

**Coalition of Business and Technology Associations:**

Association of International Automobile Manufacturers of Canada  
Canadian Bankers Association  
Canadian Chamber of Commerce  
Canadian Federation of Independent Business  
Canadian Marketing Association  
Canadian Wireless Telecommunications Association  
Canadian Vehicle Manufacturers' Association  
Electro-Federation of Canada  
Entertainment Software Association of Canada  
Information Technology Association of Canada  
Interactive Advertising Bureau of Canada  
Magazines Canada  
Retail Council of Canada

February 4, 2013  
Bruce Wallace  
Director, Security and Privacy Policy,  
Digital Policy Branch,  
Department of Industry  
Jean Edmonds Tower North  
18<sup>th</sup> floor, Room 1891D  
300 Slater Street  
Ottawa, Ontario  
K1A 0C8

**Subject: Industry Canada notice in the *Canada Gazette*, Part I dated January 5, 2013, the Electronic Commerce Protection Regulations**

We are the Coalition of Business and Technology Associations (the Coalition or the group) a group of organizations representing a broad cross-section of Canadian businesses, from sole proprietorships, to small and medium sized, businesses, to the largest Canadian and multi-national firms. Our member organizations span a wide range of industry sectors and touch almost every corner of the Canadian economy including manufacturing, retail, professional services, entertainment and business software, information, communications and telecommunications, advertising and marketing, publishing, and research and development.<sup>1</sup>

We continue to share the Government's goal of combating spam and malware, and are pleased to provide the following joint comments on the draft Electronic Commerce Protection Regulations published in Part 1 of the *Canada Gazette* on January 5, 2013 (the "draft regulations") related to Canada's Anti-Spam Legislation, S.C. 2010, c. 23 ("CASL" or the "Act").

---

<sup>1</sup> The organizations represented by the groups listed above may be referred to as the "Coalition of Business and Technology Associations ("CBTA").

We support the Government's objective of ensuring that CASL achieves its goals of reducing spam and malware while encouraging and facilitating the use of electronic means of communication and ecommerce. We have studied CASL and have provided a series of comments both to Industry Canada and to the Canadian Radio-television and Telecommunications Commission ("CRTC" or the "Commission") on the published drafts of their respective regulations. Our perspective is informed by the reality of our members' attempts to plan for compliance with this unprecedented new legislation.

We appreciate that Industry Canada has taken note of some of our previously stated concerns with respect to CASL and its original draft regulations in the current draft regulations. These new proposed regulations will help to alleviate some of the unintended consequences of CASL on legitimate business activity, without impairing CASL's goals. But we wish to emphasize that this legislation was at least equally intended to encourage and facilitate the use of electronic means of communication and ecommerce, a key pillar of any nation's digital economy strategy.

We have many concerns about CASL, which are set out and explained below, along concrete recommendations for addressing them. A summary of our recommendations is in Appendix A.

We have now been working with CASL for over two years and have a better appreciation of the compliance challenges and the potential for unintended consequences resulting from CASL's regulatory approach much more than we did when CASL was passed by Parliament. The inclusion in CASL of both open ended prohibitions and prescriptive requirements makes it very difficult to anticipate all of the impacts that CASL will have. We are now more concerned than ever that CASL will actually result in more harm than benefit to the Canadian economy and to digital commerce. We are also concerned that the harm will be exacerbated by the potential for litigation under the private rights of action.

Our concerns about CASL include the following, all of which are explained in more detail in our comments on the draft regulations below:

- CASL will require all Canadian organizations of any kind including businesses, charities and non-profit organizations, educational institutions, hospitals and others to expend significant up-front and ongoing resources to comply. These one-time costs and all of the ongoing compliance costs and red-tape will be particularly onerous for small businesses and will far outweigh the benefits CASL is intended to provide Canadians and our economy.
- It is well known that most real threats from CEMs such as those that are false or misleading and from spam, malware and spyware originate outside of Canada. These are well out of the reach of the Commission's enforcement abilities, and will not be addressed by treating all Canadians and Canadian organizations as if they were originators of spam, malware and spyware, as CASL does.
- CASL is drafted to sweep in a wide range of messages. As a result, there is significant uncertainty about what measures are necessary to comply. Guidance

received to date from the CRTC suggests that a range of service messages including messages warning consumers when they will incur roaming or other extra charges, or bringing warranty issues to their attention, could be illegal to send if consumers inadvertently unsubscribe from receiving all CEMs from an organization. CASL will therefore make it more difficult for organizations to develop services that rely purely on electronic means of doing business – digital economy businesses – because it may enable customers to unsubscribe from receiving service and transactional messages.

- The CRTC has also provided guidance that every message that includes a hyperlink to an organization's home page may make that message a CEM. Accordingly, we are concerned that CASL's scope may apply to practically every message sent by organizations, despite its intended application to CEMs only.
- CASL, as it is currently drafted, requires almost a message by message content review to determine if it is caught within the scope of the Act which is something that cannot be done systemically. This runs directly counter to the stated purpose of the Act (promoting the efficiency and adaptability of the Canadian economy, encouraging the use of electronic means to carry out commercial activities) and also results in unwarranted and unnecessary liability and risk for organizations.
- CASL will undermine the formation and growth of small and innovative businesses. Businesses without existing business or ongoing relationships will be unable fully to leverage modern means of communication. This will ultimately affect competition and consumer choice, and result in higher prices, which surely cannot have been Parliament's intent.
- CASL's rules may make it impractical, for businesses to use closed and managed messaging systems such as short codes or short message service (SMS) services, instant messaging services such as Blackberry Messenger, and social networking and other multi-user platforms.
- CASL's rules with respect to the installation of computer programs are overly broad and will limit an organization's ability to protect and secure its networks, to protect customer data, and to combat fraud and cybercrime. Ironically it will place Canadians at a disadvantage compared to other countries where organizations are more readily able to take mitigating action to protect consumers. CASL will require both Canadian and foreign-based businesses to implement costly new operational processes, even if their current worldwide processes align with industry best practices and have given rise to no customer dissatisfaction.
- CASL will create disincentives for high-tech businesses from carrying on business in Canada. Because of the extra-territorial reach of CASL, tech companies will be reluctant to establish or keep cloud computing and outsourcing operations in Canada. Multi-national companies will be incented to move their computer operations that support foreign operations outside of Canada so the businesses can compete on a level playing field with their foreign competitors.
- The transitional provisions in CASL are ineffective. This will leave many organizations exposed to immediate contraventions under threats of class action suits based on CASL's provision for private rights of action.

Our comments to the consultation are organized as follows. First, we address the draft regulations which have been proposed. Next, we identify other issues which the regulations did not address. Our comments, below dealing with the proposed new draft regulations, are addressed in the order which they appear in the draft regulations, and not necessarily in the order of most importance.

It may be that all of our recommendations cannot be made through regulations. To the extent that this is the case, we recommend that the applicable issue be reviewed by means of a task force, expert panel, review body or public consultation as appropriate (referred to here as a “Review Body”) before the draft regulations are finalized.

Please note that several of the organizations represented in this letter (and some of their members) will also file separate comments on the draft regulations which may expand upon or raise additional concerns.

## **PART 1**

### **Issues Raised by the Regulations**

#### **1. Issue: Family Relationship**

The draft regulations define ‘family relationship’ to include blood relationships that emanate from a common set of grandparents. The rationale given for this definition is that it is “in keeping with definitions in the *Income Tax Act*.” However, there are significant differences between CASL and the *Income Tax Act*. While it may make sense to have a narrow definition of family relationship to prevent tax evasion or to further the other objectives of the *Income Tax Act*,<sup>2</sup> a much wider definition of family relationship is called for under CASL.

Many businesses, especially sole-proprietorships and small businesses rely on their extended families for support including for financing and referrals. We recommend that the definition in section 2(a) of the draft regulations be amended to include all persons who are or were related by blood, marriage, common-law union or adoption.

#### **2. Issue: Personal Relationship**

The expansion of the definition to recognize virtual relationships is a significant improvement over the previous definition. However, the reference to whether the parties have “met in person” still favours in-person meetings over virtual relationships, and fails to take account of changes in the way people now interact online. The definition should be drafted in a technologically neutral fashion which would result in the removal of the factor related to an in-person meeting.

