Restoring Business Competitiveness to Canada's Anti-Spam Legislation

Issue

Canada's Anti-Spam Legislation (CASL) governs the unsolicited installation of computer programs and the sending of electronic messages for commercial purposes. CASL came into effect on July 1, 2014 with the portion governing software taking effect as of January 2015.. Other jurisdictions, such as the US (CAN-SPAM Act (2003), that require the receiver's consent to send electronic messages. CASL deviates from CAN-SPAM in a number of areas but most notably CAN-SPAM uses an 'opt-out' consent model. In an opt-out model, an individual or business may send an electronic message that's commercial in nature (what CAN-SPAM calls a commercial electronic mail message or CEMM) to someone but the sender must provide the recipient a means to unsubscribe.

CASL, on the other hand, has adopted an 'opt-in' model. Senders may only send a commercial electronic message (CEM) if they acquire consent first or meet an exception. Like CASL, Australia's Spam Act (2003) is one of the few models globally that require an opt-in consent. However the Australian model uses the concept of "inferred" consent to create much broader exceptions to the law than are available in Canada:

"via an existing business or other relationship, where there is reasonable expectation of receiving commercial electronic messages"

Unlike Australia's Spam Act, CASL's business relationship exceptions are time limited, forcing the removal of contacts from distribution lists when no two way communication has occurred.

To complicate matters further, Canada has two consent regimes – one for privacy legislation and one for CASL. Bill S-4(changes to the Personal Information and electronic Documents Act – PIPEDA) added a major new requirement for obtaining consents pertaining to the collection, use and disclosure of personal information but is still inconsistent with the requirements of CASL.

Background

CASL has been widely criticized by businesses and the legal community across the country.

In March 2015, Network Seurity Firm Cloudmark noted that while CASL has been effective in reducing the volume of spam coming from inside Canada, it had no effect on reducing spam received in Canada from other Countries, which had actually increased. More importantly, they noted that there was a 29% decrease in legitimate email traffic, confirming the fears expressed by business prior to the implementation of CASL that the law would have a chilling effect on electronic marketing:

This new law represents staggering overreach by regulators, is unnecessary due to basic tech solutions and it seems to me most importantly, the law illustrates a serious and profound disconnect between federal legislators and regulators on the one hand and the realities of Canadian business (and their need to market to effectively compete) on the other (http://digest.dx3canada.com/2015/04/28/data-finds-casls-feared-chilling-effect-on-business/)

In a July 9, 2014, Huffington Post article, Dan Kelly, the President at the Canadian Federation of Independent Business (CFIB) cites that "62 per cent of small firms have done nothing to meet the new requirements."

In a July 4, 2014 article, Mark Goldberg, a prominent technology consultant and blogger wrote, "Our government has imposed yet another impediment to the adoption of e-commerce and information technology in Canada. It is another contributor to lower levels of competition across the board in Canada's economy."

Borden, Ladner, Gervais LLP, Partner Jeffrey Graham, in a July 3, 2014 Financial Post article wrote, "A simple opt-out regime would have avoided the complex transitional rules that have been created… Why would it not be enough for the law to simply provide that if there is an existing relationship, broadly defined, and an effective opt out right clearly identified in the promotional emails, the public interest is adequately protected?"

Businesses across Canada have struggled with implementing CASL.

Almost all businesses are falling into one or more of these categories:

- Spending a disproportionate amount of money on legal consulting, operational processes, staff training, and human resources to fully implement the legislation, and/or,
- Not in compliance and violating the law, and/or,
- Have opted for alternatives to electronic marketing to avoid the risk of prosecution.

These issues demonstrate the government has not met its objectives:

To bring into force legislation that is intended to deter spam and other damaging and deceptive electronic threats such as identity theft, phishing and spyware from occurring in Canada and to help drive spammers out of Canada, in a way that phases in the violations and enforcement mechanisms over a three year period…and to protect Canadians while ensuring that businesses can continue to compete in the global marketplace.

Disproportionate compliance spending hurts the Canadian economy. Businesses could be spending this money on innovation, hiring, marketing, and expansion.

Companies that exit the electronic marketing ecosysytem creates a less competitive environment in Canada and makes Canada less competitive globally. Mark Goldberg, in a July 4, 2014, article wrote, "Commercial Electronic Messages – and I mean otherwise legal, non-fraudulent, non-malicious messages – increase competition and expand market knowledge. Why would we want to block increased competition?" (http://mhgoldberg.com/blog/?p=7337)

Companies outside Canada continue to send CEMs to Canadians, violating CASL. Extra jurisdictional enforcement mechanisms are insufficient to these illegally sent CEMs. While this continues, Canadian businesses are scaling down their email efforts. This puts Canadian companies at a disadvantage against foreign competition.

