ESPC
Email Sender & Provider Coalition

March 28, 2013

BY EMAIL

Andrea Rosen
Chief Compliance and Enforcement Officer, Compliance and Enforcement Sector
Canadian Radio-television and Telecommunications Commission
Les Terrasses de la Chaudière
Central Building
1 Promenade du Portage
Gatineau, Quebec J8X 4B1

Re: Follow-up submission of the Email Sender & Provider Coalition on Guidelines under Canada's Anti-Spam Legislation

Dear Ms. Rosen,

On behalf of the Email Sender & Provider Coalition (ESPC) I would like to thank you and your colleagues for taking the time to meet with us and hear our views on February 26, 2013 with respect to the interpretation and application of Canada's Anti-Spam Legislation (CASL).

We understand that the CRTC intends to produce further guidance on various issues under CASL in the coming months. Such guidance is very important as there is significant uncertainty among ESPC members and their customers on how to comply with the legislation with respect to a number of issues.

As a follow-up to our meeting, this letter provides further input and seeks clarity on some of the issues that are of greatest concern to ESPC members, including the following:

- Definition of a commercial electronic message: We are seeking further clarity on what is and is not a CEM for the purposes of CASL, with reference to specific examples.

- Application of CASL to legacy data: We are requesting guidance on how the CRTC intends to apply CASL to consent already obtained before the legislation comes in to force.

- Whom to identify in a commercial electronic message: The ESPC seeks further clarity on the types of organizations that are required to be identified in a commercial electronic message.

- Application of CASL to cookies: We understand that the CRTC is currently considering its position on how CASL may apply to cookies. This letter explains the importance of this issue and why CASL should not be interpreted in a restrictive manner.

Each of these issues is discussed in further detail below. Once you have had an opportunity to review we would appreciate an opportunity to meet again with you or your staff to discuss some of these issues in further detail and to respond to any questions you may have.

1. Definition of a commercial electronic message

1.1. Definition under CASL

There is a significant amount of uncertainty as to what types of messages are CEMs for the purposes of CASL, and, subsequently, what types of messages will be subject to the legislation.

CASL states that a message is a CEM for the purposes of the legislation if "it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity."[1] The guiding test is therefore whether a message "encourages participation" in a commercial activity. This means that there are many forms of messages sent in a commercial context that would not be a CEM for the purposes of the legislation. For example, a message that merely contains "commercial content," or may have some degree of "commercial value" would *not* be a CEM. If the government had intended CASL to apply to all messages sent in a commercial context it would have drafted a broader definition.

The inclusion of various categories of messages in subsection 6(6) leads to some confusion about what is and is not a CEM. With the possible exception of subsection(a) (a message that provides a quote or estimate), a message that solely performs any of the activities described in subsection 6(6) is not a CEM according to the definition in subsection 1(2). For example, it would be entirely inconsistent with subsection 1(2) to conclude that a message is a CEM where it solely:

- facilitates, completes or confirms a previously agreed to transaction;
- provides warranty, product recall, safety or security information;
- provides factual information about the ongoing use or purchase of a product, good or service, members, account or loan;
- provides information about an employment relationship or benefit plan; or
- delivers a product, good or service that was already purchased.

Based on a common understanding of these categories of messages, it would not be reasonable to conclude that *any* purpose of these messages is to encourage participation in a commercial activity. Rather, in most instances, a commercial activity has already been completed.

---

[1] *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"], ss. 1(2).

It is clear that the government intends that the definition in subsection 1(2) is to serve as the test for what is a CEM. This is reinforced by the Regulatory Impact Analysis Statement that precedes the draft *Electronic Commerce Protection Regulations* published by Industry Canada on January 5, 2013, which states as follows:

> some readers have interpreted the term "commercial electronic message" to include any messages sent in the course of a commercial activity, leading to concerns that it includes messages such as confirmations of successful unsubscribes or courtesy SMS messages sent to roaming customers. **The definition of a "commercial electronic message" is limited in the Act to a message that encourages participation in a commercial activity**. To the extent that a message is sent in a commercial context but does not fall within the definition of a commercial electronic message provided in CASL, it is not a commercial electronic message for the purposes of the Act [emphasis added].[2]

This makes it clear that subsection 6(6) is secondary to the definition of a CEM subsection 1(2) when defining a CEM. The reference to certain categories in subsection 6(6) does not categorically imply that a message that solely does any of those things is a CEM. At most it leaves open the possibility that in some edge cases a message that does one of those things could also be a CEM.