---

<sup>2</sup> We note that some of the definitions in the *Income Tax Act* are broader than the definition of “family relationship” in the draft regulations. c.f.s.252 which includes references to a great-aunt or great-uncle and former spouse.

More fundamentally, the listed factors introduce a subjective evaluation that will be difficult to apply. It appears that only very close friends will be recognized as having personal relationships under this definition.

It is important to remember that the goals of the family and personal relationship definitions was to remove from the ambit of the Act individual relationships that fundamentally were not primarily business or commercial relationships, do not require regulation, and where CASL's formalities would be excessive and needlessly burdensome.

Many businesses, especially sole-proprietorships and small businesses (and especially in their early years) rely on their network of friends, colleagues, past-colleagues, and acquaintances to help them grow their businesses. CASL's prohibitions applied to these categories of relationships would cause more harm than good.

We therefore recommend that the definition in section 2(b) be broadened and drafted in a technologically neutral fashion so that it will extend to individuals who have had direct, voluntary, two-way communications and for whom it would be reasonable to conclude that the relationship is personal such as where the individuals are friends, colleagues, acquaintances, or have relationships arising out of being members of the same clubs, associations, or voluntary organizations and the person to whom the message is sent.

### **3. Issue: Business to Business Exemption**

Section 3(a) of the draft regulations is a much-needed exemption. We agree with the Regulatory Impact Assessment Statement ("RIAS") that it removes from CASL "communications that are not the types of threats that were intended to be captured within the scope of the Act."

We note the limitation in section 3(a)(i) does not appear to exclude messages related to employment (which are covered by section 6(6)(e)). Matters related to employment may not all be considered to be "concerns the affairs of the organization". For example, the exception may not capture charity promotions (like United Way) or other more social events sent using business systems. We would recommend that the exception in section 3(a)(i) be expanded to include any message sent to the employment electronic address.

We also note that section 3(a)(ii) of the draft regulations appears inadvertently to exclude CEMs that are sent to non-business organizations. We believe that just as section 3(a)(i) recognizes the need for an exemption for CEMs sent internally within organizations, the same rationale applies to messages between organizations whether they are business or non-business organizations, such as educational institutions, charities, hospitals and other not-for-profit organizations.<sup>3</sup>

---

<sup>3</sup> In what follows, we make several recommendations for expanding exceptions that were originally available only to business organizations to "other organizations". In this submission, we use this term to refer to the defined term "person" other than an individual.

We recommend that section 3(a)(ii) be expanded to include a CEM that is sent by an employee, representative, contractor or franchisee of an organization to an employee, representative, contractor or franchisee of another organization if the organizations or any of its affiliates have or had a business, non-business, professional, or other relationship at or prior to when the message was sent, and the message concerns the affairs of the organization or any of its affiliates or that person's role, functions or duties within or on behalf of any such organization.

#### **4. Issue: Referral Relationships**

Section 4(1) of the draft regulations provides a useful exception that will permit CEMs to be sent based on a referral where the referring party has "an existing business relationship, existing non-business relationship, a personal relationship or a family relationship" with both the sender of a CEM and the recipient of that message.

We believe that the referral exception should also include situations where the referring party also has the benefit of the new business-to-business exception with one or both of the sender or CEM recipient. As drafted, the exception may not apply at all to many contemplated circumstances as the exception only applies to the individual when the individual has the specific relationships when, as a matter of law, the relationships may be those of the person's employer. We do not expect that either of these restrictions was intended. Further, the individual sending the message would in most cases not have the benefit of the existing business relationship or the new business to business relationship. The person's employer would.

We therefore recommend that section 4(1) be expanded so that section 6(1)(a) of the Act does not apply to a commercial electronic message that is sent by a person for the purpose of contacting the person to whom the message is sent following any referral by one or more persons who have an existing business relationship, an existing non-business relationship, a personal relationship or a family relationship or a relationship that qualifies the person for the exception specified in section 3(a)(ii) of the draft regulations with the person who sends the message as well as any of those relationships with the person to whom the message is sent and that discloses to the recipient the full name of the person who made the referral and states that the message is sent as a result of the referral, and (b) the exception in paragraph (a) applies only to the first commercial electronic message that is sent by an individual for the purpose of contacting the individual to whom the message is sent following any referral by one or more persons.

#### **5. Conditions for Use of Consent**

Section 5 of the draft regulations propose, without change from the first set of regulations, very onerous requirements on persons who seek consents to send CEMs on behalf of third parties. These regulations are very important as many organizations seek such consents including those that compile lists and directories as well as online service providers such as online marketplaces. These lists, directories and online

providers provide valuable and important information and services to Canadian consumers and organizations. Yet, the proposed rules would create unworkable technical requirements and extensive potential vicarious liabilities that will impede business models based on the use of third-party consents.

Under these proposed regulations, the person obtaining the consent is placed in the position of an insurer with strict liability for all breaches by all users of the information made available. Given the extensive potential liability for administrative monetary penalties and class-action suits under CASL's provision for private rights of action, organizations will be very reluctant to engage in business activities that could make them an insurer for actions that are outside their control. In an online environment where consents are obtained on behalf of a network of users, the potential liability is incalculable. The "ensure" requirements in section 5(1) and 5(2) impose an especially unreasonable burden on small and medium-sized enterprises. In addition, the provisions in section 5(3) of the draft regulations, which require a person who obtained consent, without delay, to inform any other person authorized to use that consent of the withdrawal of consent on receipt of a notification of withdrawal of consent from that person, may impose a further, significant burden.

The requirement under, section 5(1)(b) of the draft regulations, to provide an unsubscribe mechanism that "allows the person from whom consent was obtained to withdraw their consent from the person who obtained consent or any other person who is authorized to use the consent" will confront consent holders and authorized users with an impractical compliance problem. In particular, in many situations, including in many well-established affinity programs, it will be all but impossible to include an accurate list of persons who are authorized to use the consent as that list will change overtime. Furthermore, this would result in a situation whereby recipients would be faced with long, confusing and cumbersome lists of authorized consent users.

The draft regulations require sophisticated methods of tracking, by the person obtaining the consent as well as persons using the information, the status of the consent of each consenting individual including whether the individual has withdrawn his or her consent from that person, from the person obtaining the consent or from any other user of the consent. The draft regulations do not take into account the business and technical realities of what they actually require to put them into operation, or the level of interoperability required to track consent status between organizations.

In order to address these issues we recommend that section 5(1)(b) of the draft regulations be revised as follows. First, the party obtaining consents should be able to satisfy its obligations using contractual measures with third parties and by conditioning authorization to use the consents on compliance with CASL, which would make third parties who use the consents in contravention of CASL fully liable for the violations.

Second, where a message recipient unsubscribes from receiving messages from an authorized user, the authorized user should inform the consent-holder who should respect the unsubscribe for its own messages, and discontinue making arrangements

with prospective new authorized users. There should be no obligation by the consent-holder to cancel all other existing arrangements due to the impracticalities described above. The message recipient should, however, be able to curtail messages from any such authorized user by similarly unsubscribing, which would achieve the same purpose.

We also recommend that section 5 of the draft regulations be amended as follows:

For the purposes of section 10(2)(b) of the Act, a person who obtained express consent on behalf of a person whose identity was unknown may authorize a person to use the consent on the condition that in any commercial electronic message sent by the authorized person to the person from whom consent was obtained,

- (a) the person who obtained consent is identified;
- (b) the authorized person provides an unsubscribe mechanism(s) that, in addition to meeting the requirements set out in section 11 of the Act with respect to messages from the authorized person; and
- (c) allows the person from whom consent was obtained, by notice to the authorized person, to withdraw their consent from the person who obtained consent.

(2) The person who obtained consent must include, in the agreement with the authorized person for the use of the consent, a provision that requires the authorized person, upon receipt by the authorized person of an indication of withdrawal of consent referred to in paragraph 1(c), to notify the person who obtained consent that the consent has been withdrawn.

(3) Upon receipt of the notice referred to in paragraph 2(c), the person who obtained consent must treat the withdrawal of consent as an unsubscribe request pursuant to section 11(1)(a) of the Act and not thereafter enter into an agreement with a person to authorize that person to use the consent.