Here are the specific issues with the CASL legislation that businesses are struggling with:

1. *Information requirements for acquiring 'express consent' are onerous.*

When collecting consent information, a business must disclose all of the following (s. 10(1) and s. 4 of the CRTC regulation):

- Name of the company
- Mailing Address
- Either phone, email or web URL
- According to regulators, the user must make an affirmative action to subscribe (ie. opt-in check box or providing their email)
- Consent message – And the consent message needs to have details as to what the company is going to do with their information and mentioning that the user may unsubscribe at any time.

Information requirements differ depending on whom the consent is being sought on behalf of. The complexity and technical requirements often require legal and IT consulting assistance.

2. *Managing the deadlines around implied consent is too difficult.*

Under the implied consent provisions of CASL, a company may send CEMs to someone for up to 2 years from the date of last purchase and 6 months from the date of the person's product/service inquiry (s. 10(10)).

This section of the Act appears simple enough but many businesses are struggling with its implementation. For instance, consider this:

- Software is logistically necessary to track leads and structure data entry. This software must be configured to purge contacts when lead's implied consent expires. The software (or through human process), must track when a lead becomes a customer as that will re-trigger the two year rule (s. 10.10.a)

- The software (or through human process), must track when someone re-purchases, re-starting the two year rule.

This solution to implement (whether developing/implementing software or hiring staff to manage) can cost individual businesses tens of thousands of dollars or more annually to maintain.

3. *Many of the exceptions are too vague.*

Many exceptions are too vague. For instance, s. 3(d) of the CRTC regulation states:

"Section 6 of the Act does not apply to a commercial electronic message… (d) that is sent and received on an electronic messaging service if the information and unsubscribe mechanism that are required under subsection 6(2) of the Act are conspicuously published and readily available on the user interface through which the message is accessed, and the person to whom the message is sent consents to receive it either expressly or by implication."

Under CASL, an electronic address is broadly defined as an address used in connection with the transmission of an electronic message to an email account, a telephone account, an instant messaging account or any other similar account. The notion of "similar account" has generated much debate about the application of CASL to social media. In response, the CRTC has affirmed that certain social media accounts may constitute a "similar account," yet has stated that the determination will have to be made on a case-by-case basis.

4. *Record keeping standard is difficult to achieve*

According to regulators, consent can be achieved by not only digital or written format but also verbal. However, section 13 puts the onus on the sender to prove consent. This has created a predicament for businesses. They may have acquired valid consent but are unable to document in a sufficient way to meet the challenge of a future audit or civil law suit.

5. *Private right of action.*

As of July 1, 2017, individuals can bring forth legal action against a party they believe has violated CASL (s. 47).

In CASL's current iteration, compliance is out of reach for many businesses due to cost and complexity. The risks associated with electronic commerce will be further exacerbated by the threat of civil litigation.

In comparing this section to CAN-SPAM to see how other jurisdictions have addressed this topic, CAN-SPAM provides no such right of action to private individuals, nor does the Australian Spam Act (2003). According to Sharon E. Groom, a lawyer at McMillan, "Apart from a state attorney general, only *ISPs* who have been 'adversely affected by a violation' can bring an action under *CAN-SPAM*."

6. *Inaccurately purging people from their lists.*

Section 66 of CASL (transitional provisions) allows businesses up to three years to send CEMs if certain pre-requisites are met.

Unfortunately, what has occurred is many businesses (out of misunderstanding the section or receiving poor advice), went and sent out the express consent request email blasts (pre July 1) and purged anyone that didn't respond. Some of those purged, the business may have still had implied consent (under the existing business relationship rule) and didn't know any differently.

Another segment of businesses would have missed the transitional provisions opportunity entirely by not sending out a CEM to those recipients pre-July 1 (sending a CEM pre-July 1 2014 is one of the pre-requisites under s. 66).

7. *Vicarious liability.*

Section 53 creates potential personal liability for officers and directors of corporations that violate CASL where due diligence is the only defense. This is extreme.

Recommendations

That the federal government make the following reforms to CASL in order to prevent this legislation from putting Canadian businesses at a competitive disadvantage:

1. Add in a new form of implied consent, recognizing the concept of inferred consent used in the Australian model that allows communication between parties where there is a reasonable expectation of receiving commercial messages and without time limits.
2. As a result of the amendment to PIPEDA in bill S4 , recognize all consents that would be recognized as valid under the standards for consents in PIPEDA
3. Clarify in regulation that two connected people or businesses on an existing social network (eg. Facebook, Linkedin, etc.) are deemed to have implied consent without time limits.
4. Remove the "Right of Action" from CASL. While individuals should still have the right to report inappropriate CEMs to federal regulatory bodies, they should not have the right to sue senders in the civil court system.