**November 7, 2017**

**ITAC SUBMISSION TO INDU COMMITTEE REVIEW OF CANADA’S ANTI SPAM LEGISLATION**

On October 17th, David Messer of the Information Technology Association of Canada (ITAC) testified as part of the INDU Committee’s review of Canada’s Anti-Spam Legislation. ITAC’s general remarks identified significant challenges that CASL’s overly broad scope and prescriptive requirements have created for legitimate businesses, including how some elements of CASL, such as the computer software requirements, undermine innovation and cybersecurity.

To counteract these unintended consequences, and to better address the statutory objective of CASL – i.e. promoting the growth of the digital economy – there is a pressing need to rebalance the legislation and enforcement actions to better target malicious actors, botnets and harmful spammers, and make it easier and less costly for legitimate businesses to comply with CASL requirements.

ITAC has set out below 12 proposed amendments to CASL that, if adopted, will bring CASL into balance with its statutory objective.

The amendments have been carefully drafted so that they do not undermine how CASL regulates harmful spam, malware and other malicious online activities. They do not change the basic structure of the law – including the opt-in consent model – or the penalties that can be imposed on bad actors. Rather, they provide practical suggestions for eliminating CASL’s unintended impacts on legitimate businesses, while retaining the elements of the law that are designed to protect consumers.

ITAC’s proposed amendments ensure that CASL will “clean the pipes” of negative elements, while helping to overcome the concerns within the innovation economy and among SMEs and other businesses that the compliance challenges and costs are excessive and unworkable.

**Proposed Amendments**

1. **Narrow the scope of “commercial electronic message”** so that CASL regulates only messages the purpose of which is (a) advertising, marketing, promoting or otherwise offering a product, good, service, land, business, investment or gaming opportunity, or (b) promoting a person, including the public image of a person, as being a person who does anything referred to in (a).  Doing so will provide the necessary clarity as to when CASL’s e-messaging rules apply, and will ensure that these rules do not apply to factual or transactional messages (e.g., a text message from a service provider that a customer is “now roaming”).
2. **Delete section 6(6).**  By narrowing the scope of CEM, section 6(6) (which sets out an exception to consent for certain factual and transactional messages) becomes unnecessary.  Removing section 6(6) will also make clear that CASL’s e-messaging rules do not apply to factual or transactional messages.
3. **Replace the concept of implied concept** **arising from an existing business relationship with the concept of inferred consent from Australia’s anti-spam law:**
“*consent that can reasonably be inferred from:
(i) the conduct; and
(ii) the business and other relationships;
of the individual or organization concerned*.”

The Australian approach sets out a general legislative principle that can be applied to any context, rather than prescriptive implied consent rules (as found in CASL) which, by their nature, do not address all situations in which it would be reasonable for implied consent to apply.

1. **Revise definition of “electronic address”** by deleting “any similar account” or replacing “any similar account” with “any similar account prescribed by regulation that enables direct two-way communications using the electronic address”.  Allowing for similar accounts to be prescribed by regulation will ensure that there is careful consideration given as to whether CASL should apply to additional forms of digital communication.  Clarifying that “similar accounts” must enable direct two-way communications using the electronic address helps to provide certainty that CASL does not apply to online advertising, pop-up messages, online chats and similar communications.
2. **Permit consents to be obtained on an enterprise basis** where doing so would be consistent with the reasonable expectations of the recipient (e.g., across a brand).  This revision would reduce needless complexity and compliance costs, without subjecting a consumer to unexpected messages.
3. **Replace the sections of CASL dealing with the installation of computer programs so that CASL regulates only malicious software**.  Define “malicious software” to mean: “*a computer program designed to:
(i) disrupt or deny operation of a computer system or other computer program;
(ii) disrupt or deny access to or use of the resources of a computer system; or
(iii) collect personal, financial or proprietary information stored on the computer system;
that, in each case, is installed without authorization*.”

Define “without authorization” to mean “*without authorization of the owner or an authorized user of the computer system, including where authorization is obtained with an intent to deceive or defraud or where a computer system is accessed in contravention of an Act of Parliament*.”

1. **Amend section 6(2)(a) of CASL to read**: “*identify the person who sent the message or the person – if different – who authorized the sending of the message*”.  This wording, which draws on the approach in Australia’s anti-spam law, will remove unnecessary complexity and cost associated with the “*on behalf of*” wording in CASL.
2. **Replace all references in CASL to “*on whose behalf the commercial electronic message is sent*”** with “*who authorized the sending of the message*.” This wording, which draws on the approach in Australia’s anti-spam law, will remove unnecessary complexity and cost associated with the “*on behalf of*” wording in CASL.
3. **Amend section 10(1)(b) of CASL to read:** “*information that clearly and accurately (i) identifies the person seeking consent or, if the person is seeking consent on behalf of another person, that other person, and (ii) information about how the person seeking consent or, if the person is seeking consent on behalf of another person, that other person, can be readily contacted*.”  This revision will have the effect of replacing prescriptive rules with a general principle that allows for more flexibility, without undermining the objective of the provision.
4. **Amend section 47 to restrict standing to sue under the private right of** **action to those businesses that are directly impacted by spam, spyware and other online threats** (i.e., telecommunications companies, online companies and internet service providers).  Doing so will (as is the case in the United States) enable those businesses who are best positioned to do so, to pursue bad actors in the courts, while addressing the material risk created by the current wording of section 47, that the PRA will result in costly, unwarranted class actions against legitimate companies.
5. **Authorize the CRTC to share information** and complaints about spam and malicious software with telecommunications companies, online companies and internet service providers.  Doing so will enable industry to collaborate with the CRTC in an effort to enforce CASL.
6. **Revise section 64 of CASL so that the Governor in Council has sole regulation making authority** (rather than this authority being split with the CRTC).  The Governor in Council can then replace the CRTC regulations with regulations that do not add prescriptive rules to CASL.

ITAC would be happy to discuss or answer questions about these proposed amendments with the Committee at your nearest convenience. For further information please contact David Messer at dmesser@itac.ca