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

Table of Contents

ESPC
Email Sender & Provider Coalition

1. Executive Summary

The Email Sender and Provider Coalition ("ESPC") asks that the House of Commons Standing Committee on Industry, Science and Technology consider the following five recommendations for improving Canada's Anti-Spam Legislation ("CASL"):

1. **Issue**: Subsection 6(6) was included in CASL in a misguided effort to provide greater certainty that the law would not prevent businesses from sending important transactional and relationship-type messages. However, this subsection is unnecessary, poorly written, and has been interpreted by the Canadian Radio-television and Telecommunications Commission ("CRTC") to mean that CASL applies to many messages that are otherwise clearly excluded according to the definition of a "commercial electronic message". This has resulted in significant confusion and challenges for senders, and is possibly unconstitutional.

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

2. **Issue**: 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. However, a reference to cookies was included in CASL in a misguided effort to provide greater certainty that CASL would not apply. As a result, the CRTC has taken the position that cookies are computer programs, creating significant confusion, risk, and the potential for CASL to completely disrupt how the Internet functions.

   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.

3. **Issue**: CASL creates confusion about what it means for one person to "send" a CEM "on behalf of" another person. As a result, the CRTC has taken the position that some service providers who assist senders in creating and delivering email campaigns send "on behalf of" their clients. This interpretation is arbitrary and confusing for senders, service providers, and consumers.

   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.*"

4. **Issue**: 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 a penalty provide the CRTC with no meaningful guidance.

Recommendation: CASL should be amended to reduce the maximum penalties under CASL to $15,000 per campaign, and to impose more specific conditions on how penalties are determined.

5. **Issue**: The private right of action is unnecessary, serving only to compound the unpredictability and legal risk under CASL.

   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.

2. Introduction

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.[1] The 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.

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 (the "Committee") on the review of CASL.

The ESPC does not propose a dramatic overhaul of CASL. Rather, the ESPC seeks to bring the following issues to the attention of the Committee, which are of the highest priority to its members:

- the application of CASL to transactional and relationship messages;
- the application of CASL to cookies;
- which parties must be identified in a commercial electronic message ("CEM");
- the administrative monetary penalty regime; and
- the private right of action.

Each of these issues are described in detail, following which concrete recommendations for improving CASL are provided. The ESPC would like to thank the Committee in advance for taking the time to review this written brief.

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

3. CASL: Challenges and Recommendations

3.1. Transactional and Relationship Messages

3.1.1. Relationship Between Subsections 1(2) and 6(6)

A commercial electronic message ("CEM") is defined in CASL as a message that "*it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity.*"[2] This definition is crucial to determining when the Act applies to electronic messaging activities.

Subsection 6(6) of CASL states that consent is not required for a CEM that solely

> *(a) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land, if the quote or estimate was requested by the person to whom the message is sent;*
>
> *(b) facilitates, completes or confirms a commercial transaction that the person to whom the message is sent previously agreed to enter into with the person who sent the message or the person — if different — on whose behalf it is sent;*
>
> *(c) provides warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased;*
>
> *(d) provides notification of factual information about*
>
> > *(i) the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or the person — if different — on whose behalf it is sent, or*
> >
> > *(ii) the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent;*
>
> *(e) provides information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved, is currently participating or is currently enrolled;*
>
> *(f) delivers a product, goods or a service, including product updates or upgrades, that the person to whom the message is sent is entitled to receive under the terms of a transaction*

[2] *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*, SC 2010, c 23 ("CASL"), subs. 1(2).

that they have previously entered into with the person who sent the message or the person — if different — on whose behalf it is sent

The types of messages described in subsection 6(6) are commonly referred to as "transactional and relationship" messages. Although consent is not required for these messages, the identification and unsubscribe requirements found elsewhere in sections 6 and 11 do apply.

It is the ESPC's understanding that subsection 6(6) was added to the bill that created CASL to address concerns raised by some stakeholders that the legislation might prevent companies from sending important information by email, including such things as product safety, warranty, and recall information.[3] However, such concerns were unfounded, because, with the possible exception of paragraph (a) (a message that provides a quote or estimate), a message that solely performs any of the functions described in subsection 6(6) is not a CEM according to the definition in subsection 1(2).

There is one way to interpret subsection 6(6) so that it is logically consistent with the rest of the Act. That is, subsection 6(6) applies only if a message: 1) is a type described in one of the paragraphs in subsection 6(6); and 2) meets the definition of a CEM in subsection 1(2).