Interpreting CASL to apply to all messages sent in a commercial context serves no benefit from an anti-spam perspective and effectively undermines the objective of the legislation to promote the efficiency of the Canadian economy.

1.2. Request for clarity

With the forgoing considerations in mind, we are requesting guidance with respect to the types of messages that the CRTC considers to be CEMs for the purposes of CASL. We ask that the CRTC make reference to specific examples of content that would and would not render a message a CEM, including a rationale for the CRTC's interpretation. In particular, we would like to see the following examples referred to in guidance:

- a company logo;
- a company logo that includes a hyperlink to a company homepage;
- advertising slogan/tag line;
- a URL to the company's home page in a signature line;
- a request to "Like" a company on Facebook;
- a coupon or reward of some form;
- a reference to an ongoing or upcoming promotion;

[2] Canada Gazette, Part I, *Electronic Commerce Protection Regulations*, Vol. 147, No. 1, Jan. 5, 2013.

- a request to join a loyalty program.

2. Application of CASL to legacy data

One of the most common questions among ESPC members is with respect to how CASL will apply to existing lists of email subscribers. We therefore request that the CRTC provide guidance on how it intends to apply CASL to express consent obtained before CASL comes in to force. In particular, we seek guidance on two key issues.

- Express consent that is not technically compliant: We would like to know how the CRTC will apply CASL to CEMs that are sent based on consent that may have been compliant with privacy legislation and industry best practices that existed when consent was obtained, but may not meet certain requirements specified under CASL and/or regulations and guidelines. For example, consent may have been obtained with an opt-out express consent approach (e.g., a pre-checked box), or a request may not have contained all of the prescribed information required in the regulations.
- Evidence of consent: Senders have not always retained comprehensive records of when and how express consent is obtained given that there has never been a regulatory requirement to do so. We would like to know what standard the CRTC will apply to evidence of consent obtained before the law comes in to force. For example, where a definitive record of consent does not exist, it would be reasonable for the CRTC to consider as evidence of consent such factors as the approximate length of time that a given recipient has been an email subscriber without complaint, open and click through rates on email messages, and similar evidence.

3. Further clarity on whom to identify in a CEM

The ESPC has requested that the CRTC provide clarity on what it means to "send on behalf of" another person for the purposes of CASL. This is important as it determines which parties must be identified in a message.

The CRTC partially addressed this issue in the CRTC Guidelines, which state as follows:

> The Commission considers that section 2 of the Regulations does not require that persons situated between the person sending the message and the person on whose behalf the message is sent need necessarily be identified. For example, persons so situated may facilitate the distribution of a CEM but have no role in its content or choice of the recipients. In that event, the Commission considers that they do not

need to be identified.[3]

However, this still does not clarify what it means for one person to "send on behalf of" another, leaving open an important compliance question and creating uncertainty for every organization that sends email, as well as the service providers who assist them. Furthermore, by only referring to persons situated "situated between the person sending the message and the person on whose behalf the message is sent," this would likely only include a very narrow category of service providers. Most providers are situated between the person sending and the person receiving the message.

Finally, it is not uncommon for service providers to assist in developing content or selecting which recipients will receive a given email.

Further to the discussion on this topic during our meeting, it would be helpful to provide some background on the nature and role of email service providers in the email ecosystem.

3.1. What email service providers do

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

As such, ESPs provide the necessary infrastructure and knowledge that enable the development and delivery of email campaigns for clients. Although the services can vary between providers, there are a general set of core services that are common to most ESPs. Each of these services can be provided on a self service or full service basis, or a mix 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 and personalization: ESPs assist clients in identifying and creating segments of subscribers, allowing clients to effectively target marketing campaigns and transactional messages.

[3] Compliance and Enforcement Information Bulletin CRTC 2012-548: *Guidelines on the interpretation of the Electronic Commerce Protection Regulations (CRTC)* ["Bulletin CRTC 2012-548"], para 6.

- Anti-spam analysis: ESP tools can analyse email before it is sent to determine the likelihood that a given email might be considered spam and therefore subject to complaint and/or blocked by an anti-spam filter.
- Infrastructure: ESPs provide specialized servers that enable large volumes of email to be sent.
- Deliverability: ESPs assist clients in maximising deliverability of email campaigns. 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.

