CANADIAN WIRELESS TELECOMMUNICATIONS ASSOCIATION

Submission to the House of Commons Standing Committee on Industry, Science and Technology

STATUTORY REVIEW OF AN ACT TO PROMOTE THE EFFICIENCY AND ADAPTABILITY OF THE CANADIAN ECONOMY BY REGULATING CERTAIN ACTIVITIES THAT DISCOURAGE RELIANCE ON ELECTRONIC MEANS OF CARRYING OUT COMMERCIAL ACTIVITIES, AND TO AMEND THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION ACT, THE COMPETITION ACT, THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT AND THE TELECOMMUNICATIONS ACT

Submitted November 9, 2017

Email: indu@parl.gc.ca
Robert Ghiz, President

T 613 233 4888 F 613 233 2032 www.cwta.ca
300-80 rue Elgin Street Ottawa, ON K1P 6R2

1. Introduction.

The Canadian Wireless Telecommunications Association (CWTA) is the recognized authority on wireless issues, developments and trends in Canada. It represents wireless service providers as well as companies that develop and produce products and services for the industry, including handset and equipment manufacturers, content and application creators and business-to-business service providers. CWTA is pleased to submit its comments with the respect to the above-noted statutory review.

CWTA supports the purpose of Canada's Anti-Spam Legislation ("CASL" or the "Act"), which is to foster Canadians' confidence in electronic commerce by outlawing "damaging and deceptive spam, spyware, malicious code, botnets, and other related network threats."[1] However, in attempting to curtail these undesired activities, Parliament enacted legislation that is overly broad, lacking in clarity, and whose enforcement is neither transparent nor proportionately applied. CWTA encourages a thorough review of CASL, and resulting changes, to ensure the goal of protecting Canadians is achieved without unduly hampering the conduct of legitimate business.

2. Issues and Recommendations

2.1 Lack of Clarity and Overly Broad

A key benchmark for assessing the success of CASL should be whether it is easy to understand which activities are captured by the legislation and what is required to comply. A consistent refrain heard in oral and written evidence provided to the committee is that CASL is overly complex and lacks clarity. Determining whether a specific activity or message is covered by the Act, or falls within an exception, is often a difficult task even for companies with in-house legal teams and subject matter experts. This often makes it more difficult and, including compliance costs, almost as expense to send an email as it is to send a letter, flyer, or brochure to someone's home.

In addition, the Act is overly broad and potentially captures activities that do not fall within CASL's stated purpose. For example, messages restricted to providing factual information about products or services purchased by a customer, such as a notice that a mobile phone user is approaching their data cap, should not be considered commercial messages, yet CASL seems to require they include the same unsubscribe options required of commercial messages.

It is important that the Committee review CASL in its entirety with a view to reducing its complexity and limiting its scope to "damaging and deceptive spam" as well as other malicious acts that threaten the security of computer systems or data, including personal information. It should also be less prescriptive and instead be principle-based so that senders of messages can implement the Act's requirements in a way that is compatible with the form of message used and context.

Examples of the problems identified above include:

- The definition of Commercial Electronic Messages ("CEM") lacks clarity and is overly broad. Businesses are often confused as to whether a particular message falls under the definition of CEM.
- Subsection 6(6) exempts from the consent requirement specific types of messages, most of which do not fall within the definition of CEM under subsection 1(2) of CASL, but rather provide the recipient with information concerning products or services they have already purchased or to

[1] Regulatory Impact Analysis Statement, Paragraph 3 –"Objectives" at http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html

which they subscribe. Yet CASL still seems to require senders of such messages to abide by format requirements, such as inclusion of an unsubscribe option. In regulating the sending of non-commercial electronic messages, CASL overreaches its purpose. It also creates the potential unintended consequence that a customer may not receive important information about the products and services they use.

- CASL prescribes the content of CEMs, and some non-commercial messages, without regard to the nature or limitations of individual messaging platforms. For example, it is impractical to include all of the prescribed information in a single SMS message.

Recommendations:

- The definition of Commercial Electronic Message should be amended. The definition should be narrowed to reflect the stated purpose of the Act and additional guidance should be issued to clarify what types of messages are not CEMs.
- Subsection 6(6) should be deleted from the Act. Consideration could also be given to adding the types of messages listed in subsection 6(6) to subsection 1(2) as examples of electronic messages that are not considered CEMs and are not governed by the Act.
- Other areas of CASL that are causing confusion or uncertainty and require re-examination include, without limitation: the definition of implied consent arising from an existing business relationship; the requirements for installing computer programs (which should be limited to a prohibition on installing without authorization malicious software or software that collects personal information); the definition of "electronic address" ; and, business-to-business communications.

2.2 Investigative Process and Enforcement

While it is important that the CRTC possesses the appropriate tools and powers to target malicious actors who seek to deceive or harm Canadians, we have concerns with the manner in which these tools and powers have been exercised. We understand that in a number of cases involving unintentional non-compliance the CRTC did not issue warning letters or give the targeted party the opportunity to rectify the issue prior to launching an investigation and seeking monetary penalties.

Recommendations:

- Enforcement should focus on those who set out to do harm, while those who are trying to comply with complex regulations should be given the opportunity to cooperate with the regulator without fear of hefty penalties and with the mutual goal of achieving compliance.
- The CRTC should be required to publish reasons for its decisions so that the public can gain insight into the CRTC's interpretation of the Act and its decision-making processes.
- Businesses should be able to seek clarification and guidance from the CRTC on a without prejudice basis so that good faith efforts at compliance do not give rise to investigations.

2.3 Administrative Monetary Penalties

A violation of CASL carries with it a maximum administrative penalty ("AMP") of $10 million per violation. While large monetary penalties may be necessary to deter and deal with malicious actors who intentionally set out to cause harm to Canadians, it is entirely inappropriate for businesses that are making good-faith efforts to comply with CASL to be faced with the risk of massive penalties for mistakes or unintentional acts.

Recommendations:

- A framework for the assessment of fines should be established that takes into consideration the intent of the person, the person's history of violations, and the magnitude of the violation. For example, the intentional dissemination of malware should carry a much higher penalty than a technical malfunction of an unsubscribe function.
- It should be made explicit that penalties are to be applied on a campaign level and not for each individual email within a given campaign.

2.4 Private Right of Action

CWTA supports the June 7, 2017, decision by the Federal Minister for Innovation, Science & Economic Development to indefinitely suspend the Private Right of Action ("PRA") provisions of CASL. The PRA is not necessary to achieve the purpose of CASL. The federal agencies responsible for enforcement have sufficient enforcement powers to deter potential violations and to impose remedial actions and, where warranted, proportionate monetary penalties. There is no evidence to show that a private right of action will further advance the purpose of CASL. Instead, a PRA would likely encourage individuals to pursue actions against businesses in Canada without regard to the business' intent or exercise of due diligence, and with no requirement to demonstrate actual harm.

Recommendations:

- The private right of action should be removed from CASL.
- If government determines that the private right of action is necessary, the ability to award statutory damages should be removed so that actual harm must be proven.

3. Conclusion.

The vast majority of Canadian businesses are well-intentioned and seek to use electronic messaging in a responsible way. However, the complexity of CASL has made it difficult for many businesses to be certain that their legitimate business activities are compliant with CASL, and face potentially large penalties if they make a mistake. CASL requires a thorough examination and further consultation in order to reduce its complexity and to ensure that its enforcement is primarily focused on those actors who intentionally seek to do harm. We appreciate the opportunity to provide input on areas of CASL that should be improved. We remain available to further discuss our concerns and potential solutions.