Unfortunately, it seems that Canadian Radio-television and Telecommunications Commission ("CRTC") staff have taken a different approach, indicating that any message described in subsection 6(6) is deemed to be a CEM, regardless of whether it also meets the definition of a CEM in subsection 1(2). Although it does not appear that the CRTC has put this in writing, this interpretation was confirmed in person to the ESPC during a meeting with the ESPC in 2011, and subsequently in person to the ESPC's Canadian counsel on multiple occasions. Thus, according to the CRTC, although consent is not required for subsection 6(6) messages, all such messages must include both prescribed identification information as well as an unsubscribe mechanism.

3.1.2. Problems With the CRTC's Interpretation

The CRTC's interpretation of subsection 6(6) poses significant challenges for senders. Although it is generally not difficult to include the identification information required by CASL and prescribed in regulation, the requirement to include an unsubscribe mechanism in transactional and relationship messages is highly problematic.

First, this often requires a significant change in business practices. Senders treat transactional and relationship messages differently than marketing communications, often using different sending

[3] 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. Rather, this first appeared in the version as amended by INDU (then subsection 6(5.1)): http://www.parl.ca/Content/Bills/402/Government/C-27/C-27_2/C-27_2.PDF

processes and platforms. In many cases it is not even possible to include an unsubscribe mechanism without significant effort and cost.

Second, if consent is not required for messages described in subsection 6(6), it is unclear how a sender is supposed to give effect to an unsubscribe mechanism included in such a message. For example, it is unclear whether the recipient needs to be able to unsubscribe from the transactional and relationship messages containing the unsubscribe mechanism, or if the mechanism is only required to apply to promotional communications. To interpret CASL so that senders are required to allow recipients to unsubscribe from transactional and relationship messages could make it difficult for companies to send important information by email, creating the problem that the government attempted to solve with subsection 6(6) in the first place.

Senders seeking to comply with the CRTC's interpretation of subsection 6(6) have essentially three options: 1) provide an unsubscribe mechanism in all messages, including transactional and relationship messages, that allows recipients to unsubscribe from all categories of messages; 2) provide an unsubscribe mechanism in all messages, including transactional and relationship messages, that only allows the recipient to unsubscribe from messages that are CEMs according to the definition in subsection 1(2) of CASL; or, 3) ignore the CRTC's interpretation of subsection 6(6), and do not include an unsubscribe mechanism in transactional and relationship messages.

Regardless of the approach taken in an effort to comply with CASL, the inclusion of subsection 6(6) in CASL creates significant and unnecessary risk, confusion, and cost for senders.

It is worth noting that some of the problems caused by subsection 6(6) were at least partially resolved with exceptions provided in regulations,[4] which were finalized over two years after CASL received royal assent. For example, these regulations exclude any CEM sent to satisfy a legal obligation, which likely includes things like e-receipts, and warranty, safety and recall information. There are many categories of messages that are potentially addressed by both subsection 6(6) and exceptions defined in regulations, which makes the law even more confusing.

3.1.3. Constitutionality

It is possible that the CRTC's interpretation of subsection 6(6) is unconstitutional. CASL is based on the federal government's authority to regulate trade and commerce under section 91(2) of the *Constitution Act, 1867*.[5] For the most part, it appears that the government was careful to draft CASL in a way that it only purports to apply to activities conducted in the course of *commercial activity*.[6] However, according to the CRTC's interpretation of 6(6), it applies to activities that seem to fall more squarely within the domain of the provinces. For example, paragraphs (c), (d) and (e) deal with consumer

protection, contracts, and employment relationships, respectively, all areas of regulation that generally fall to the provinces under section 92 of the *Constitution Act*. The CRTC's interpretation therefore appears to directly interfere with the ability of senders to meet their obligations on provincial regulatory matters.

As noted above, the only scenario in which subsection 6(6) appears to serve any purpose is with respect to quotes and estimates. However, regulations finalized after CASL was passed provide a complete exception for any CEM "*that is sent in response to a request, inquiry or complaint or is otherwise solicited by the person to whom the message is sent*".[7] This exception applies to any message described in paragraph 6(6)(a), meaning that subsection 6(6) serves no purpose at all.

3.1.4. Recommendation

The ESPC recommends that subsection 6(6) be removed from CASL. It serves no purpose and its existence in the Act is confusing to those companies to whom it purports to regulate.