## **6. Specified Computer Programs**

Section 6 of the draft regulations proposes two categories of deemed consent for the installation of a computer program in limited circumstances.

The first category requires that three conditions be met, namely (1) the program is installed by a telecommunication service provider ("TSP"), (2) the only reason can be to prevent activities that the TSP reasonably believes are in contravention of an Act of Parliament, and (3) there is an imminent risk to the security of its network. We submit that each of these conditions is too narrow.

CASL's computer program rules could make it illegal for Canadian organizations to fight threats to their computer systems, networks and to their customers' personal

information and privacy. Ironically, they will make it more difficult to engage in self-defence measures against those that would cause extensive damage. This could result in law-abiding organizations that are trying to do the right thing in the face of cyber-threats inadvertently violating CASL.

The first condition limits the deemed consent to TSPs. This limitation ignores the reality that organizations across many industries, including financial institutions, retailers, health networks, and computer services organizations, operate computer networks. These organizations may not be considered to be TSPs, particularly where they are not acting as passive transmitters of third-party information.<sup>4</sup> In our view, the deemed consent should apply to the operators of any network.

The second limitation is that the TSP reasonably believes the installation is necessary to prevent activities that the TSP reasonably believes are in contravention of an Act of Parliament. This limitation would prevent TSPs and others from taking similar actions in the context of other threats to a network including security, privacy, non-compliance with contractual terms including detailed policies of acceptable behaviour or terms of service that could affect network management, or a contraventions of other laws. It would also prevent prompt action because a legal opinion may be required to satisfy this condition.

The third limitation is that there must be an imminent risk to the security of the TSP's network. This limitation would prevent TSPs and others from acting: (i) where there has already been a violation of security and the action is necessary to investigate the incident and collect evidence, (ii) where there is a foreseeable risk, but not necessarily an imminent one, requiring that the timing before an intervention can occur be carefully measured in the face of significant possible harms, (iii) where threats relate to other *bona fide* concerns other than security such as fraud, cyber-crime, violations of privacy laws, identity theft, or other threats to public safety, and (iv) where threats are to persons or property other than the TSPs network such as computer systems, facilities or devices used in conjunction with the network such as network-connected equipment and consumer smartphones.

None of these limitations are necessary in our view. The reality of the exceptional circumstances that give rise to these situations is that the usual requirements for obtaining express consent and information disclosures do not make sense.

The second category of deemed consent in s.6 of the draft regulations requires that a program can be installed only for the purpose of updating or upgrading a TSP's network. It must be done by or on behalf of the TSP, which must own or operate the network, and on the computer systems that constitute all or part of the network.

The conditions associated with this exemption also limit the deemed consent to TSPs. As noted above, this limitation ignores the reality that organizations across many industries operate computer networks. They have the same needs as TSPs.

---

<sup>4</sup> See, *Reference re Broadcasting Act*, 2012 SCC 4.

The conditions also limit the ability to install a program without consent to “updating or upgrading” a network. However, there are many legitimate reasons why programs may need to be installed, including the following:

- network management, security, or the detection or prevention of unauthorized or fraudulent use of a service or system;
- safety and warranty issues, to satisfy a legal requirement (in addition to an order);
- computer programs installed temporarily during the performance of warranty or support services;
- the re-installation of a computer program (e.g., in the context of service work being performed on a computer system); and
- computer programs installed on an employee’s device by the employer’s IS department as part of a “bring your own device” program.

The conditions also limit the installation of the computer programs to the network operated by the TSP. This may not apply to platform upgrades of devices used in conjunction with the network including devices such as smartphones and network PVRs, and thus may limit its effectiveness.

We also note that there are other circumstances in which computer programs need to be installed and it would be impossible or impractical to obtain prior consent or to make the necessary disclosures. These include the following:

- computers, smartphones, tablets and other devices sold in a retail store where the software is pre-installed;
- retailers that provide computer installation, repair and maintenance service, where the technicians would not have the information to provide the necessary disclosures and it would be unreasonable to hold their employers liable for software they do not manufacture; and
- where the organization provides services in the context of one of the relationships set out in section 3 of the regulation (once amended as recommended in this letter).

CASL, unlike legislation in other countries, targets programs that have no harmful effects at all in addition to malware and spyware. It is apparent from the examples above that the sweeping approach to regulating the installation of computer programs will give rise to very significant unintended consequences.

We also note that Industry Canada proposes to use section 10(8)(a)(vi) of the Act to create the new deemed consent exemptions. However, any such exemptions are still subject to section 10(8)(b), which requires that it is reasonable to believe that the target of the program installation consents to the program’s installation. It may be that this condition would often not be met, especially in the circumstances of section 6 of the draft regulation. To address the related uncertainty, this amendment may have to be

made by an amendment to the Act to avoid creating TSP and other liability when they take bona fide self-defence measures that protect their networks, computer systems, and their customers' privacy.

Accordingly, we make two recommendations to address these issues. First, if this matter cannot be addressed through the regulations, the Government consider referring the prohibitions in section 8 to a Review Body for consideration before the draft regulations are finalized. This should include consideration of limiting the scope of the computer program provisions to malware and spyware and the appropriateness of the condition in section 10(8)(b) of the Act.

Second, if this recommendation is not accepted, that pursuant to section 64(1)(m), the following computer programs be exempt from section 8 of the Act:

- (a) a program that is installed by or on behalf of a person to prevent, detect, investigate, or terminate activities that the person reasonably believes (i) present a risk or threatens the security, privacy, or unauthorized or fraudulent use, of a computer system, telecommunications facility, or network, or (ii) involves the contravention of any law of Canada, of a province or municipality of Canada or of a foreign state;
- (b) a program that is installed, by or on behalf of a person who provides services related to the operation of the Internet or another digital network or who operates a network including a telecommunications service provider for the purposes of network management;
- (c) a program that is installed, by or on behalf of a person who provides services related to the operation of the Internet or another digital network including a telecommunications service provider for the purpose of updating or upgrading the network, or part thereof, or computer systems which are capable of transmitting data to or from the network;
- (d) a computer program that consists of an update or upgrade of a computer program the installation or use of which was expressly consented to if the person who gave the consent is consented to receive the update or upgrade under the terms of the express consent and the update or upgrade is installed in accordance with those terms;
- (e) an update or upgrade of a computer program, where the same update or upgrade is being applied or made available by the owner or licensor thereof to substantially all the users of that program, and where the update or upgrade is necessary or useful for the continued use of the program;
- (f) a computer program which is required to be installed to comply with any a law of Canada, of a province or municipality of Canada or of a foreign state, or for reasons of public safety;

(g) a computer program that was pre-installed on a computer system acquired by the person, and where the program is subject to an end-user agreement that was binding on the person at first use of the program on that computer system;

(h) a computer program installed by a person performing maintenance, repair or reinstallation services for a computer system on which the computer program is installed;

(i) a computer program installed (i) at the request of a person contacting a service provider, including the software publisher's, computer system, telecommunications facility or network provider's, or manufacturer's, help desk to install the program, or (ii) temporarily during the performance of warranty or support services;

(j) a computer program installed by a person on another person's computer system where the person has one of the relationships set out in section 3 of this Regulation.<sup>5</sup>

## **PART 2**

### **Issues Not Addressed in the Draft Regulations**

#### **7. Scope of CEMs; Service and Transactional Messages and Warranty, Recall, Safety and Security Messages**

The definition of the term CEM is very broad. It is defined in an open-ended way to be "an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity".

We understand that the Commission takes a very broad view of this definition, having publically stated that it would even include hyperlinks to business websites including home pages. As home page URLs are now equivalent to addresses on letterheads, and a great many electronic messages that have nothing at all to do with marketing now include such references, they all seem liable to be considered as CEMs. Such a broad interpretation of CASL concerns us greatly.

Under the Commission's broad interpretation of CEM, even a trade-mark or logo, in a message could make it a CEM. Providing contact information for information purposes in any product or message delivered electronically could turn the message into a CEM. The definition is so vague that businesses do not know where the line can be drawn. Or, conversely, it may lead to businesses publishing contact or home page details less

---

<sup>5</sup> Note, we intend to include the section 3 relationships, amended in accordance with these recommendations.

frequently, to avoid messages being caught by CASL, which would not be in the public interest.

