Canadian HR Reporter
THE NATIONAL JOURNAL OF HUMAN RESOURCE MANAGEMENT www.hrreporter.com
REPRINT

New CASL deadline looms

Private right of action could mean costlier penalties

BY SARAH DOBSON

JUST over three years ago, employers faced a daunting headline: Compliance with Canada's anti-spam legislation (CASL) by July 1, 2014. Essentially, that meant any commercial electronic messages (CEMs) such as emails or texts sent by employers needed consent, identification information and an unsubscribe mechanism. The installation of computer programs without express consent was also not allowed, and there were restrictions around the collection of personal information and electronic addresses.

Over the transition period that followed, companies were allowed to rely on "implied consent" based on a prior relationship and prior communications with recipients. But that grace period is ending as of July 1, 2017 — and, this time, the potential penalties are more severe.

So, are employers ready? Not really, according to legal experts.

"I have yet to run into any of them that were in compliance before I got there," said Peter Clausi, executive vice-president of corporate affairs and general counsel at GTC Resources and Mining in Burlington, Ont. "Firms aren't taking it seriously."

Employer compliance is all over the map, with larger companies more on top of it, said Kirsten Thompson, a partner in the national technology group at McCarthy Tétrault in Toronto.

Many employers feel the rules don't really apply to them because they're not spammers — but the legislation is very broad, she said.

"It's also very vague, which makes it hard to comply with. Even if you are the most diligent company in the world trying to put in a client strategy, it's very difficult to determine what the difference is between a permissible transaction email and impermissible personal electronic message — there are definitions but there's a lot of vagueness."

A number of prosecutions by the Canadian Radio-television and Telecommunications Commission (CRTC) have hit companies that weren't making particularly rigorous efforts, she said. And with some brand name companies, it was more about a technical or administrative oversight, "which emphasizes the need for routine audits of your processes."

In some cases, it was about inappropriate timelines, while in others, it was about emails sent by a third-party vendor not following process, said Thompson.

"These are reputable companies that you'd never think they'd fall under the category of egregious spammers but they nonetheless got tripped up by the technical requirements of the legislation."

In 2015, Porter Airlines, for example, agreed to pay $150,000 for alleged violations concerning its unsubscribe mechanism, and being unable to provide proof it obtained consent for some electronic addresses.

And in 2015, a notice of violation was issued against training school Compu-Finder, with a penalty of $1.1 million, after an investigation found the company sent CEMs without the recipient's consent, as well as emails where the unsubscribe mechanism did not function properly.

Private right of action

But employers will want to get it right come July, as that's when CASL's private right of action (PRA) comes into force. This allows individuals and organizations who are affected by an act or omission that is in contravention of the law to bring a private right of action in court against these individuals and organizations. It will allow an applicant to seek actual and statutory damages, though the latter may not be pursued if the person or organization against whom the contravention is alleged has entered into an undertaking or has been served with a notice of violation by the government.

The potential remedies are significant, according to David Young at David Young Law in Toronto. In addition to actual losses or expenses, people who feel wronged may be able to recover, without any proof of loss, $200 for each non-compliant CEM — up to a maximum of $1 million per day — or, in the case of computer hacking, misleading electronic messages or email harvesting, up to $1 million per day.

"The potential risks of private litigation under the PRA, and particularly in the event of a class action, could be — not to be understated — potentially devastating and point to an important need for organizations to focus on their CASL-related risk management and avoidance strategies," he said.

Where previously a violation was just subject to regulatory action, after July 1, there's a private right of action involved, said Thompson, so anyone who's received an offending email is in a position to sue and recover statutory damages.

"As a class action, there's a significant amount of money potentially at stake. So that's caught a lot of people's attention. So a lot of companies are reviewing their CASL compliance efforts that they've put into place one, two, three years ago to make sure they're actually being followed and their efforts are up to date."