3.1. Cookies

3.1.1. Cookies are Not Computer Programs

Cookies[8] are crucial to many important and common features of the Internet. Among other things, they: enable websites to remember authentication information and personal settings; facilitate the "shopping cart" function on e-commerce sites; provide website owners with important analytical information about website use; and allow websites to provide Internet users with content and advertisements that are tailored to the specific personal interests of each user in an anonymous manner. Unfortunately, the reference to cookies in subsection 10(8) results in significant legal risk for businesses that use cookies, and creates the possibility that the computer program rules under CASL could completely disrupt the ability of businesses to continue to use cookies for many important purposes.

To define a "computer program", CASL references the following definition in the *Criminal Code*: "*data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function*."[9] Cookies are not computer programs according to this definition. As a simple text file used to store information on a web browser, a cookie is akin to the contents of an email or Word document. Just like an email or a Word document, cookies are not "executable," and therefore cannot cause a computer program to perform a function. They are merely text files that contain information.

[8] The term "cookies" is used here specifically in reference to Hypertext Transfer Protocol (HTTP) cookies.

[9] *Criminal Code*, RSC 1985, c C-46, subs. 342.1(2).

During the Committee's review of the bill that created CASL, some stakeholders raised concerns about how CASL might apply to cookies. Despite assurances that the definition of a computer program under the *Criminal Code* does not include cookies,[10] some stakeholders nonetheless pushed for greater certainty.[11] As with subsection 6(6), the government responded with a misguided effort to provide clarity by adding an explicit reference to cookies. Subsection 10(8) provides that

> *A person is considered to expressly consent to the installation of a computer program if…the program is…a cookie…and…the person's conduct is such that it is reasonable to believe that they consent to the program's installation.*

This reference to cookies was a mistake because it failed to categorically exclude cookies from the application of CASL. As with subsection 6(6), the attempt to provide further certainty had the opposite effect, creating the possibility that CASL could apply to activities that were otherwise excluded.

There are at least two possible interpretations of subsection 10(8). The only reasonable interpretation is that subsection 10(8) applies if a cookie also happens to be a computer program according to the *Criminal Code* definition, because subsection 10(8) cannot alter the *Criminal Code* definition. And, because it is impossible for cookies to meet this definition, the reference to cookies in subsection 10(8) is redundant.

However, the CRTC has taken the position that cookies are computer programs for the purpose of CASL.[12] In what appears to be an attempt to shoehorn cookies into the Act, the CRTC created the following definition: "*Cookies are **non executable** computer programs that cannot carry viruses and install malware*" [emphasis added].

Given that a computer program means "*data representing instructions or statements that, **when executed in a computer system**, causes the computer system to perform a function*" [emphasis added], the CRTC's cookie definition is inherently illogical and contradictory, as there can be no such thing as a "non-executable" computer program. The problems with this approach are addressed below.

---

[10] 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. It doesn't run anything, and if you take a look at the definition of software programs referred to here, they require something more than just being a text file itself.*"

[11] See, for example, INDU, Evidence, 2nd Session, 40th Parliament, 30 September 2009, 1615 (Mrs. 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.*"

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

3.1.2. How Cookies Are Regulated

Cookies are regulated in Canada through a mix of industry self-regulation and privacy legislation. To the extent that a cookie involves the collection, use or disclosure of personal information (in the course of commercial activity), the *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[13] applies. The Office of the Privacy Commissioner of Canada ("OPC") has stated that PIPEDA applies to the use of cookies for such things as online behavioural advertising ("OBA").[14] After extensive consultation and careful consideration over many years, the OPC concluded that it is reasonable for organizations to rely on a form of opt-out/implied consent to use cookies for OBA purposes so long as certain conditions are met.[15] Recognizing the undesirable consequences of an overly rigid and prescriptive approach to cookies, the OPC stated that

> *constant notifications to users about cookies and blocked access to ad-supported sites will frustrate users and potentially create fatigue or a backlash against efforts to protect their personal information.*[16]

As a broad, principle-based regime, PIPEDA provides a flexible standard that allows the OPC to continue to adapt its position on cookies with changes in technologies and business practices.

Cookies used for OBA purposes are also addressed by the *Self-Regulatory Principles for Online Behavioral Advertising*,[17] a set of principles developed through collaboration among various marketing and advertising trade groups (the "Digital Advertising Alliance, or "DAA"), in consultation with other stakeholders. These *Self-Regulatory Principles* are augmented by a consumer opt-out mechanism developed by the Network Advertising Initiative ("NAI").[18] First applied in the U.S., the *Self-Regulatory Principles* have since been adapted for use in Canada by the Digital Advertising Alliance of Canada ("DAAC"), and are intended to assist organizations in meeting the OPC's conditions when using cookies for OBA.[19]

The *Self-Regulatory Principles* have evolved to keep pace with advances in technology and the Internet advertising industry, as the DAA has developed guidance on the application of *Self-Regulatory*

---

[13] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

[14] Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, December 2015, ("*Policy Position on OBA*"). Similar guidance has existed as far back as June, 2012.

