



Don't Get Too Excited for the Second Phase of Canada's Anti-Spam Law

Government

Technology, Privacy, and eCommerce



On January 15, 2015, the second stage of Canada's Anti-Spam Law (CASL) went into effect, this time focusing on software installation. If it is anything like the first phase of the law, which required consent to send a commercial electronic message, be prepared for a disruptive, confusing and unproductive regulation that will not yield the desired results.

The genesis of CASL is certainly noble. The goal of the legislation is to curtail the amount of unwanted spam, spyware and malware that ends up on computers of private Canadian citizens. The Canadian business community sounded alarm bells during public hearings but a few small changes amounted to little and the law was passed almost as drafted.

The flurry of emails filled Canadian inboxes in the weeks leading up to July 1, 2014, when the first phase of the law went into effect. Any company that communicated with a Canadian customer sent an email to request an extension of the business relationship. Facebook, Amazon and any other business, from newspapers to daily deal sites to ACC, bombarded customers with opt-in language. One of the few benefits of the legislation was a chance for removal from old business contacts.

Ironically, a law designed to decrease the amount of emails received resulted in a deluge of emails requesting the receiver to opt-in and consent to further communications.

July 1 came and went. Spam continued to pile up. Sexual enhancement pill advertisements stacked above emails from neglected princes in far away lands. In short, not much changed.

The law's jurisdictional scope was its Achilles heel. The severe penalties for noncompliance, including criminal and civil charges and personal liability for company officers and directors up to \$10 million, do not apply to non-Canadian entities. The vast majority of spam comes from overseas. In

essence, the law is creating more work for legitimate Canadian companies because they need to jump through its tangled regulatory framework.

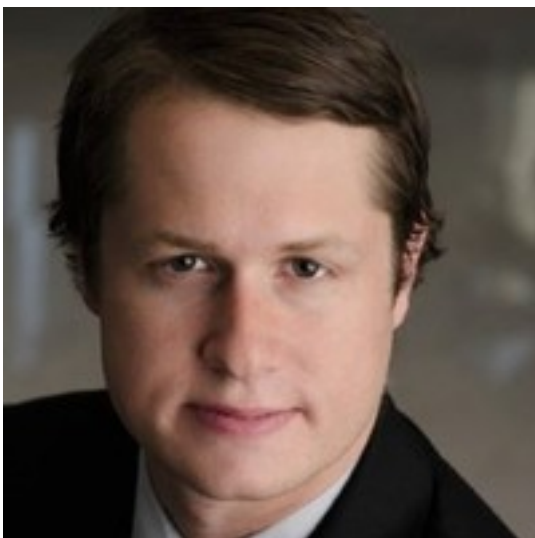
“If you’re a software manufacturer, it’s going to be extremely important that you are on top of regulations and how they are going to work,” says Robert Piasentin, general counsel for Sierra Systems, an IT services firm based in Vancouver, British Columbia. “If you’re a Microsoft or an Adobe, you aren’t likely to be installing malware or spyware anyway. But everyone will have to take the time to learn the regulations, implement the steps to be compliant and that is going to affect your bottom line.”

Piasentin says nothing has changed post-legislation and has no doubt that the second phase of the law will be equally unproductive.

“In reality, it hasn’t been a great victory and it has really caused a lot of grief and cost a lot of money that shouldn’t have necessarily been spent,” he says. “But the voters who will complain about it will probably be in the minority so it’s worth the politician’s gamble for them.”

The next important date for CASL is July 1, 2017, when the transitional period for commercial electronic messages ends and the three-year mandatory review for CASL will start.

[Joshua H. Shields](#)



Editor

Association of Corporate Counsel