The scope problem is compounded because of the drafting of section 6(6). The Act partially exempts certain CEMs from the requirement to obtain consent, including CEMs that facilitate a commercial transaction, provide warranty or safety information about a product the recipient has purchased, provide factual information about the use or ongoing purchase of a product or subscription, provide information related to an employment relationship, and deliver a product, good or service (including product updates or upgrades). However, the Act requires these CEMs to comply with the prescribed information and unsubscribe requirements.

It is unclear which of these types of messages, and whether other transactional or service-related messages, are CEMs. This uncertainty has significant impacts on compliance planning. Businesses, for example, need to know whether any of the variety of messages that they routinely send their customers – and to which customers rarely, object – are someday going to be considered CEMs based on an unknowable or unpredictable standard. This is an issue that must be resolved quickly so that businesses can scope the enormous database and systems-design tasks that CASL entails. The three-year transition period in section 66 provides no assistance because all individuals and organizations must have their compliance systems in place on the day the law comes into force. Some of these service messages may be required by law, which is another reason why the new proposed exception for compliance with laws is important. However, some are required to be sent as a matter of good business practice or to comply with a voluntary code. (e.g., the Wireless Code, currently the subject of an otherwise unrelated consultation by the Commission, that would require wireless service providers to deliver roaming alert messages to customers).

We believe that transactional and service-related messages should be exempt from the definition of CEM. We believe further that there should be no requirement to limit artificially the information contained in such messages in the ordinary course of business in order for such messages to fall within the exemption. One reason is that CASL requires giving individuals the right to unsubscribe from receiving all CEMs. If individuals choose such an option, it would be illegal to send them messages with information of importance to them and which they, in all likelihood, did not intend to unsubscribe from.

An example is notifications sent by Canadian carriers to warn consumers that additional charges may apply or that special packages are available to avoid or reduce such charges (which would clearly be to the consumer's benefit). SMS alerts sent to individuals to inform them that their wireless pre-paid account is almost depleted and in need of a 'top-up' by adding funds is another. Other examples include messages with respect to renewal of service, reminders that a subscription or maintenance service term is about to end, and messages informing bank customers that mortgages, GICs, or other investments are coming up for renewal or to provide electronic banking and other statements.

Consumers deprived of receiving such messages will blame the organizations with whom they are doing business and will not comprehend that CASL makes it illegal both to send such messages and to ask consumers in an electronic message for their consent to continue sending them after receiving a blanket unsubscribe request.

The problems associated with transactional and service messages may necessitate a message by message content review every time a message is sent by anyone in an organization to determine if it falls within CASL. This will involve extensive and very costly review of all current electronic channels to determine what changes would be necessary to ensure these types of messages do not inadvertently fall within CASL. It will also involve requiring expensive duplication of processes and systems as organizations will need to have both “non-CASL caught” versions of messages and a “CASL caught versions” for messages that may contain incidental marketing that are not normally considered spam – e.g. electronic statements that have some minor messaging around new interest rates or products that consumers really want to know about, or a logo or hyperlink to an organization’s web site.

Organizations would also need to have two versions of messages, one for recipients who have opted out of “all” CEMs and ones for those have not opted out. The inclusion of transactional and service messages such as the list of messages in section 6(6) has no element of common sense, reasonableness or scale since even a relatively minor content inclusion in the message could deem the message to be a CEM.

If customers with existing business relationships could opt-out of receiving service-related and transactional messages it would interfere with normal business operations, particularly as more and more customers communicate with businesses primarily by electronic means. Even in cases where the vendor has a non-electronic address for a client, it would be more expensive and less efficient to force a vendor to send such messages by non-electronic means. This would fundamentally violate the stated purpose of CASL, namely to promote the efficiency and adaptability of the Canadian economy.

In regards to CEMs containing warranty information, product-recall information or safety or security information, it is difficult to see any rationale for overriding applicable contracts and enabling consumers to unsubscribe from receiving these messages electronically. Moreover, these messages often come from the manufacturer, not the retailer, and therefore may not be encompassed with the definition of “existing business relationship”. Hence a wider exemption is needed.

Another important area of concern for Canadian business is ensuring that the definition of a commercial electronic message cannot be misinterpreted to include online advertising, including advertising displayed alongside other content in contexts such as websites and mobile apps. Notwithstanding that Parliament did not intend CASL to apply to online advertising, we are aware of remarks by some officials to the effect that such advertising would, indeed, be considered to be CEMs, since it encourages

participation in a commercial activity and can be directed to a computer via an IP address, Cookie ID, device IDs, or other electronic identifier or address. These types of identifiers do not have the character of email addresses or telephone numbers and were never contemplated within the context of the Act. This unfortunate ambiguity can be addressed via regulation, and save millions of dollars in litigation and the crippling of Canada's online advertising and cultural industries online.

As the Act permits private rights of action, we do not believe that the solution to these problems is to have Industry Canada and the Commission use interpretational guidelines and other guidance material to provide clarity. The frightening reality facing every Canadian organization (at least those that have heard of CASL to date) is that the Act permits private rights of action which can be prosecuted independent of the enforcement agencies' policies or priorities. Further, if there are to be limitations on freedom of commercial speech they should be prescribed by Parliament and not the agencies to which enforcing the statute has been delegated. As well, the uncertainty has significant impacts on compliance planning, which need to be resolved before the draft regulations that define the rules are finalized.

We make two recommendations to address these issues. First, if this matter cannot be addressed by regulations, that the matter be referred to a Review Body for consideration before the regulations are finalized.

Second, if this recommendation is not accepted, that at the very least, the following new exceptions be created:

An exemption under section 6(5) for the commercial electronic messages in circumstances where the only reason the electronic message would be considered a commercial electronic message is because it includes a business trade-mark or logo or hyperlinks in the message to a home page, contact page or unsubscribe page on a website of the sender or an affiliate, franchisee, franchisor, dealer or distributor of the sender.

An exemption under section 6(5) for the types of commercial electronic messages referred to in section 6(6)(a), (b), (c), (d) or (f) of the Act.

A regulation that the definition of "electronic address" in s.1(1) does not include IP addresses, Cookie IDs, device IDs or other similar addresses. Or in the alternative, a regulation, pursuant to s.6(6)(g) exempting online and mobile advertising, including but not limited to where such advertising is targeted at a specific address, device, browser or user.

## **8. Issues related to Affiliates**

Many corporate affiliates provide a variety of services bundled as a single consumer offering or market them under a common brand. Often, these products or services are from different, but related entities. There is no obvious consumer benefit in listing the individual affiliates or their franchisees responsible for specific components of their

product or service offerings. In fact, many of our vertically integrated companies and franchisors are of the view that their customers are less confused by and more comfortable dealing with providers by brand rather than by the numerous specific affiliated or related legal entities responsible for components of a given offering.

The Commission's regulations, however, require that each request for consent identify the entity seeking consent and if the consent is intended to cover affiliates or related entities such as franchisees, that such entities be fully described in the request for consent including all of the prescribed information related to each such related person. As well, each CEM must also include such information.

This problem can be solved either by the draft regulations, or ideally by amendments to the existing CRTC regulations. We recommend that Industry Canada coordinate with the Commission to revise the CRTC regulations to permit the entity seeking consent or sending out a CEM to meet the requirements of section 6.2(a) and 10(1)(b) for identifying other entities to simply refer to "affiliated entities" and/or "franchisees", "franchisors", "dealers" or "distributors", provided that such entities (1) share common branding; and (2) where it would be reasonable for the recipient of the request for consent or CEM to conclude that they were dealing with the same entity or an affiliate or an entity which is a franchisee or franchisor or dealer or distributor of the person seeking consent or sending the CEM.

## **9. Cross-border reach**

Section 6 of CASL will apply when a computer system located in Canada is used to send a CEM. CASL also applies to computer programs that are installed on computers anywhere in the world by or acting on the direction of a person located in Canada. This wide extra-territorial reach runs counter to CASL's stated objective to promote the efficiency and adaptability of the Canadian economy.

First, Canadian multi-national companies sending legitimate messages to non-Canadian customers are incited to use vendors located outside Canada to send those messages, because otherwise the messages will have to comply with unnecessarily burdensome CASL requirements. This would result in service jobs leaving the country. In fact, our group is aware of several Canadian organizations contemplating moving their foreign market-related messaging operations outside of Canada as a result of the significant disadvantage that CASL would create for them.