[15] *Ibid.*

[16] *Ibid.*

[17] Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising*.

[18] Network Advertising Initiative Consumer Opt-Out.

[19] https://youradchoices.ca/

Principles to multi-site data[20], the mobile environment[21], and, most recently, to data used across devices[22].

Of course, PIPEDA also applies to cookies used for purposes other than OBA that involve personal information. The point is, where cookies raise privacy concerns, PIPEDA provides a flexible regulatory framework, overseen by the OPC, which has almost two decades of experience applying PIPEDA to cookies and related technologies.

3.1.3. Problems With the CRTC's Interpretation

The CRTC appears to take the position that CASL applies to all cookies. If CASL applies, then consent obtained in accordance with the strict requirements of the legislation is required to set a cookie on a web browser. Consent to the use of a cookie can also be "deemed" to exist where "*the person's conduct is such that it is reasonable to believe that they consent to the program's installation.*"

To require CASL-compliant express consent for the use of cookies directly contradicts the OPC's stated desire to avoid "*constant notifications to users about cookies and blocked access to ad-supported sites.*" This would result in dramatic and undesirable changes to how the Internet functions.

That CASL allows consent to be "deemed" for the use of cookies provides no comfort. This is because 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.

The ESPC strongly believes the CRTC's interpretation that CASL applies to cookies is incorrect. However, the CRTC still has the ability to bring enforcement actions, requiring companies to endure significant time and costs to defend a CRTC action. Also, the private right of action could allow plaintiffs to bring lawsuits seeking $1 million in statutory damages (i.e., no need to demonstrate harm) per alleged violation on the basis that a cookie is "unreasonable".

This undermines OPC regulatory guidance and industry self-regulation on cookies, developed over several years through extensive consideration and collaboration, which ensures that the privacy interests of end-users are a central factor in how cookies are used in a continuously evolving Internet.

For the government to so significantly change the rules on cookies should be a deliberate policy decision, made after extensive consultation and careful consideration. However, the CRTC's interpretation of CASL's application to cookies is the result of a mistake, as there is no evidence that

---

[20] Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*.

[21] Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment*.

[22] Digital Advertising Alliance, *Application of the DAA Principles of Transparency and Control to Data Used Across Devices*.

cookies have ever been considered a problem to be addressed by anti-spam legislation. For example, the 2005 Report of Task Force on Spam specifically acknowledged that cookies are addressed by PIPEDA, and made no reference to cookies in its recommendation.[23] Further, cookies were never raised during the Committee's review of Bills C-27 or C-28 as problems to be addressed under those bills.

3.1.4. Recommendation

Cookies are not computer programs for the purpose of CASL. Because it appears that the CRTC's claim that cookies are computer programs is derived from the reference to cookies in subsection 10(8), it should be sufficient to merely remove the reference to cookies in this subsection.

However, the ESPC is concerned that this may not be sufficiently clear, and the that CRTC may persist in its view that cookies are "non-executable" computer programs despite an amendment to subsection 10(8). The ESPC therefore recommends that

- Subsection 10(8) be revised to remove the reference to cookies; and
- Subsection 1(1) of CASL specify that cookies are not computer programs by revising the definition of a computer program as follows: "*computer program has the same meaning as in* subsection 342.1(2) *of the* Criminal Code, ***and does not include cookies***".

3.2. Identification of Senders in CEMs

3.2.1. Uncertainty in CASL

CASL contemplates that one person may "send" a CEM "on behalf of" another person. There are several references to a message being sent on behalf of another person in the Act, including the following:

- Subsection 6(2): "*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]".
- Subsection 6(5): "*This section does not apply to a commercial electronic message….that is* ***sent by or on behalf of*** *an individual to another individual with whom they have a personal or family relationship* [emphasis added]".
- Subsection 11(1): "*The unsubscribe mechanism referred to in paragraph 6(2)(c) must….enable the person to whom the commercial electronic message is sent to indicate, at no cost to them, the*

[23] Industry Canada, *Stopping Spam: Creating a Stronger, Safer Internet, Report of the Task Force on Spam*, May 2005 ("*Report of the Task Force on Spam*").

