

# A \$250,000 REMINDER THAT "CASL" IS NOT JUST AN ANTI-SPAM LAW

Posted on July 16, 2018

Categories: [Insights](#), [Publications](#)

On July 11, 2018, the Canadian Radio-television and Telecommunications Commission ("**CRTC**") announced that it has taken enforcement action against Datablocks Inc. ("**Datablocks**") and Sunlight Media Network Inc. ("**Sunlight Media**"), two apparently related companies. This marks the first time that an action has been taken under Canada's "**Anti-Spam Law**"<sup>[1]</sup> ("**Act**") using section 8 of the Act, which prohibits the installation of software without consent, including malware.

## **Datablocks and Sunlight Media**

Datablocks and Sunlight Media were each issued notices of violation by the CRTC alleging that each had committed a violation of section 9 of the Act through their actions or omissions, by aiding in the commission of acts contrary to sections 6-8 of the Act: in their case, section 8, the installation of computer programs on another person's computer system without express consent.<sup>[2]</sup>

The CRTC found that Datablocks and Sunlight Media enabled Sunlight Media's clients to repeatedly violate section 8 by providing the means to commit the prohibited acts, and benefitted financially from the commission of these prohibited acts.

Datablocks, through its software and network infrastructure, provides a real time bidding platform through which website advertisements may be customized for visitors. Sunlight Media, using Datablocks' platform, operates an ad network through which it acts as a broker between advertisers and publishers of online content. The CRTC found evidence that these services had been used by Sunlight Media's clients to display advertisements that surreptitiously installed malicious programs onto the systems of those that received them.

If true, each instance of installation constitutes a violation of the Act – under section 8 for the person who actually installs the program, and under section 9 for the parties that "aid, induce, procure or cause to be procured" a section 8 violation.

In finding a contravention of section 9, the CRTC determined that the companies failed to implement basic safeguards common in the industry, despite evidence that they had been made aware that their services were

being used to commit prohibited acts. Importantly, the CRTC concluded that the companies had no written contracts in place with their clients requiring them to comply with the Act, no monitoring measures in place to govern how clients used their services, and no corporate compliance policies and procedures in place. Unhelpfully, other “safeguards common in the industry” are not suggested by the CRTC.

As a result of these violations, the CRTC assessed monetary penalties of \$100,000 against Datablocks and \$150,000 against Sunlight Media. Datablocks and Sunlight Media have 30 days to file written representations to the CRTC or to pay the penalties.

## **Beyond Spam**

While the Act is colloquially known as “Canada’s Anti-Spam Law” or “CASL” for short, it is important to bear in mind that its full breadth extends far beyond simply regulating “spam”. The stated purpose of the Act is to, “promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities.” To that effect, the Act regulates a number of activities that may hinder electronic commerce, including sending unsolicited commercial electronic messages, altering data transmission and installing computer programs. The Act broadens these prohibitions by prohibiting any person from aiding, inducing, procuring, or causing a CASL contravention.

Section 6, commonly known as the “anti-spam” provision, is the most well-known provision within the Act, prohibiting commercial electronic messages without the consent, whether express or statutorily implied, of the intended recipient. Because a commercial electronic message is essentially any message sent by means of telecommunication for the purpose of encouraging participation in a commercial activity,<sup>[3]</sup> this definition extends beyond the traditional conception of “spam” and regulates genuine business activities, subject to limited exceptions.

Section 7 prohibits the alteration of transmission data in an electronic message that causes the message to be delivered to a destination other than that specified by the sender without the express consent of the sender or the intended recipient. This section notably targets “phishing” and “man-in-the-middle” attacks whereby information is surreptitiously misdirected or misappropriated, but, in the same way that section 6 is agnostic about what “spam” is, section 7 prohibits the action without giving much regard to intent or maliciousness.<sup>[4]</sup>

Section 8, which gave rise to this CRTC action, prohibits the installation of computer programs on another person’s computer system without their express consent, and further prohibits causing a computer system to communicate with another computer system if one has so installed a computer program. While this section notably targets malware, spyware, viruses or other malicious computer programs it extends to all computer programs, with certain exceptions.<sup>[5]</sup>

## Conclusion

The term “CASL” is a misnomer. The scope of the Act extends far beyond simply regulating spam emails, and even the word “spam” is subjective enough that one rarely applies it to one’s own communications. This has been known for some time,<sup>[6]</sup> and in fact when the Standing Committee on Industry, Science and Technology released its 2017 report entitled “Canada’s Anti-Spam Legislation: Clarifications are in Order”,<sup>[7]</sup> its first recommendation was that the Act be given a short title more befitting its scope. (The Standing Committee’s suggestion was “Electronic Commerce Protection Act”. The authors of this article have previously suggested “Prohibited Electronic Interactions Act” or the “Regulation of Electronic Interactions Act”.)

Furthermore, the Act applies not only to those who commit prohibited acts, but to those who enable, facilitate or solicit the commission of prohibited acts, as the CRTC’s findings with respect to Datablocks and Sunlight Media have made clear in the present case. The CRTC plainly found that the acts, or omissions, of those companies crossed the line into prohibited territory. Yet, there are many intermediaries involved in displaying content on websites, and there has been little guidance from the CRTC about what responsibility each party has under the Act. What of the website and content publishers, who may have been able to do something to prevent the malicious advertisements from being displayed? Could, and should, the ISP or website host have filtered such content? What about search results from search engines that point to websites with malicious content?

While this case indicates that the CRTC expects a degree of diligence on the part of service providers and content publishers, including the implementation of basic safeguards to prevent the commission of prohibited activities, businesses that are involved in the dissemination of content that potentially violates the Act must seriously consider what measures they are taking to prevent themselves from being found to aid, induce, procure, or cause a third party, even an unrelated one, to commit a violation.<sup>[8]</sup>

by Ryan J. Black, Janine MacNeil, Lyndsay A. Wasser and Joshua Sved (Temporary Articled Student)

[1] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23[ps2id id='1' target='']

[2] [Investigation into the installation of malicious computer programs through online ads](#)[ps2id id='2' target='']

[3] Andrew Aguilar & Ryan Black, *Internet Law Essentials: Canada’s Anti-Spam Law (CASL)*, 2nd ed (Vancouver: Specialty Technical Publishers, 2017) at 19 [Internet Law Essentials][ps2id id='3' target='']

[4] *ibid* at 45[ps2id id='4' target='']

[5] *ibid* at 50. See our Bulletin [Green Eggs And Spam: The Surprising Side Dish to Canada's Anti-Spam Law that May Catch Software Businesses Off Guard](#) (“Green Eggs”)[ps2id id='5' target='']

[6] See *Green Eggs*[ps2id id='6' target='']

[7] See [Canada's Anti-Spam Legislation: Clarifications are in Order](#)[ps2id id='7' target='']

[8] This case is a clear demonstration the wisdom of the government’s decision to delay the “Private Right of Action”, whereby individuals (or more likely, classes of individuals) would have had a remedy under CASL; until there is clear guidance or amendments to the Act about just how far Section 9 goes, it should not be up to creative plaintiff lawyers to decide what constitutes a violation of Section 9.[ps2id id='8' target='']

### **A Cautionary Note**

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2018