Second, this will discourage foreign companies from locating server farms and other facilities related to cloud computing in Canada, as both they and their customers will be burdened with the significant costs of complying with CASL even though their facilities can be used to send messages or provide services including providing software installation services on behalf of customers outside of Canada.

Third, Canadian providers of outsourced services to non-Canadian businesses will be at a major disadvantage compared to competitors in other countries. By selecting a

Canadian service provider, a foreign entity would have to comply with CASL in addition to the laws of its home jurisdiction.

Fourth, the considerable extra burdens and potential liabilities associated with CASL will discourage computer software service operations from locating operations in Canada that support foreign operations.

One simple solution would have been to create an exemption from the section 6 and section 8 requirements for CEMs and programs sent from Canada, as long as the CEM or program complied with an anti-spam or anti-malware law of the recipient country.

The Government previously rejected this proposal, stating that it “would create the potential for abuse since these commercial communications would be subject only to the other country’s legislation, if any. Given concerns that such an exemption would create a loophole that could be abused by spammers, and the difficulties inherent in determining the lawfulness of activities in foreign jurisdictions, the suggested exemption is not included in these proposed Regulations in order to maintain the intended balance in the Act.”

We do not agree. Courts in Canada routinely make findings of foreign law in the course of proceedings. There is no reason the Commission could not do the same. Moreover, we do not agree with the implicit Government policy that the ease of enforcement of CASL against a few spammers or purveyors of malware outweighs the harm that would be experienced by the ICT and related industries in Canada.

To solve these problems, we recommend adding an exemption pursuant to section 6(5) for a CEM that is sent from a computer system located in Canada to a recipient that the person has reason to believe is located in a country outside of Canada where the CEM is not sent in violation of an opt-out request and is not misleading or fraudulent.

We also recommend a regulation that specifies the following computer programs for the purposes of section 10(8)(a)(vi) of the Act, namely a program that is installed on a computer system in a country outside of Canada. We note that, pursuant to section 10(8)(b), deemed consent does not provide complete protection for such programs because the conduct of the recipients must be such that it is reasonable to believe that they consent to the program’s installation.

## **10. Closed Messaging Services**

In previous submissions, various members of this group requested that closed messaging systems such as certain short code messaging systems, (SMS) such as Line and Blackberry Messenger (BBM), be exempted completely from the requirements of CASL. Both such services involve sending messages to electronic addresses that are covered by the Act.

Closed opt-in, messaging platforms allow members to effectively manage the receipt of messages, including commercial electronic messages in a way that Internet email does

not. In so doing, they offer a level of protection that in fact exceeds that of the Act. As such, there is no need to impose the Act's consent, unsubscribe and message formality requirements, particularly given the impossibility, near-impossibility and impracticality in various scenarios of complying with them on platforms that only enable, or which are primarily designed, for, very short messages.

To have these systems subject to CASL would impose completely unnecessary and unexpected burdens on users with little to no benefit. We trust that it was never contemplated that CASL would impede or effectively make it illegal to send CEMs on modern messaging systems, yet that could be the result if this problem is not resolved.

Furthermore, in many closed messaging platforms, unsubscribe functions are not controlled by the sender but are built into the platform and the user controls the messages he or she wishes to receive. For instance, many mobile "apps" including mobile games include a setting that permits users to switch off notifications that could be construed as CEMs. Under these circumstances, it would not be possible for a sender to comply with CASL as the sender simply does not control the unsubscribe mechanism and it is the user who maintains control over the receipt of messages.

We recommend an exemption pursuant to section 6(5)(c) so that section 6 does not apply to a CEM sent to a recipient over a messaging network where (a) a commercial electronic message can only be sent from a sender to a recipient if the recipient has requested to receive messages from the sender or has given prior consent to the receipt of messages from that sender or users of the messaging network, and (b) the messaging network allows the recipient readily to discontinue the receipt of messages from senders that are specified by the recipient.

Our recommendation assumes that our recommendations regarding the definitions of "family relationships" and "personal relationships" will be accepted. If they are not, we recommend that this exemption be expanded to include "messages sent by or on behalf of a person who is participating in a messaging network to invite another person to participate in the messaging network."

## **11. Managed Messaging Systems**

In previous submissions, various members of this group also requested that managed messaging systems, such as those associated with social networking and other multi-user platforms, be exempted completely from the requirements of CASL. In responding to these submissions Industry Canada said "Another example is the concern that it would be difficult to satisfy identification and unsubscribe requirements on popular social networking services or instant messaging services. Currently, where they are not sent to electronic addresses, the publication of blog posts or other publications on microblogging and social media sites is not within the intended scope of the Act."

However, the RIAS failed to address the fact that some of the CEMs that are transmitted using these networks are sent to electronic addresses. At the very least there is uncertainty as to what components may be subject to CASL and what parts are

not. Notwithstanding that Parliament did not intend for CASL to apply to online advertising, the Commission is on record as saying publically that it is not sure whether CEMs sent to an IP address known to be identified with a person would be considered sent to an electronic address and be subject to CASL. An example would be an advertisement that is transmitted to an IP address, Cookie ID, device ID or other similar addresses associated with a person. If the Commission is unsure of the scope of CASL, the community that is subject to it (meaning every organization of any kind that might send a single CEM) will also be unable to know with any degree of certainty which parts of managed messaging systems like social networks are subject to CASL.

We recommend that this unfortunate ambiguity be addressed through a regulation expressly stipulating that an IP address, device ID or other similar addresses associated with a person is not an electronic address for the purposes of section 6.<sup>6</sup>

In any event there is no need for managed messaging systems to be regulated by CASL. Unlike Internet email (which appear to be the primary focus of the Act and regulations), many popular social networks are inherently opt-in and rules-based, with the ready availability of enforcement mechanisms. The rules are made known in advance, and typically limit the circumstances for the sending of commercial electronic messages. They also offer a level of protection that exceeds the Act. As such, there is no need to impose the Act's unwieldy and often counter-intuitive consent, unsubscribe and message formality requirements. To do so would be impose completely unnecessary and unexpected burdens on users with little if any benefit.

These types of messaging systems, like closed messaging systems, are typically designed to function in the same manner internationally. As CASL, imposes unique Canada-only requirements there are real concerns as to whether social networks including ones that are very popular among consumers and organizations, will continue to make them available in Canada for fear of potential liability for "aiding" the sending of non-compliant CEMs, the potential extent of such liability their Canadian legal advisors are unable confidently to explain or quantify.

For these reasons, we recommend an exemption pursuant to section 6(5)(c) that section 6 does not apply to a CEM sent to a recipient over a messaging network where (a) the operator of the messaging network requires that, before a user is permitted to send or receive electronic messages over the messaging network, the user enters into an agreement that requires compliance with rules for messaging activities established by the operator and applicable law, (b) the messaging network enables a user to make available an electronic address, or a means of identification that links to an electronic address, for the purpose of receiving electronic messages through the messaging network, (c) users are able to readily report violations of the rules to the operator or other enforcement authority, and (d) the operator or other enforcement authority has the right to undertake enforcement action against such violations.

---

<sup>6</sup> This recommendation is also made under the heading "Scope of CEMs".

Our recommendation assumes that our recommendations regarding the definitions of “family relationships” and “personal relationships” will be accepted. If they are not, we recommend that this exemption be expanded to include “messages sent by or on behalf of a person who is participating in a messaging network to invite another person to participate in the messaging network.”

**12. Clarifying that section 10(12) Includes transfer of all consents to Acquirer and Successor Entities**

In the context of the acquisition of a business, section 10(12) of the Act clarifies that existing business relationships between an acquired company and a third party will continue to exist after the acquisition. There are no other provisions in the Act in respect of the effect of acquisitions on other consents. This leaves purchasers of businesses potentially without consents to continue to send CEMs to those individuals for whom consents have been obtained or are otherwise available including express consents, to the “business card” and “conspicuously published” consent exceptions, and to the new implied business relationships implied consent exception.

Section 10(12) also fails to recognize that businesses will need express consents to comply with section 8. This leaves purchasers of businesses potentially without consents to continue to install computer programs, transmit messages from the computer program, and install updates and upgrades where express consents have been obtained.