> *wish to no longer receive any commercial electronic messages, or any specified class of such messages,* ***from the person who sent the message or the person — if different — on whose behalf the message is sent*** [emphasis added]."

Regulations promulgated by the CRTC set out the prescribed identifying information that must be included in CEMs. These regulations state that "*if the message is sent on behalf of another person*", it must include "*the name by which the person on whose behalf the message is sent carries on business, if different from their name, if not, the name of the person on whose behalf the message is sent*", as well as "*a statement indicating which person is sending the message and which person on whose behalf the message is sent*".[24]

The question of what it means for one person to send on behalf of another has direct implications for who needs to be identified as the person who "sends", and under what circumstances a person needs to be identified as the person "on whose behalf" the message is sent.

The confusion and uncertainty on this issue stems largely from the fact that CASL does not define what it means for a person to "send" a CEM under CASL. The preferable interpretation is to focus on the person who has or purports to have a consent relationship with the recipient, and who ultimately benefits from the message; i.e., the person with whom the recipient is encouraged to engage in commercial activity. The ESPC requested in 2011 that the government pass a regulation that reinforces this approach, which it did not do.

The ESPC subsequently urged the CRTC to adopt an interpretation that focusses on the consent relationship and the advertiser in a message. It appears that CRTC staff may have attempted to accommodate concerns expressed by the ESPC, to a limited extent, with the following guidance:

> *…not every person who is involved in the sending of a CEM must be identified. Rather, only the persons who play a material role in the content of the CEM and/or the choice of the recipients must be identified. For example, an email service provider that provides a service to its clients to send emails, where the email service provider has no input on the content of the message, nor on the recipient list, does not need to be identified in the CEMs sent by clients using its service. Bear in mind however, that though the email service provider does not need to be identified in this scenario, it still shares its responsibilities with its clients in terms of ensuring that the CEMs are sent with valid consent (either express or implied) and contain an unsubscribe mechanism. Both the email service provider and its clients are sending, causing or permitting to send CEMs, and as such, they both have obligations under CASL.*

[24] *Electronic Commerce Protection Regulations (CRTC),* SOR/2012-36, paras. 2(b),(c) ("*CRTC Regulations*").

This guidance implies that an ESP who "*plays a material role in the content of the CEM and/or the choice of the recipients*" is the person who sends a CEM on behalf of their client for the purpose of CASL. To understand why this interpretation is problematic, it is helpful describe what ESPs do.

3.2.2. What Email Service Providers Do

Successfully delivering large volumes of email to end-users requires a significant investment in specialized knowledge and technology. While some senders may choose to invest the necessary resources in-house, most choose to outsource this non-core business function to an ESP who can perform this task in a more efficient and effective manner.

ESPs provide the necessary infrastructure and knowledge that enable the development and delivery of email campaigns for clients. Although specific offerings vary between providers, the following are a general set of core services common to many ESPs, any of which can be provided on a self-service or full service basis, or a combination thereof.

- Email templates: ESPs provide custom email templates that include prescribed information necessary to comply with legislation and industry best practices.
- List management: ESPs provide tools that allow clients to manage lists, which includes tools that facilitate importing lists, obtaining consent and adding new subscribers, processing unsubscribe requests from subscribers, and removing subscribers who are no longer active.
- Segmentation: ESPs assist clients in identifying and creating segments of subscribers, allowing clients to effectively target marketing campaigns and transactional messages.
- Personalization: Some ESPs offer technologies that enable clients to personalize the content and timing of email messages to better appeal to the interests of each individual recipient.
- Infrastructure: ESPs provide specialized servers that enable large volumes of email to be sent.
- Deliverability: A core function of all ESPs, deliverability refers to the ability to ensure that emails are delivered to the inbox of intended recipients. Deliverability is maximized by analyzing the content of emails for content likely to be captured by spam filters, minimizing complaint rates and bounces, and maintaining domain reputation.
- Analytics: ESPs provide detailed statistics on each email sent by a client, including deliverability rates, open rates and click-through rates.

The goal throughout the process of developing and delivering an email campaign is to provide a seamless email experience, and, as far as the consumer is concerned, the advertiser is the sender, not the ESP, the digital agency, advertising agency, nor any other person involved in the process. As a provider of volume email delivery services, the ESP is no more the sender of an email than Canada Post is the sender of direct mail by providing direct mail services.

3.2.1. Problems With the CRTC's Interpretation

There are several problems with the CRTC's interpretation of who needs to be identified in a CEM.

