email throughout North America and around the world. Although the ESPC's membership consists largely of U.S.-based companies, many of its members send email to Canadians on behalf of business customers located in Canada and the U.S.

Keenly aware of the harmful impacts of spam and other threats, the ESPC has helped lead in the prevention of email abuse since its inception, becoming one of the first industry associations to develop and advocate for email best practices that focus on consumer consent.[8]

ESPC members have collectively delivered many billions of emails and other electronic messages in the three years since CASL has been in effect. During that time, the ESPC has heard from its members on the most significant challenges they face, and appreciates this opportunity to share its unique and important perspective with members of the House of Commons Standing Committee on Industry, Science and Technology on the review of CASL.

[8] See, for example, *ESPC Best Practices Guide*, Feb. 2016.