OSLER

Preparing for CASL's private right of action

APRIL 6, 2017 8 MIN READ

Related Expertise

- Class Action Defence
- Privacy and Data Management

Authors: Christopher Naudie, Adam Kardash

Update: CASL private right of action has been suspended

CASL's private right of action is coming into force on July 1, 2017. In this article, Adam Kardash, Head of Osler's National Privacy and Data Management Practice, interviews Christopher Naudie, Osler litigation partner and Co-Chair of the firm's National Class Action Specialty Group, about the implications of the provision and how businesses can prepare.

ADAM: We have been talking a lot on the AccessPrivacy monthly calls about Canada's Anti-Spam Law (CASL). Our focus to date on CASL has primarily been on compliance. Namely, how organizations can bring themselves into compliance with the law and what are the risks of regulatory enforcement by the CRTC. While this remains a critical issue, the CASL landscape is going to change, we believe significantly, as of July 1, 2017. To speak to this, we have Christopher (Chris) Naudie here from our litigation department.

Chris, what is happening on July 1 of this year?

CHRIS: As you know, the majority of CASL provisions came into force on July 1, 2014. Since then, the anti-spam and anti-malware portions of the legislation have been enforced by the CRTC. However, the implementation of certain parts of the legislation were delayed until 2017, giving organizations a form of grace period to come into compliance.

As of July 1, 2017, that grace period is over, and non-CASL compliant organizations will be subject to lawsuits brought by affected individuals. You will hear this referred to as CASL's "private right of action." Basically, the legislation will allow affected individuals to sue organizations and their officers, directors and agents for alleged CASL violations.

ADAM: Why do we expect this to be a major change in the landscape? We all know it is expensive to bring a private law suit – prohibitively so for most individuals. It is hard to imagine, for example, that a consumer who received a spam email from a retailer would hire lawyers and spend thousands of dollars pursuing that retailer for what would have to be a minimal recovery?

CHRIS: That is where class actions come in. You are right of course that an individual CASL action would make little economic sense for an individual. Unless that individual was part of the plaintiff-side class action bar representing potential classes of thousands of individuals affected by spam. We expect that the greatest impact of the private right of action will be motivated class action lawyers, working on contingency, who will pursue these claims.

As many of you know, anti-spam and anti-robocall type class actions have been very big business for plaintiff class action lawyers in the U.S., and many organizations operating in the U.S. have been affected, including those involved in high-profile examples such as Uber, Facebook, Twitter and Bed, Bath & Beyond. But the activities that fall under CASL-type legislation in the U.S. are, in most cases, far less broad than here.

Given that fact, and the fact that many of the organizations affected by these U.S. anti-spam class actions run parallel marketing campaigns in Canada, Canadian plaintiff lawyers, who often work closely with the U.S. class actions bar, will, in many cases, have little work to do in copying these U.S.-style anti-spam claims and adjusting them to CASL.

Notably, these lawyers have also known about the July 1 date for two years. They've had time to develop and consider their approach, research appropriate targets and prepare. If I'm being cynical, I am going to guess that several top class actions firms already have draft claims on their desktops, ready to serve at 12:01 a.m. on July 1.

ADAM: So in addition to the risk of CRTC enforcement, individuals will now also be able to sue organizations directly for violations of CASL? What about organizations already targeted by CRTC investigations and sanctions?

CHRIS: Yes. An organization can be subject to these individual actions in addition to a CRTC investigation and sanctioned. However, under CASL, the court is more limited in what compensation it can award an individual in a CASL class action, if the affected organization has already entered into an undertaking with the CRTC or has been served with a notice of violation regarding the same conduct. Given the relatively sporadic CRTC enforcement of CASL to date this may not prove much of a practical impairment.

ADAM: What type of conduct is covered?

CHRIS: In essence, CASL claims can be brought against organizations for the following:

- sending commercial electronic messages, unless the recipient provided express or implied consent and the message complies with the prescribed form and content requirements,
- installing a computer program on a device without consent and
- sending false or misleading electronic messages or e-mail harvesting.