First, advertisers should not be required to identify their ESPs (or other service providers) in the CEMs that they send. Email advertising is intended to build brand recognition and a positive relationship between the consumer and the advertiser, and recipients do not care which service provider may have assisted the advertiser in sending the message. Further, identifying an ESP provides more confusion than clarification, and in no way assists in the prevention of spam.

Second, the CRTC's guidance is arbitrary and illogical, as it makes no sense that the deciding factor in requiring an ESP to be identified is whether the ESP plays a role in the choice of content and/or recipients. In other words, it is unclear why recipients need to know who the ESP is merely because they perform or assist in performing either of these functions.

Third, the CRTC's guidance appears to capture more than just ESPs. There are often multiple service providers involved in the creation and delivery of an email marketing campaign, all of whom can play some role in assisting the client in the choice of content and/or recipients. This can include advertising agencies, digital agencies, and other providers and consultants, in addition to the ESP. According to the CRTC's guidance, an advertiser may need to identify all of these parties as the person (or person(s)) who send on behalf of the client advertiser. This is an absurd result.

Moreover, it is more than just a theoretical problem. At least one ESPC member has been informed by CRTC staff that, in the CRTC staff's opinion, certain CEMs sent through that member's platform should indicate that the messages are "sent" by the member "on behalf of" the member's clients. CRTC staff stated that this requirement applies when clients use the member's personalization technologies, which enable clients to generate and send email campaigns that are personalized to recipients utilizing customized email content and email list segments. To be clear, the member in this instance is merely a provider of technology services, which includes systems for sending and for personalizing emails, both of which are used and controlled by the client. The ESPC member has no substantive control over or input on the choice of content or recipients. Further, it is the client's products and services that are advertised, and recipients consent to receiving CEMs from the client, not the member.

3.2.1. Recommendation

One of the key objectives of anti-spam legislation is to ensure that advertisers are accountable for messages they send, as it is the advertisers who are ultimately responsible for both the choice of content and recipients of messages, regardless of who assists with those tasks. Advertisers procure the services of ESPs to assist in the delivery of advertisements that appear as though they are sent from the advertiser in a clean and seamless manner.

It is notable that a "*sender*" under the U.S. CAN-SPAM Act is a person who "*initiates*" a message, and "*and whose product, service, or Internet web site is advertised or promoted by the message*." Thus, a

sender is a person who: 1) either sends the message (i.e., clicks a "send" button), or procures someone to do this on their behalf; and 2) is the advertiser. This definition, which clarifies that ESPs and other service providers are not senders under the legislation, is based on sound reasoning and policy.

Because CASL generally requires senders to have prior consent to send CEMs, unlike the U.S. CAN-SPAM Act, there is an even simpler solution for assigning responsibility for who needs to be identified in a CEM. For the purposes of the identification requirements, the person who "sends" a CEM should be the person who has, or purports to have, consent to send the CEM. Where messages are sent without consent because consent is not required, the person who sends should be the person whose products or services are advertised.[25] This achieves the objective of requiring identification in the first place: to ensure accountability for the person claiming to have the consent relationship, and who bears the most responsibility for having caused the message to be sent in the first place. More importantly, it avoids the confusion resulting from the CRTC's interpretation.

This approach also accounts for "list rental"-type scenarios. In this context, a list rental refers to a scenario where a list owner, such as a newsletter, magazine or other publisher, has compiled a list of email addresses, with the objective of sending content on behalf of other advertisers. In this case, the list owner is the person who sends because they have the consent relationship with the recipients. It is the ESPC's view that this is in fact the type of scenario that the government had contemplated when it included a reference to one person sending "on behalf of" another person.

The ESPC therefore recommends that a new subsection be included in CASL, such as the following:

Person who sent

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.

3.3. Administrative Monetary Penalties

3.3.1. Changing Context for Enforcement

CASL is likely the most prescriptive regulatory law in Canada. The enforcement regime in CASL is based on recommendations by the Task Force on Spam to create new civil and strict-liability offences to address spam and related threats, and to support those offences with meaningful statutory penalties.[26]

[25] For example, section 4 of the *Electronic Commerce Protection Regulations*, SOR/2013-221, states that consent is not required for the first email sent as the result of a referral where certain conditions are met.

[26] *Report of the Task Force on Spam*, p. 4.

It is important to understand the context within which the Task Force on Spam made its recommendations, and how the nature of spam and related issues have changed since 2005. In particular, the Task Force Report reflects the shared frustration among a group of stakeholders attempting to address a specific problem, which, over a decade later, has been largely addressed through a combination of technology and market forces.