Some ESPs may also offer services assisting in the development of the creative component of an email campaign; i.e., developing the content of an email message, selecting the segment(s) to which it will be delivered, frequency, etc. Alternatively, in many cases these specific services are outsourced by the sender to an advertising agency.

Either way, the entire process of executing an email marketing campaign, from development to delivery and analysis, is commonly outsourced by a sender. This may specifically include developing the content of an email as well as selecting the recipients of an email. The goal throughout the process is to deliver a seamless email experience, and, as far as the consumer is concerned, the advertiser is the sender, not the ESP, the 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 volume direct mail services.

3.2. Request for clarification

The sender of an email campaign is the person with whom the end recipient of a CEM has a relationship, i.e., the person who has either express or implied consent under CASL to send a CEM. In many cases this would be an advertiser who has requested consent from a recipient to send a CEM. Thus, even though the advertiser may outsource some or all aspects of developing and delivering an email campaign, the advertiser is still the sender.

In other instances an advertiser may hire another sender to deliver an email campaign to that sender's list of recipients. For example, the owner of a publication may have requested consent from its subscribers to receive communications from other third parties pertaining to certain types of products or services, and sell access to that list as a service. This would commonly be referred to as a "list rental." In this case the owner of the publication would be the sender, as it is the person who has a consent-based relationship with recipients. Thus, the owner of the publication would be "sending on behalf of" the advertiser.

As we have stated before, there is no value in identifying the various service providers who may assist in the delivery of email an email campaign. From a policy perspective it would serve only to confuse rather than empower consumers.

The ESPC therefore requests that the CRTC provide further clarity in the following two ways:

- Clarify that the person who "sends" a CEM for the purposes of CASL is the person who has a consent-based relationship with the recipient.

- Broaden the class of providers that are exempt from the need to be identified. In this regard, it would be preferable for the CRTC to clarify that any person who *merely provides services facilitating the transmission or creation of a commercial electronic message* does not need to be identified in a CEM.

4. Cookies

4.1. Cookies are not computer programs

Cookies[4] are an essential component of the internet. Among many other things, they: enable websites to remember authentication information and personal settings; facilitate the 'shopping cart' function on e-commerce sites; provide businesses 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.

It is unfortunate that CASL has been drafted in such a way to create the potential for confusion about if and how the rules that apply to the installation of computer programs also apply to cookies. By all reasonable accounts it seems clear that it was the government's specific intention that the legislation not apply to cookies. As explained further below, interpreting CASL to apply to cookies could dramatically harm the internet experience for Canadian consumers.

In order to define a computer program for the purposes of CASL, the government chose to reference the *Criminal Code*, which defines a computer program as "*data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function*."[5] It is impossible to categorically conclude that cookies are 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 files that contain information.

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

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

There are no court decisions or any other precedents in Canadian law that interpret this definition to include cookies. If the government had intended for CASL apply to cookies, it would have drafted a new, broader definition.

During the Parliamentary review process of the bill that created CASL, a few stakeholders raised concerns about if and how CASL might apply to cookies. Despite assurances that the definition of a computer program did not include cookies, these stakeholders nonetheless pushed for greater certainty. The government responded by adding a reference to cookies in subsection 10(8) in an attempt to clarify that CASL would not apply to cookies. However, as you are aware, the government's response failed to provide the necessary clarity.

During our February 26 meeting with you one official expressed the view that cookies are computer programs as a result of subsection 10(8). The particular language referred to is as follows:

> A person is considered to expressly consent to the installation of a computer program if
>
> (a) the program is
>
> (i) a cookie

According to the interpretation expressed during our meeting, this language implies that all cookies are computer programs, which is entirely inconsistent with the definition of a computer program in the *Criminal Code*. It is also inconsistent with the government's intention that CASL should not apply cookies.

The preferable approach is to interpret CASL as specifically intended by Parliament. Although the approach has created some confusion, it is clear that the government included a reference to cookies in subsection 10(8) in order clarify that the rules that apply to executable computer programs (e.g., malware), do not apply to cookies. This reference does not and cannot alter the definition of a computer program found in the *Criminal Code*. We therefore urge the CRTC to avoid an attempt to expand the definition of a computer program and create an entirely new, unnecessary and unintended regime for the regulation of cookies on the Internet.