The failure to recognize such consents could impair a company’s value and artificially impose business acquisition structures that may not otherwise be desirable merely to meet an inadvertent gap in CASL’s drafting.

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if a person has an express or implied consent with another person in accordance with section 10(10), and the business is sold, the person who purchases the business is considered to have, in respect of that business, the express or implied consent of the person who had such consent. A similar exemption is required for computer programs. If this inadvertent problem is not capable or being rectified through regulations, we recommend that it be referred to a Review Body for review prior to the regulations being finalized.

**13. Expanding the ‘Conspicuously Published’ Exception in section 10(9)(b) to apply to Non-Business Entities**

While uncertain, the “conspicuously published” exception in section 10(9)(b) of the Act may be interpreted narrowly so that it inadvertently limits its application to businesses. Thus, persons desiring to send CEMs that are relevant to the person’s organization, role, functions or duties in the person’s organizational capacity may not be able to legally send the CEM.

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if the person to whom the message is sent has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's organization, role, functions or duties in a business or non-business or official capacity.

**14. Expanding the 'Business Card' exception in section 10(9)(c) to apply to Non-Business Entities**

The "business card" exception in section 10(9)(c) of the Act also includes wording that may be interpreted narrowly so that it inadvertently limits its application to businesses. Thus, persons desiring to send CEMs that are relevant to the person's organization, role, functions or duties in the person's organizational capacity may not be able to legally send the CEM.

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if the person to whom the message is sent has disclosed, to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's organization, role, functions or duties in a business or non-business or official capacity.

**15. Transition and Coming into Force**

CASL contains transitional provisions intended to assist organizations in meeting the Act's requirements. They operate by purporting to "grandfather" or recognize certain consents during the three-year transition period. However, these provisions do not accomplish what is intended by the Government.

*Commercial electronic messages*

Under section 66, a person's consent to receiving commercial electronic messages from another person is implied if two conditions are met: (i) there is an existing business relationship or an existing non-business relationship, as defined in section 10(10) or section 10(13), respectively, without regard to the period mentioned in that section; and (ii) the relationship includes the communication between them of commercial electronic messages.

The transitional provisions were intended to enable organizations to continue to use consents they had already obtained from persons because of the realization that it is impossible or impractical for organizations to have or obtain express consents from everyone with whom they have relationships. However, the "existing business and non-

business relationship” categories do not materially solve the problem. The reason is that many organizations have relied on consents from a variety of sources including consents obtained under PIPEDA or comparable statutes in various provinces. The databases which are used to determine if there is a consent that permits sending a CEM were not compiled with CASL in mind. Accordingly, they do not necessarily contain data which enables organizations to ascertain whether they have either of these forms of consent, meaning that organizations may not be able to rely on them in connection with s.66.

Many companies have obtained consent to send CEMs applying the rules of PIPEDA, and equivalent provincial privacy legislation. This approach has worked well for many years and, accordingly, these consents should be grandfathered under the Act. On a going-forward basis, we also consider it sensible that the PIPEDA consents standard continue to be recognized as proper and effective under the Act. PIPEDA already calls for prior consent to send commercial electronic messages to such addresses, and when this is combined with the new unsubscribe provisions and enforcement framework of CASL, ample protection will be provided to Canadians. Enforcement authorities are given solid grounds for going after spammers who typically collect and use electronic addresses without any notion of consent. Grandfathering PIPEDA-compliant consents would significantly decrease compliance costs without undermining the objectives of the Act.

We also note that individuals can always choose if they want to withdraw their PIPEDA consent after CASL comes into force. There is no need for these consents not to be recognized. There would be minimal impact to individuals in allowing organizations to continue to rely upon PIPEDA consents they obtained prior to the coming into force of CASL. This will leave the decision up to the individuals affected. Failing to grandfather these legally obtained consents would, in effect, be taking the choice away from consumers and other message recipients.

At the very least, and to accomplish the goals of the transitional provisions, we recommend that all consents to send CEMs obtained prior to CASL coming into force that meet the PIPEDA rules should be recognized. To help with the transition, we also recommend that any such consents continue to be effective even after CASL comes into force in the same way that prior express consents continue to remain valid, until a notification of withdrawal of consent is received. This would eliminate the need to obtain new express consents and would avoid the very costly exercise of replacing all prior non-express consents during the three year transition period.

In addition, because of the all-encompassing CASL prohibitions, the limited and narrow categories of deemed implied consent and exclusions, and the uncertainty over the scope of what is a CEM, no one can predict all of the circumstances in which it may not be feasible to obtain an express consent. Accordingly, we recommend that consents obtained using PIPEDA compliant rules be acceptable until a date prescribed by an Order in Council and published in the *Canada Gazette*.

Based on the above, we recommend a regulation as follows:

(a) for the purposes of section 10(9)(d) of the Act, consent is implied where

(i) the person who sends a commercial electronic message has obtained consent in accordance with requirements of the *Personal Information Protection and Electronic Documents Act* to send the message, or

(ii) the person who sends a commercial electronic message had obtained consent in accordance with requirements of legislation of a province or territory that is substantially similar to the *Personal Information Protection and Electronic Documents Act*, or

(iii) the electronic address of the person to whom the message is sent is publically available and is specified by the regulations under the *Personal Information Protection and Electronic Documents Act* or legislation of a province or territory that is substantially similar to the *Personal Information Protection and Electronic Documents Act*.

prior to a day prescribed by an Order in Council and published in the Canada Gazette until the person gives notification that they no longer consent to receiving such messages from that other person.

Many organizations have already obtained express consents to send CEMs. Organizations have been informed by the Commission that they can rely on such consents, even if the person who sought the express consent did not comply with provisions of section 10(1), (which did not exist at the time). Because of its importance, we request that this be confirmed.

Accordingly, we recommend that a regulation be promulgated that pursuant to section 64(1)(m), if an express consent was obtained before section 6 comes into force, that the consent be deemed to have been provided for the purposes of section 6, and shall continue to be valid to the same extent as and for the same time period as a consent obtained pursuant to section 10(1).

### *Computer programs*

Section 67 provides a transitional period for computer programs. Under the section, if “a computer program was installed on a person’s computer system before section 8 comes into force, the person’s consent to the installation of an update or upgrade to the program is implied until the person gives notification that they no longer consent to receiving such an installation or until three years after the day on which section 8 comes into force, whichever is earlier.”

This transitional provision was intended to provide for a deemed consent for computer programs already installed on computer systems when CASL comes into force. However, as drafted, it is uncertain to what extent it provides protection.

Section 8 of CASL requires express consent for the installation of a computer program or, having so installed or caused to be installed a computer program, to cause an electronic message to be sent from that computer system. Section 10(7) permits the update or upgrade to computer programs where the original installation was expressly consented to in accordance with section 10(1) and (3), if the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and the update or upgrade is installed in accordance with those terms.

As a result, and notwithstanding that it is clear Parliament intended to provide businesses with a three-year transition period during which it would be unnecessary for express consent to be obtained in respect of the installation of an update or upgrade to a computer program that was installed on a person's computer system before section 8 comes into force, a drafting error in section 67 makes it uncertain whether a business can confidently rely on it.

Additionally, the transitional provisions do not permit an installed computer program to continue to function by sending messages from the computer system because no express consent under section 8 is deemed to have been obtained.

Section 67 provides for the transition period to end at the end of the three-year period. However, in many instances, there would be no way for a person to obtain an express consent for computer programs that have been distributed over the course of many years. In many cases, the person who installed the computer program, would not have contact details. Moreover, contacting the person with the computer program could violate the anti-spam provisions since there may also not be any express or implied consent to send the message suggesting the person install an upgrade. Accordingly, a person who installed a computer program well before CASL comes into force, could become subject to a liability that could not have been predicted at the time the computer program was installed.

The draft transitional provision thus may provide none of the intended benefits contemplated and intended by Parliament.

If these are problems which are not capable of rectification by the regulations, we recommend that the Government have this matter reviewed by the Review Body to consider how the issue could be rectified before the draft regulations are finalized.