In providing for virtually unlimited penalties and statutory damages in CASL, policymakers responded to a period of time from the late 1990s to early 2000s during which the use of spam and malware appeared to be a very lucrative enterprise. High-profile lawsuits under the U.S. CAN-SPAM Act suggested that certain spammers in North American could easily earn many millions of dollars per year.[27] This led to an assumption that anti-spam legislation requires astronomical penalties to be effective.

For example, a government official gave the following statement to the Committee in response to concerns that the penalties in CASL were too high:

> *…we can tell you about international cases, such as a case going on in Australia, for example, where two brothers had one very small shop and a few computers. They had this spam outfit going where they were changing the labels on herbal remedies to call them penis enlargers and sending them out all over the world. In a matter of three and a half months, these guys raked in over $3.5 million of net profit.*
>
> *So the reason we need penalties in this amount is to address the business model. These guys are making a ton of money, and if we throw a $15,000 fine at them, they'll pay it and go merrily about their business and just keeping doing it and doing it. We have to go after their finances.*[28]

However, the nature of the problems addressed by CASL have changed since 2005. Even by 2008, research suggested that the profitability of spam had significantly decreased.[29]

Reputable data demonstrates that the proportion of email considered to be spam fell from 85% to 56% globally between 2012 and 2015.[30] Much more importantly though, the amount of spam reaching consumer inboxes has been dramatically reduced through a combination of improved filtering technology, blacklists and market forces.

---

[27] For example, see: Dan Tynan and PC World, "Will the Real Spam King Please Stand Up?", *abcNEWS*, Oct. 13, 2008.

[28] INDU, Evidence, 2nd Session, 40th Parliament, 7 October 2009, 1640 (Mr. Andre Leduc, Policy Analyst, Industry Canada).

[29] Mike Masnick, "Researchers Become Spammers To See How Successful Spam Is", *techdirt*, Nov. 10, 2008.

[30] Return Path, 2012 *Return Path Sender Score Benchmark Report*; Return Path, *2016 Sender Score Benchmark Report*.

Internet service providers apply sophisticated filters that look at such things as email content and sender information to block spam. Also, blacklists allow network providers to block email based on the IP address and/or domain of the sender.

Mailbox providers, such as Gmail, Hotmail, AOL and Yahoo, also apply filters to incoming email, and rely heavily on their own client-fed internal data from things such as spam complaints and behaviour like opens and clicks with emails, as well as data feeds from outside third parties like senderscore.org for sender reputation to determine which emails should be delivered to recipients' inboxes. For example, in 2016, senders scoring above 90 on the Return Path Sender Score had their messages delivered to the inbox 92 percent of the time, while senders scoring 80 or lower had more than half of their messages rejected by filters. Senders scoring in the 1 to 10 band only had 1 percent of messages delivered.[31] A Sender Score is comprised of several factors, including complaints, hard bounces (emails rejected because they are sent to invalid email addresses), consumer engagement (e.g., opens and clicks), and emails caught in spam traps.

ESPs play a crucial role in preventing spam. ESPs are incentivized to carefully regulate and monitor client email activity to maximize deliverability, as spam-like behaviour by one client can negatively impact the reputation and deliverability of all clients. Members of the ESPC employ at least some, if not all, of the following safeguards to prevent spam:

- reviewing and vetting the sending practices of prospective clients before providing services;
- providing guidance on anti-spam legislation and best practices;
- prohibiting spam and related activities in service agreements;
- automatically including required identification information and unsubscribe mechanisms;
- responding quickly to complaints about email abuse;
- applying outbound filtering to block spam-like messages before they are sent; and
- separating clients by IP address(es) and domain(s).

Email authentication, using techniques such as the Sender Policy Framework ("SPF"), and Domain Keys Identified Mail ("DKIM"), is another important tool for minimizing spam because it enables recipients (like ISPs and email inboxes) to verify the identity of email senders. Non-authenticated email is much less likely to be delivered as it poses a risk that the sender is attempting to "spoof" another sender (a key element of "phishing" and other forms of social engineering). Email senders also use Domain-based Message Authentication, Reporting & Conformance ("DMARC"), an email authentication, policy, and reporting protocol that guides email receivers on how to treat a sender's email that does not meet email authentication tests; e.g., either block or send email to the spam or junk folder.

[31] Return Path, *2017 Sender Score Benchmark Report*.

