The CASL Fines are Starting to Pile Up

The CRTC recently rolled out another conviction under CASL.

Here are the barebones of CASL compliance from a video interview last January:

CASL is a piece of legislation with good intentions. It's meant to enhance Canada's economy and increase efficiencies by eliminating waste. That sounds great. What the government has done is passed a law that says if you send an electronic message to another person's account you must have that person's consent before you send that message. Notice it doesn't say email. It says electronic communication. Notice it doesn't say email account. The legislation reads, to an account. As a result it is so broad, so encompassing, that it catches every aspect of your business.

After talking about it since 2012, it was about a year ago that we started emphatically writing about Canada's AntiSpam Legislation ("CASL"), when we wrote, "it is by far the most pernicious legislation I've ever seen."

In another article we called it "corporate ebola" and elsewhere said that it poses a tremendous uninsurable risk for every business sending or receiving email in Canada.

We also warned that under CASL the CRTC (Canadian Radio-Television and Telecommunications Commission) had the power to obtain warrants, enforceable by the Royal Canadian Mounted Police. We can't think of anyone who took it seriously at the time. They did when the CRTC obtained and enforced two warrants under CASL. Suddenly businesses were paying a bit more attention.

Other companies have treated CASL casually, and paid a hefty

price. Look at CompuFinder (fined $1,100,000 for CASL infractions), Porter Airlines ($150,000), Plenty of Fish ($48,000), Rogers Media ($200,000) and Kellogg's ($60,000).

From inside sources we know that Rogers' legals for internal and external counsel was roughly $2,000,000, not including lost time and the resources then consumed by an after-the-fact compliance effort.

Look at the article here for background and links to prior articles spelling out what CASL is, what its requirements are, and why it will be extremely difficult to comply without a management-led attack on the issue.

The CRTC has told us it will enforce CASL to exacting high standards. An Enforcement Advisory published earlier this year described those very high standards.

That's all background. On October 26, 2016, the CRTC found that Blackstone Learning Corp. committed nine violations of CASL by sending commercial electronic messages without consent, and imposed an administrative monetary penalty (AMP) of $50,000 on the company. The really scary part was that in the original notice of violation, the CRTC was seeking a AMP of $640,000. Six hundred and forty thousand dollars, for sending business emails.

Scary.

So picture Blackstone getting that Notice of Violation. Its board of directors had a difficult decision to make: pay the $640,000 AMP, or pay its lawyers a crippling amount of money to fight the CRTC in the hope of having that AMP reduced to a manageable level. I don't know how much Blackstone paid, but I do know the legal industry, so my guess is the legals for this process were at least $300,000. Not an easy decision.

Blackstone sent emails primarily to government employees, advertising educational and training services offered by the

company. The employees complained to the CRTC that they had not consented to receiving those emails. The onus was then on Blackstone to prove to the CRTC that it had prior consent to send the emails. Since Blackstone could not prove on a balance of probabilities that it had express or implied consent, the CRTC found Blackstone guilty.

The Blackstone facts also addressed the internet practice known as “scraping”. Also known as “web harvesting” and “web data extraction”, scraping is an automated process that extracts information from thousands of websites. In this context, the target information is all email addresses posted at that website, and then the scraper will use that contact information to market its services to those email addresses. How those publicly posted email addresses can be legally used is called “the conspicuous publication exemption”.

For the first time, the CRTC offered a detailed analysis of the “conspicuous publication exemption” found in section 10 (9)(b) of CASL. That’s the good news, as it provides guidance and some certainty for compliance departments and Heads of Risk. The bad news is, the CRTC interpreted the exemption fairly narrowly, which guarantees future violations.

Here’s the CRTC’s own words from section 28 of the reasons:

Paragraph 10(9)(b) of the Act does not provide persons sending commercial electronic messages with a broad licence to contact any electronic address they find online; rather, it provides for circumstances in which consent can be implied by such publication, to be evaluated on a case-by-case basis. Pursuant to section 13 of the Act, the onus of proving consent, including the elements of implied consent under paragraph 10(9)(b) of the Act, rests with the person relying on it.

In its reasons, the CRTC did knock down the AMP to $50,000 from its initial $640,000, but think of the incredible legal fees Blackstone had to incur to achieve that. And that’s the

reason we get so worked up about CASL; it’s not the potential for fines, it’s the staggering legal costs involved in defending a Notice of Violation. There aren’t many companies that can digest millions of dollars of uninsurable legal fees.

And it’s going to get worse. As of July 1, 2017, the CRTC isn’t your worry. As of that date, a private right of action will be created, which means that anyone can sue you and allege that you breached CASL. Then, as the CRTC pointed out in *Blackstone*, “the onus of proving consent … rests with the person relying on it.”

That private right of action is supportable by class action litigation, with plaintiff lawyers working on contingency. Meanwhile, the legal defence fees will be in the millions of dollars.

It’s cheaper to get into compliance than to pay your lawyers. Get into compliance with CASL now.