It's going to be interesting to see how the tribunal interprets the legislation because it's possible this right of action can be taken without any proof of damages, relying on the $200 provision, said Antoine Aylwin, a partner at Fasken Martineau in Montreal.

"If the tribunal accepts that principle, we could very well see many class actions taken and it goes fast — when you send an email to 1,000 persons, well, it's $200,000 per communication, so say you send five, you're at $1 million, just by the mathematics of it."

And when it comes to any al-

leged contravention of CASL, the defence of due diligence applies, said Young, meaning a person will not be found to have contravened a provision if she can establish she exercised due diligence to avoid such non-compliance.

This involves not only putting in place compliant systems and procedures, but also reviewing them on a regular basis and, where necessary, making adjustments to ensure they meet the legislative requirements, he said.

As a due diligence offence, an employer is guilty unless proven innocent, said Clausi.

"So all the CRTC has to say is 'Johnny Smith over there alleges you sent him email, he did not consent in advance. Did you?' The onus then shifts to you to produce all your records — not just ones involving Johnny but everybody — to prove that your pattern of behaviour is such that you did not commit that act concerning Johnny or anyone else," he said.

"It is an incredible exercise. I know a few companies who have received a notice of violation and their legal cost to respond is roughly half-a-million dollars… Because nobody knows about it, my thinking is this is where the plaintiff class action will feast. Ignorance of the law is no excuse."

It's also important to remember the liability could also go on the directors, "so the consequences are huge," said Aylwin.

"It might well lead to debates on the reach of the D&O (directors' and officers') insurance policies because to go to the directors and officers, there might be allegations of knowingly letting the emails be sent and if it's intentional, well, typically the insurance policy will not cover intentional behaviours."

HR's involvement

From the start, the CRTC has been saying human resources needs to be involved, said Clausi.

"HR is a key element of any initial compliance solution and must be the driving force behind ongoing compliance. Compliance without human resources is not compliance."

The government has said employers need to designate a senior official to be the point of contact for all CASL issues, and designate another senior executive responsible to respond to any data or CASL breaches, he said. Plus, all employees must be properly trained on CASL, and disciplined if they breach CASL — and these are all activities involving human beings, said Clausi.

"In a perfect world, HR is actively engaged in this, as it must be in other data-related issues."

The heightened compliance focus gives employers reason to redouble their efforts to have training in place for employees, said Young, "which a conscientious, diligent employer would have had already, with persons in communications, marketing, whatever, in their CASL compliance programs. So it behooves employers to redouble those in light of the heightened compliance focus that will come into effect on July 1," he said.

"It's not only important to give the guidance through policies, procedures and training sessions, but I'm seeing increasingly a heightened standard where you should be testing the employees to confirm they do understand it, so simple acknowledgement may not be enough. And that would certainly improve your due diligence standard."

Much of the focus should be on the marketing department, which sends out the most CEMs, and training is important, said Aylwin.

"And make sure that you have the proper technological environment to manage consent, and communications, and to keep track of all this because this is all needed by the legislation," he said.

"Make sure that everything that would be seen as electronic commercial messages, the management of it, should all be centralized within the company because compliance could be very difficult to manage if you do not have a centralization of either communications or at least guidelines… you put yourself at risk."

Education and updated policies are a good chunk of what's required, along with looking at consent, said Thompson.

"If they haven't looked at deemed consent and can't find either a relationship to ground the validity of the message or they haven't sought expressed consent, a number of companies are now pushing before July to get that expressed consent. "

In addition, if a company is audited on an annual basis, there will be qualitative tests in addition to quantitative ones starting in 2018-19, said Clausi, and the auditor will be required to make a judgment call on the quality of management.

"Part of that is looking at compliance with all laws and regulations. CASL will become a large enough problem that the auditor will have to say, as part of his management rep letter: 'Are you in compliance with all known laws and regulations? Are you in compliance with CASL?'… And then the auditor will have to make disclosure in the audit of non-compliance."