Organizations that seek to engage in legitimate business by offering real products and services for sale therefore have very little incentive to send spam, even in the absence of anti-spam laws such as CASL. The vast majority of spam that remains is sent by criminals and other individuals, most of whom are located in foreign jurisdictions far beyond the reach of Canadian law. Regardless of how strict CASL may be, it is unlikely to have any influence over such spammers.

That the CRTC has imposed penalties in only three instances involving activities that even resemble spam-type behaviour is telling.[32] In every other case, the CRTC has negotiated payments through undertakings with legitimate businesses who appear to have, at worst, committed minor violations of CASL.[33] This does not help promote the Canadian economy or protect consumers.

3.3.2. Penalties Under CASL are Disproportional

At up to $10 million per violation, the CRTC has the ability to impose penalties that are virtually unlimited. Further, although CASL provides a list of factors to be taken into account when determining the amount of a penalty, these factors fail to establish meaningful limits or guidance, as the CRTC is free to apply and interpret the factors as it sees fit. This makes it impossible for businesses subject to CASL to quantify and understand their legal risk, because one mistake could result in a business being fined out of existence.

The business risk is exacerbated given the many areas under CASL that are unclear and subject to competing interpretations.

The administrative monetary regime under CASL is in sharp contrast to other penalty regimes. For example, the *Telecommunications Act* provides maximum penalties of $15,000 for a violation of the Unsolicited Telecommunications Rules ("UTR").[34] The UTR, which deal with telemarketing and are also enforced by the CRTC, are closely related to CASL in terms of the activities that they seek to address (although telemarketing is arguably a much bigger nuisance than spam). It is nonsensical that the penalties for spam and related activities should be so much higher than for telemarketing.

---

[32] Canadian Radio-television and Telecommunications Commission, *Undertaking: Plentyoffish Media Inc.*, Mar. 18, 2015; Canadian Radio-television and Telecommunications Commission, *Undertaking: Porter Airlines Inc.*, Jun. 26, 2015; Canadian Radio-television and Telecommunications Commission, *Undertaking: Rogers Media Inc.*, Nov. 20, 2015; Canadian Radio-television and Telecommunications Commission, *Undertaking: Kellogg Canada Inc.*, Sep. 1, 2016; Canadian Radio-television and Telecommunications Commission, *Undertaking: Mr. Halazon and TCC*, Jun. 12, 2017.

[33] Canadian Radio-television and Telecommunications Commission, *Notice of Violation: 3510395 Canada Inc. (Compu.Finder)*, Mar. 5, 2015; Canadian Radio-television and Telecommunications Commission, *Compliance and Enforcement Decision CRTC 2016-428*, Oct. 26, 2016; Canadian Radio-television and Telecommunications Commission, *Compliance and Enforcement Decision CRTC 2017-65*, Mar. 9, 2017.

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

The penalty regime under the *Canada Consumer Product Safety Act*[35] ("CCPSA") also helps to put CASL in perspective. The CCPSA provides a maximum penalty of $25,000, while seeking to prevent Canadians from the significant harms that can result from unsafe consumer products. Further, regulations under that Act establish an objective and prescriptive framework for determining the amount of a penalty.[36] A penalty amount is based on the "gravity factor" of a violation, which depends on the type of violation, as well as the history of violations committed by a person.

3.3.3. 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.

3.4. Private Right of Action

3.4.1. The Private Right of Action is Unnecessary and Harmful

The private right of action in CASL establishes an extraordinary remedy for alleged violations of the law. Not only does it allow any person affected by an alleged violation to sue for actual damages, it also authorizes 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 the lack of clarity found in many provisions of the law. There is no question that the private right of action would create an unpredictable and unmanageable risk for businesses, in addition to the risk that already exists with CRTC enforcement.

---

[35] *Canada Consumer Product Safety Act*, SC 2010, c 21.

[36] *Administrative Monetary Penalties (Consumer Products) Regulations*, SOR/2013-101.

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 spammers.

Thus, not only is the private right of action unnecessary, it would be highly disruptive and harmful to Canadian businesses.

3.4.2. Recommendation

The ESPC recommends that the private right of action be removed from CASL. In the alternative, if the government believes that a private right of action is necessary, the ESPC recommends that the statutory damages be removed from the private right of action.

4. Conclusion

The ESPC appreciates your time and attention, and would be pleased to speak or meet to discuss the review of CASL. The ESPC has given careful and extensive consideration to the issues discussed in this brief, and strongly believes that the recommendations provided would significantly improve CASL. Given the breadth and impact this legislation, the Committee's review is of great importance not only to ESPC members, but to Canadian economy as a whole.