CASL: A high-level look at the looming disaster

Sometimes Chicken Little is right. The sky is about to fall on every company that sends commercial email to any Canadian.

This is a large complicated issue to be digested in parts. Today is a high-level look at the looming disaster and we'll get into details over the next few weeks.

It's hard to believe that antispam legislation can be this disastrous, but it's true. This is real. General Counsel, Risk Management and Compliance across Canada are scrambling to understand and then get in front of this issue, and the litigation lawyers see fortunes to be made from this. It is a massive problem and will get worse, with civil and criminal ramifications.

First off: CASL. Canadian AntiSpam Legislation. The full text of the statute is here. It applies across Canada, in every province and every territory.

Canada has the reasonable goal of wanting to increase the economy's efficiency by discouraging spam. To help achieve this goal, under CASL, before you send an email for a business purpose you must have the intended recipient's express or reasonably implied consent. If as the sender you can't prove you had consent BEFORE you sent the message, you have sent spam and are in breach of CASL. If there is prior consent then it's not spam and not a CASL breach.

(That's a simple non-legal summary of the legislative impact. Next week we'll get more technical with a more granular examination of the statutory definitions and exceptions.)

CASL compliance is about consent, not content. You need

consent BEFORE you send the email. You cannot email someone to ask for consent to send that person email. If challenged, the onus is on you as the sender to prove you had prior consent.

Actually, it’s worse than that.

CASL applies not only to email but also to text messages, software updates, cookies, push marketing, BBMs, and any form of communication intended for an electronic account. It doesn’t matter whether the recipient is receiving the communication on a desktop, laptop, smartphone, tablet or smartTV, directly by email or through Facebook for business. It doesn’t matter whether it’s by WiFi, Bluetooth, NFC or ethernet; at home or in the mall; in the office or on the road. If you can’t prove you had consent BEFORE you sent the message to an account, you are in breach of CASL.

That’s draconian. And it’s even worse than that.

Every message you send must have a built-in unsubscribe feature. Must. If you don’t, you’re in breach of CASL.

The consequences of being in breach of CASL can be disastrous, including an investigation by the Canadian Radio-television Telecommunications Commission (CRTC) and possible fines. The maximum penalty for a violation is $1,000,000 for an individual and $10,000,000 for a corporation (section 20(4)). This doesn’t include the legal cost of defending against the investigation or the public relations fall-out that would have to be managed.

The statute is so broad, the consequences so harsh, that most of us in the compliance industry did not think it could be rigorously enforced. The CRTC simply lacked the resources or the will to enforce CASL in any meaningful way.

We were wrong.

In March of 2015, the CRTC gave notice of its intentions when

it punished a numbered corp with an administrative monetary penalty of $1,100,000 for having sent emails without the recipients' consents as well as for sending commercial emails that did not have a properly functioning unsubscribe mechanism. We didn't criticize the penalty since the numbered corp was what we normally think of as a true spammer – atta go, CRTC!

Then Plenty of Fish got hit for $48,000. We didn't really care since it's a free dating website, so we all just giggled a little, albeit nervously.

We began to really care in June of this year when regional flyer Porter Airlines was hit by the CRTC for $150,000 for CASL breaches. And we really paid attention a few weeks ago when Rogers Communications agreed to a $200,000 fine, for the "offence" of sending corporate emails that did not always have a fully functioning "unsubscribe" mechanism.

Look at the email you send. Is there a fully functioning unsubscribe mechanism in every email you send?

Here is the link to the government of Canada's website for these decisions.

These is some policy wisdom behind this for the empire builders at the CRTC. The CRTC has found itself marginalized over the years. There is no relevant battle left to be fought over television. Cable now polices itself – Bell watches Rogers who spies on Cogeco who tattle-tales on Shaw. Outside of the internet the CRTC has been reduced to a responsible parent in a room of sneaky but studious teenagers.

But on the internet, the CRTC has room to flex its muscles and carve out a space for itself.

And carve it is. The monetary penalties described above are bad enough. Then last week the CRTC announced it had issued its first warrant under CASL, aimed at a Toronto botnet server

as part of a global effort to combat the Win32/Dorkbot malware. The warrant was granted by the Ontario Court of Justice and was carried out with the RCMP's assistance.

A warrant is a court-blessed invasion into your affairs, allowing a law enforcement official to enter your home / business / car and peruse your personal affairs. Warrants are useful but dangerous government tools.

No one is going to complain about the CRTC getting a warrant to help attack a dangerous virus family, and that makes it the easy thin edge of the wedge. The larger question is, just as the CRTC went after Porter Airlines and Rogers after penalizing the true spammer, who will be next in the CRTC's gunsights?

I have met with numerous companies to advise on this issue and assist them with getting into CASL compliance. They know that if challenged by the CRTC they have to be able to PROVE they are in compliance. That will consume IT and human resources as these issues are addressed. To date, I have seen only three companies that I believe are in full CASL compliance – everyone else is at risk of a CRTC investigation and penalty.

Wait, it gets even worse than that.

On July 1, 2017, anyone who alleges being affected by a CASL breach can apply to a judge for a order against the offender. In other words, I can sue you if you send an email to me and I don't think I gave you consent in advance to send it. Then the onus is on you as the sender to prove you had my consent BEFORE you sent me that email.

The class action litigators are drooling over this. Director and officer insurance premiums will be affected as section 44 does impose liability for some corporate acts on the officers and directors. Data riders to general liability insurance will have to be purchased. Companies, both public and private, will have to be able to prove they are in CASL compliance or face

class action litigation.

It is that bad and it is the law of Canada.

We will come back to CASL over the next few weeks to look at the law in greater detail. There are some exceptions and backdoors to be aware of, and the definitions matter. Until then, look at the email you send every day: are you in compliance? If not, you could be next.