Alternatively, we recommend that a regulation be promulgated that pursuant to section 64(1)(m), if a computer program was installed on a person's computer system before section 8 comes into force the person's express consent to the installation of a computer program and an update or upgrade to the program is deemed to have been

obtained until the person gives notification that they no longer consent to receiving such an installation.

### *Other Transition Issues*

In addition, we recommend that the private right of action created under CASL be suspended for at least the full transition period. As demonstrated above, CASL's provisions are very complex and its scope is very uncertain. We expect that even if all of our recommendations are put into effect, if the CASL's current structure remains substantially what it is, many organizations including potentially some of our members will face class action lawsuits by those seeking to capitalize on CASL's ambiguities and wide ambit by way of the private right of action.

Section 65 of the Act requires Parliament to review CASL after three years of it being in force. During this review Parliament could assess CASL and determine whether its provisions are, in fact, as troublesome as many including us believe. It could also assess whether these provisions are really needed or if they should be narrowed to allow for private actions to be commenced solely by service providers (which is the case under the CAN SPAM Act in the United States). We recommend that the Government not proclaim into force the provisions related to the private right of action until the completion of the Parliamentary review.

As with many stakeholders concerned about CASL, our members are appreciative of the issues addressed by the draft regulations. However, we remain concerned that so many issues of significant impact to legitimate business but ancillary to the actual purpose of the Act remain unresolved. In order for our members and other organizations to better prepare for the Act we recommend that another round of public consultation be undertaken once the Government has revised the draft regulations in response to comments received during this round and following any Parliamentary review of the issues raised here.

Last, we recommend that the Act not be proclaimed into force until at least twelve months after the final regulations have been published. While the Act may have received Royal Assent in December 2010, specific rules and regulations have remained uncertain and undetermined. This time is needed to transition to CASL, especially because CASL requires significant investments in new computer systems to develop the infrastructure to be able to comply. It would be unfair to expose legitimate businesses and other organizations to investigations (and consequent legal expenses) and potentially significant penalties until they have been given a reasonable amount of time to properly assess and implement the onerous compliance requirements.

## **PART 3**

### **CONCLUSION**

Our group fully supports the goal of developing an effective enforcement regime to combat fraudulent messages, malware and other malicious online activities, and to significantly reduce unwanted messages online. In fact, if those were all that CASL regulated, it could well be in force by now, but unfortunately CASL, as drafted, will regulate every single commercial electronic message and software installation that will ever take place in Canada. This is why detailed, principled, and authoritative legal certainty on the scope and requirements of the legislation is needed now. Our comments are driven by our members' real-life, good-faith attempts to understand and advise on what compliance measures must be designed, budgeted for, and built now. All too often, those attempts have been stymied by interpretive uncertainty and practical barriers. We remain convinced that many Canadian businesses have not even begun this challenging task, and that they, too, will discover unique uncertainties and barriers in their attempts to understand and comply with this most unusual legislation. We strongly believe that the policy objective of CASL can be achieved more effectively through more precise measures targeted at actual illegitimate activity, without unduly burdening all legitimate and well-meaning businesses with layers of costs and complexity that are not called for.

We, therefore, urge that the Government to reconsider elements of the draft regulations and to take into consideration all of our recommendations, bearing in mind that CASL is intended to protect and promote legitimate electronic commerce, not discourage it.

## **APPENDIX A SUMMARY OF RECOMMENDATIONS**

### **PART 1**

#### **Issues Raised by the Regulations**

##### **1. Issue: Family Relationship**

We recommend that the definition in s.2(a) of the draft regulations be amended to include all persons who are related by blood, marriage, common-law union or adoption.

##### **2. Issue: Personal Relationship**

We recommend that the definition in section 2(b) be broadened and drafted in a technologically neutral fashion so that it will extend to individuals who have had direct, voluntary, two-way communications and for whom it would be reasonable to conclude that the relationship is personal such as where the individuals are friends, colleagues, acquaintances, or have relationships arising out of being members of the same clubs, associations, or voluntary organizations and the person to whom the message is sent.

##### **3. Issue: Business to Business Exemption**

We recommend that section 3(a)(ii) be expanded to include a CEM that is sent by an employee, representative, contractor or franchisee of an organization to an employee, representative, contractor or franchisee of another organization if the organizations or any of its affiliates have or had a business, non-business, professional, or other relationship at or prior to when the message was sent, and the message concerns the affairs of the organization or any of its affiliates or that person's role, functions or duties within or on behalf of any such organization.

##### **4. Issue: S.4 - Referral Relationships**

We recommend that section 4(1) be expanded so that section 6(1)(a) of the Act does not apply to a commercial electronic message that is sent by a person for the purpose of contacting the person to whom the message is sent following any referral by one or more persons who have an existing business relationship, an existing non-business relationship, a personal relationship or a family relationship or a relationship that qualifies the person for the exception specified in section 3(a)(ii) of the draft regulations

with the person who sends the message as well as any of those relationships with the person to whom the message is sent and that discloses to the recipient the full name of the person who made the referral and states that the message is sent as a result of the referral, and (b) the exception in paragraph (a) applies only to the first commercial electronic message that is sent by a individual for the purpose of contacting the individual to whom the message is sent following any referral by one or more persons.

## **5. Conditions for Use of Consent**

A. We recommend that section 5(1)(b) of the draft regulations be revised as follows:

- a) The party obtaining consents should be able to satisfy its obligations using contractual measures with third parties and by conditioning authorization to use the consents on compliance with CASL. This would make third parties who use the consents in contravention of CASL fully liable for the violations.
- b) Where a message recipient unsubscribes from receiving messages from an authorized user, the authorized user should inform the consent-holder who should respect the unsubscribe for its own messages, and discontinue making arrangements with prospective new authorized users. There should be no obligation by the consent-holder to cancel all other existing arrangements due to the impracticalities associated with such a requirement. The message recipient should, however, be able to curtail messages from any such authorized user by similarly unsubscribing, which would achieve the same purpose.

B. We recommend that section 5 of the draft regulations be amended as follows:

For the purposes of section 10(2)(b) of the Act, a person who obtained express consent on behalf of a person whose identity was unknown may authorize a person to use the consent on the condition that in any commercial electronic message sent by the authorized person to the person from whom consent was obtained,

- (d) the person who obtained consent is identified;
- (e) the authorized person provides an unsubscribe mechanism(s) that, in addition to meeting the requirements set out in section 11 of the Act with respect to messages from the authorized person; and
- (f) allows the person from whom consent was obtained, by notice to the authorized person, to withdraw their consent from the person who obtained consent.

(2) The person who obtained consent must include, in the agreement with the authorized person for the use of the consent, a provision that requires the authorized person, upon receipt by the authorized person of an indication of withdrawal of

consent referred to in paragraph 1(c), to notify the person who obtained consent that the consent has been withdrawn.

(3) Upon receipt of the notice referred to in paragraph 2(c), the person who obtained consent must treat the withdrawal of consent as an unsubscribe request pursuant to section 11(1)(a) of the Act and not thereafter enter into an agreement with a person to authorize that person to use the consent.

## **6. Specified Computer Programs**

We make two recommendations to address issues associated with specified computer programs.

First, if this matter cannot be addressed through the regulations, the Government consider referring the prohibitions in section 8 to a Review Body for consideration before the draft regulations are finalized. This should include consideration of limiting the scope of the computer program provisions to malware and spyware and the appropriateness of the condition in section 10(8)(b) of the Act.

