# Strap on your Helmet …

… and put in your mouthguard. The summer of 2017 is going to be brutal.

I'm not talking climate change, TrumpAftershock, the death of bumblebees, racism, the global shortage of cobalt or a refugee crisis. This is about the world-wide implications of the CRTC (Canadian Radio-Television and Communications Commission) enforcing Canada's AntiSpam Legislation (CASL).

Unless you like paying global lawyers obscene amounts of money, pay attention.

The background to CASL is here. There are hotlinks in that article linking backwards to prior articles looking at the broad scope of the legislation, the search warrants already obtained by the CRTC under CASL (!!!), and the incredibly high standard of compliance required to meet the law.

CASL really has only two key requirements. The first is that you, as the sender of a commercial electronic message (CEM) (including *any* business email or text), are prohibited from sending that CEM unless you can prove you had prior consent to send it to that person. You have to be able to prove you had prior consent. You can't email someone to ask for consent to email them.

Second, all CEM's must be transparent – it must clearly disclose who the sender is and it must include a simple unsubscribe link. This element is fairly straightforward. If you apply some business intelligence, human resources training and forethought, you can comply with this part of CASL.

It all seems simple, doesn't it.

Whether you like these two elements is not relevant. This has been the law in Canada for several years. It doesn't matter if you think it's a silly law or a disproportionate one – this is a law with global exposure, as the CRTC has assumed jurisdiction if the email is sent or received in Canada (just passing through an ISP doesn't count). Does your business operate outside of Canada but email into Canada on occasion? You're caught. Are you a Canadian business sending any email outside of Canada? You're caught too.

It doesn't matter if you don't think you're sending spam. Technically, even the sending of one errant email brings you within CASL's walls.

The first element above is going to be the one that gets you in trouble. The CRTC seems to think so, too. Last week the Enforcement Branch of the CTRC issued an Enforcement Advisory titled "Notice for businesses and individuals on how to keep records of consent". It's a short scary document – please read it and then come back.

Scary, eh? How's this sentence from the Advisory: "The onus of proving consent always remains with the person(s) sending, causing or permitting the sending of CEMs."

This reminds me of my time articling with Gord Wood and Geoff Adair. I began litigating, believing in the romantic abstraction that truth will be revealed and justice will be served. Mr. Adair, a renowned insurance litigator, knocked it into my naive head that the truth doesn't matter in a court of law – only the truth you can prove. Find your facts, go get

the evidence you need. What evidence do you have to support your position? If you can't prove it, it doesn't matter.

Likewise, the having of consent under CASL is not relevant. What matters is being able to *prove* you had that prior consent. Not being able to *prove* you had prior consent is the same as having no consent at all. You lose.

The CRTC has given all of us fair notice that this is the standard it expects to be met. You can't say you weren't warned.

But a CRTC isn't really the problem. The Commission's limited resources mean you can probably sleep at night without worrying about the CRTC showing up at your office tomorrow. What you should be afraid of is July 1, 2017. Mark that date in your calendar. That's the day when your company's breaches of CASL, until then relatively innocuous, can be punished by a private right of action. Anyone to whom you send an email or text will have the right to sue – all they have to prove is that they received your message, and then the onus shifts to you to prove you had prior consent to do so.

That's what CASL itself and the CRTC's Enforcement Advisory are telling us.

After you get sued, you will then need to put forward evidence that you had prior consent to send that email. This would be part of the discovery process in the litigation, and since this type of litigation supports class action litigation, your legal bills are going to be astronomical. And if any of the recipients are outside of Canada, watch for creative aggressive plaintiff counsel to figure out ways to trace liability back to that jurisdiction. Double the litigation, double the legal expenses.

Those legal bills may not be covered by insurance. To date, to the best of my knowledge, no insurance company has yet written a policy that will cover legals for CASL breaches, or pay

damages for those breaches. (I met someone in Winnipeg who thought there might be an Alberta insurer underwriting this under a broad Comprehensive General Liability policy, but I haven't seen it yet.)

Think of the CRTC having jurisdiction as being the pre-season. The season starts in 11 months when the private right of action is created. What do you need?

1. a senior executive to champion the creation and implementation of your compliance model
2. a senior executive to supervise compliance and respond to potential breaches
3. Human Resources to add sections to the Employee Handbook on the proper use of email addresses and phone numbers
4. initial training of all staff, directors and management
5. annual testing to ensure continued compliance
6. a technology model that has been architected to achieve all the business goals set out in CASL and as interpreted by the CRTC
7. initial and on-going stress testing of the system

All of these items work together to create your due diligence defence.

This is not an easy list and it cannot be satisfied overnight. My best advice is to immediately investigate the out-sourcing of the technology model on an ongoing basis, and create your own internal HR and corporate policies to show best practices.

You're in the game whether you want to be or not, so get your equipment on.