ADAM: Can these CASL actions be brought against non-Canadian organizations?

CHRIS: Yes. Organizations located outside of Canada that send messages to computers located in Canada or that install computer programs on devices in Canada must also comply with CASL requirements. Since electronic messages and computer software often cross borders, it is likely that if a class action is started in the U.S., alleging certain conduct, we can expect to see a similar class action started in Canada.

ADAM: If an organization finds itself on the wrong end of a CASL class action, what is the potential financial exposure?

CHRIS: There are a number of things that will affect financial exposure, depending on how the law suit is framed. However, for example, let's say in a non-compliant email marketing campaign, we could expect to see claims of up to $200 for each non-compliant email sent – up to a maximum of $1,000,000 a day. To use a very simplified example, it would be very typical for an organization's email marketing campaign to include 5,000+ individuals on its mailing lists, and with that we've hit up to a $1,000,000 claim for a one-day campaign. It would also be typical that any real marketing initiative would have more than one touch. That one same campaign – let's say for a holiday season sale at a retailer – may have three

mailings or touches – again, not unrealistic – and we're at a $3,000,000 claim.

In addition, these lawsuits may also include claims for any other kind of "harm" that affected persons have experienced from the CASL breach – for example, lost time in stating complaints or in trying to unsubscribe from the list or their computers crashing because of malware.

Of course, there will also be the legal costs of defending a class action, which can escalate pretty quickly.

ADAM: This sounds pretty doomsday. Are there likely to be good defences to these class action claims?

CHRIS: Yes. CASL provides for a due diligence defence. In order to establish the due diligence defence, an organization needs to show that it took all reasonable steps to avoid the particular event that transpired. Whether an organization can prove this will depend on the context and the facts in each case. The court will review a number of factors, including the organization's use of any preventative systems and procedures. Preventative measures can include training programs, internal and external audits, and risk assessments. Evidence of continuous, genuine and comprehensive efforts on the part of the corporation to implement a CASL policy will significantly support a finding that the corporation exercised the required due diligence.

That being said, in a class action context, it may unfortunately mean years of defending a case before arriving at strong substantive arguments on the defence. If you are concerned that your organization is at risk, there are a number of key preliminary strategies that can be pursued to limit the scope of claims, nip claims in the bud, and push early settlement if your organization's exposure is too great. Organizations should be working well in advance of July 1, 2017, to both review their processes to try to reduce the risk of being subject to a CASL proceeding as well as to assess their realistic exposure and best lines of defence to a class action if it hits.

ADAM: What about conduct that took place before these new parts of the law came into force? Will applicants be able to sue retroactively based on conduct that happened two or three years ago?

CHRIS: The short answer is that no one really knows for certain. We are aware that certain members of the plaintiffs class action bar will likely attempt to file lawsuits, alleging violations of CASL that took place before July 1, 2017.

However, this is something we intend to challenge if it does happen. Looking at the broader context and intention of the government, it is clear that the purpose in delaying the private right of action was so that it could not be applied to alleged contraventions occurring before July 1, 2017. A finding to the contrary would defeat the purpose of delaying the private right of action in the first place.

ADAM: What are some other ways that you think the law can be challenged right out of the gate?

CHRIS: There has been some discussion in academic and legal circles that CASL could be challenged on constitutional grounds on the basis that it unduly restricts freedom of speech. CASL's definition of commercial electronic messaging is vague, broad and all encompassing – it casts a wide net that catches many valid commercial activities. In addition, it is very onerous to comply with. While some restrictions are justified, CASL is overbroad and resembles too closely a complete ban.

The possibility of CASL being struck down should not, however, be a reason not to comply with CASL. It could take years before an action gets far enough to see that result, – and that result is by no means assured.

This article is a slightly revised transcript from Osler's AccessPrivacy Monthly Call held in January 2017. To subscribe to participate in these complimentary monthly Privacy conference calls, please register here.