4.2. When it is reasonable to deem consent

If the CRTC takes the position that cookies are computer programs, then it would be required to determine when a "person’s conduct is such that it is reasonable to believe that they consent to" the installation of a cookie. This would require the CRTC to consider when it would be reasonable to deem consent for all forms of cookies, including cookies that are first-party vs. third-party, those that are used for various purposes including website analytics, website personalization, preference-based advertising, etc.

We ask the CRTC to consider the fact that all cookies including those for the purposes described above are already subject to regulation in Canada. To the extent that a cookie involves the collection, use or disclosure of personal information, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies. After extensive consultation and careful consideration of the issues, the Office of the Privacy Commissioner of Canada (OPC) has concluded that it is reasonable for organizations to rely on a form of opt-out/implied consent to the use of cookies for online behavioural advertising (OBA) purposes so long as certain conditions are met.[6] Recognizing the undesirable consequences of an overly rigid and prescriptive approach to regulating 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.[7]

As a broad, principle-based regime, PIPEDA provides a flexible standard that allows the OPC to revise its position as technologies evolve, where necessary. CASL, on the other hand, creates a set of strict and rigid rules that may be appropriate when applied to actual computer programs, but not cookies. These rules would directly contradict the views of the OPC on how cookies should be regulated.

In the U.S., cookies used for OBA purposes are subject *Self-Regulatory Principles for Online Behavioral Advertising*,[8] a set of principles developed by a number of industry groups in consolation with a range of stakeholders. These principles -- which generally align with the OPC's guidance on OBA -- are augmented by a consumer opt-out mechanism developed by the Network Advertising Initiative (NAI). [9] Industry stakeholders are also currently working with privacy advocates, regulators and technology and security experts to develop a standard for a browser-based opt-out mechanism (commonly referred to as "Do Not Track").

In addition to the NAI opt-out mechanism and the Do Not Track mechanism, users can easily control the types of cookies that can be set on a web browser by adjusting browser settings. In this regard, Internet users can choose to accept all, some, or no cookies at all. Therefore, if the CRTC were to conclude that cookies are computer programs for the CASL we would urge the CRTC to consider the fact that mechanisms already exist for users to exert control over cookies.

---

[6] Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, June 6, 2012, [*Policy Position*].

[7] *Ibid*.

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

[9] Network Advertising Initiative Consumer Opt-Out.

More specifically, a user should be deemed to consent to the use of cookies based on their ability to opt-out through browser settings as well as industry developed solutions such as the NAI opt-out and header-based mechanisms (e.g., Do Not Track).

4.3. Consequences of an express consent-based regime for cookies

In 2009 the European Commission amended the EU *Directive 2002/58/EC on Privacy and Electronic Communications* (the Directive) that would, among other things, require member states to pass legislation requiring website operators to obtain consent for the use of certain types of cookies. The directive has been widely criticized as overly cumbersome and prescriptive, with some member states still refusing to implement the directive. If the rules under CASL that apply to computer programs were also applied to cookies, this would create a much stricter regime than that created by the EU Directive.

The consequences of such a regime would be significant for the internet ecosystem. As a convenient tool to store information, cookies allow website owners to provide countless products and services that otherwise would not be possible, including the vast majority of content that internet users currently enjoy online for free. Requiring express consent for cookies would not only lead to a significant amount of inconvenience for internet users, it would significantly drive up the cost of owning and operating a website, reduce innovation and impact the availability of products and services offered to internet users because many websites rely on advertising powered by cookies to survive.

If the government chooses to make such a drastic change to the internet and the availability of free content, it should be on a deliberate basis after careful consideration and consultation with stakeholders. We therefore urge the CRTC to carefully consider an overly broad interpretation of the definition of a computer program.

As the role of cookies in the Internet ecosystem and how they are currently addressed through technology, industry principles and regulation is a very complex matter, we would appreciate the opportunity to meet with you or your staff to discuss this issue further.

Thank you for taking the time to consider our views and concerns. The interpretation and application of CASL will have a significant impact on our members and their clients, and is therefore of great interest to the ESPC. We hope to have a follow-up meeting with you or your staff to discuss these issues in further detail once you have had an opportunity to review the forgoing.

Sincerely,

D.R. Freeman/sb

D. Reed Freeman, Jr. Esq.
Outside Counsel, Email Sender & Provider Coalition
Morrison & Foerster LLP
2000 Pennsylvania Avenue, NW, Suite 6000
Washington, DC 20006
202.887.6948
rfreeman@mofo.com

cc: ESPC Board of Directors
ESPC Members
Shaun Brown, Esq.