Second, if this recommendation is not accepted, that pursuant to section 64(1)(m), the following computer programs be exempt from section 8 of the Act:

- (a) a program that is installed by or on behalf of a person to prevent, detect, investigate, or terminate activities that the person reasonably believes (i) present a risk or threatens the security, privacy, or unauthorized or fraudulent use, of a computer system, telecommunications facility, or network, or (ii) involves the contravention of any law of Canada, of a province or municipality of Canada or of a foreign state;
- (b) a program that is installed, by or on behalf of a person who provides services related to the operation of the Internet or another digital network or who operates a network including a telecommunications service provider for the purposes of network management;
- (c) a program that is installed, by or on behalf of a person who provides services related to the operation of the Internet or another digital network including a telecommunications service provider for the purpose of updating or upgrading the network, or part thereof, or computer systems which are capable of transmitting data to or from the network;
- (d) a computer program that consists of an update or upgrade of a computer program the installation or use of which was expressly consented to if the person who gave the consent is consented to receive the update or upgrade under the

terms of the express consent and the update or upgrade is installed in accordance with those terms;

- (e) an update or upgrade of a computer program, where the same update or upgrade is being applied or made available by the owner or licensor thereof to substantially all the users of that program, and where the update or upgrade is necessary or useful for the continued use of the program;
- (f) a computer program which is required to be installed to comply with any a law of Canada, of a province or municipality of Canada or of a foreign state, or for reasons of public safety;
- (g) a computer program that was pre-installed on a computer system acquired by the person, and where the program is subject to an end-user agreement that was binding on the person at first use of the program on that computer system;
- (h) a computer program installed by a person performing maintenance, repair or reinstallation services for a computer system on which the computer program is installed;
- (i) a computer program installed (i) at the request of a person contacting a service provider, including the software publisher's, computer system, telecommunications facility or network provider's, or manufacturer's help desk to install the program, or (ii) temporarily during the performance of warranty or support services;
- (j) a computer program installed by a person on another person's computer system where the person has one of the relationships set out in section 3 of this Regulation.

## **PART 2**

### **Issues Not Addressed in the Draft Regulations**

#### **7. Scope of CEMs; Service and Transactional Messages and Warranty, Recall, Safety and Security Messages**

We make two recommendations to address issues regarding the scope of CEMs, Service and Transactional Messages and Warranty, Recall, Safety and Security Messages.

First, if this matter cannot be addressed by regulations, that the matter be referred to a Review Body for consideration before the regulations are finalized.

Second, if this recommendation is not accepted, that at the very least, the following new exceptions be created:

An exemption under section 6(5) for the commercial electronic messages in circumstances where the only reason the electronic message would be

considered a commercial electronic message is because it includes a business trade-mark or logo or hyperlinks in the message to a home page, contact page or unsubscribe page on a website of the sender or an affiliate, franchisee, franchisor, dealer or distributor of the sender.

An exemption under section 6(5) for the types of commercial electronic messages referred to in section 6(6)(a), (b), (c), (d) or (f) of the Act.

A regulation that the definition of “electronic address” in s.1(1) does not include IP addresses, Cookie IDs, device IDs or other similar addresses.

Or in the alternative, a regulation, pursuant to s.6(6)(g) exempting online and mobile advertising, including but not limited to where such advertising is targeted at a specific address, device, browser or user.

## **8. Issues Related to Affiliates**

We recommend that Industry Canada coordinate with the Commission to revise the CRTC regulations to permit the entity seeking consent or sending out a CEM to meet the requirements of section 6.2(a) and 10(1)(b) for identifying other entities to simply refer to “affiliated entities” and/or “franchisees”, “franchisors”, “dealers” or “distributors”, provided that such entities (1) share common branding; and (2) where it would be reasonable for the recipient of the request for consent or CEM to conclude that they were dealing with the same entity or an affiliate or an entity which is a franchisee or franchisor or dealer or distributor of the person seeking consent or sending the CEM.

## **9. Cross-border Reach**

We recommend adding an exemption pursuant to section 6(5) for a CEM that is sent from a computer system located in Canada to a recipient that the person has reason to believe is located in a country outside of Canada where the CEM is not sent in violation of an opt-out request and is not misleading or fraudulent.

We also recommend a regulation that specifies the following computer programs for the purposes of section 10(8)(a)(vi) of the Act, namely a program that is installed on a computer system in a country outside of Canada. We note that, pursuant to section 10(8)(b), deemed consent does not provide complete protection for such programs because the conduct of the recipients must be such that it is reasonable to believe that they consent to the program’s installation.

## **10. Closed Messaging Services**

We recommend adding an exemption pursuant to section 6(5)(c) so that section 6 does not apply to a CEM sent to a recipient over a messaging network where (a) a commercial electronic message can only be sent from a sender to a recipient if the recipient has requested to receive messages from the sender or has given prior consent

to the receipt of messages from that sender or users of the messaging network, and (b) the messaging network allows the recipient readily to discontinue the receipt of messages from senders that are specified by the recipient.

Our recommendation assumes that our recommendations regarding the definitions of “family relationships” and “personal relationships” will be accepted. If they are not, we recommend that this exemption be expanded to include “messages sent by or on behalf of a person who is participating in a messaging network to invite another person to participate in the messaging network.”

### **11. Managed Messaging Systems**

We recommend adding a regulation expressly stipulating that an IP address, device ID or other similar addresses associated with a person is not an electronic address for the purposes of section 6.

We also recommend adding an exemption pursuant to s.6(5)(c) that s.6 does not apply to a CEM sent to a recipient over a messaging network where (a) the operator of the messaging network requires that, before a user is permitted to send or receive electronic messages over the messaging network, the user enters into an agreement that requires compliance with rules for messaging activities established by the operator and applicable law, (b) the messaging network enables a user to make available an electronic address, or a means of identification that links to an electronic address, for the purpose of receiving electronic messages through the messaging network, (c) users are able to readily report violations of the rules to the operator or other enforcement authority, and (d) the operator or other enforcement authority has the right to undertake enforcement action against such violations.

### **12. Clarifying section 10(12) Includes transfer of all consents to Acquirer and Successor Entities**

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if a person has an express or implied consent with another person in accordance with section 10(10), and the business is sold, the person who purchases the business is considered to have, in respect of that business, the express or implied consent of the person who had such consent. A similar exemption is required for computer programs. If this inadvertent problem is not capable or being rectified through regulations, we recommend that it be referred to a Review Body for review prior to the regulations being finalized.

### **13. Expanding the ‘Conspicuously Published’ Exception in s.10(9)(b) to Apply to Non-Business Entities**

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if the person to whom the message is sent has conspicuously published, or has caused to be

conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's organization, role, functions or duties in a business or non-business or official capacity.

#### **14. Expanding the 'Business Card' exception in 10(9)(c) to Apply to Non-Business Entities**

We recommend that a new category of implied consent be recognized pursuant to section 10(9)(d) of CASL so that consent is implied for the purpose of section 6 if the person to whom the message is sent has disclosed, to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's organization, role, functions or duties in a business or non-business or official capacity.

#### **15. Transition and Coming into Force**

##### *Commercial electronic messages*

We recommend a regulation as follows:

(a) for the purposes of section 10(9)(d) of the Act, consent is implied where

(i) the person who sends a commercial electronic message has obtained consent in accordance with requirements of the *Personal Information Protection and Electronic Documents Act* to send the message, or

(ii) the person who sends a commercial electronic message had obtained consent in accordance with requirements of legislation of a province or territory that is substantially similar to the *Personal Information Protection and Electronic Documents Act*, or

(iii) the electronic address of the person to whom the message is sent is publically available and is specified by the regulations under the *Personal Information Protection and Electronic Documents Act* or legislation of a province or territory that is substantially similar to the *Personal Information Protection and Electronic Documents Act*.

prior to a day prescribed by an Order in Council and published in the Canada Gazette until the person gives notification that they no longer consent to receiving such messages from that other person.

We also recommend that a regulation be promulgated that pursuant to section 64(1)(m), if an express consent was obtained before section 6 comes into force, that the consent be deemed to have been provided for the purposes of section 6, and shall continue to be valid to the same extent as and for the same time period as a consent obtained pursuant to section 10(1).

### *Computer programs*

We recommend that the Government have issues regarding the transition and the coming into force of CASL reviewed by the Review Body to consider how such issues could be rectified before the draft regulations are finalized.

Alternatively, we recommend that a regulation be promulgated that pursuant to section 64(1)(m), if a computer program was installed on a person's computer system before section 8 comes into force, the person's express consent to the installation of a computer program and an update or upgrade to the program is deemed to have been obtained until the person gives notification that they no longer consent to receiving such an installation.

### ***Other Transition Issues***

We recommend that:

- the private right of action created under CASL be suspended for at least the full transition period;
- the Government not proclaim into force the provisions related to the private right of action, until the completion of the Parliamentary review;
- another round of public consultation be undertaken once the Government has revised the draft regulations in response to comments received during this round and following any Parliamentary review of the issues raised here; and
- the Act not be proclaimed into force until at least twelve months after the final regulations have been published.