Beyond Spam: Using CASL to Combat Malware and Promote Secure Online Business Practices

Neil Barratt
Director, Electronic Commerce Enforcement
Canadian Radio-television and Telecommunications Commission

SecTor2019
Disclaimer

This presentation has been prepared by Commission staff to provide general information with respect to Canada’s Anti-Spam Legislation (CASL). This material is not to be considered legal advice nor is it binding on the Commission itself.

Further, it does not reflect an interpretation of CASL and/or its accompanying regulations by the Office of the Privacy Commissioner, the Competition Bureau or Innovation, Science and Economic Development Canada.
What is CASL?

- 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 (Canada’s Anti-Spam Legislation)

- Enforced by the CRTC, Competition Bureau and Office of the Privacy Commissioner
Section 6: It is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless ... the person to whom the message is sent has consented to receiving it.
Formal Powers

• Section 15: Preservation Demand
  – Sent to a TSP, “requiring it to preserve transmission data that is in, or comes into, its possession or control.”

• Section 17: Notice to Produce (NTP)
  – Sent to ISPs, TSPs, financial institutions, ESPs and other senders, “requiring them to produce a copy of a document that is in their possession or control, or to prepare a document based on data, information or documents that are in their possession or control and to produce that document”

• Section 19: Warrant
  – Allows designated persons to enter a place such as a private residence, an office or a business, in order to verify compliance with the Act.
Enforcement Actions

- Warning Letter
- Undertaking
- Notice of Violation
- Injunction

- Effect on Compliance
  - Prior Violations
  - Degree of Cooperation
  - Degree of Harm
  - Nature & Scope
Scope of the Problem

Total of ~ 1.62 Million submissions
Email submissions to spam@fightspam.gc.ca – 9 month period, from October 2018 to June 2019
Insights from the Spam Reporting Centre

Emails with a Malicious Link Hosted in Canada

Ratio of Commercial to Phishing: Email and SMS

SMS:
- Other: 72.9
- Commercial/marketing: 1.9
- Phishing: 25.2

Email:
- Other: 40.8
- Commercial/marketing: 41.3
- Phishing: 17.9
CASL and Info/Cyber Security

• It’s not just about e-marketing!

• In the absence of consent, CASL also prohibits:
  – altering the transmission data in an electronic message (section 7);
  and
  – installing a computer program (section 8).

• CASL also imposes requirements on intermediaries to ensure that they are taking adequate steps to protect their infrastructure.
Section 9

• *Compliance and Enforcement Information Bulletin* [CRTC 2018-415](https://www.crtc.gc.ca)

• Intended to help stakeholders understand their risks, and take reasonable steps to comply.

• Stakeholders can reduce risks by:
  – knowing who they’re working with, and
  – putting processes in place to prevent, report and stop abuses on their networks.
Know Your Customer
Malvertising in Canada

Datablocks Inc. and Sunlight Media Network Inc.

• Installation of malicious computer programs through online ads (section 8 violations).

• Companies allegedly aided in the commission of these acts (section 9 violation).

• Notices of Violation, including administrative monetary penalties of $100,000 to Datablocks and $150,000 to Sunlight Media.

Note: These notices of violation are currently under review by the Commission
Canadian Hosting Landscape

• Data gathered by the CRTC identified malware being distributed by way of Canadian web hosting infrastructure.

• Web hosting providers and operators of other networked infrastructure are critical in safeguarding Canadian cyber security.

• Letters sent in November 2018 to engage main Canadian hosting companies.

• The CRTC is continuing to monitor activity.
Partnerships are Critical to Success

- Government partners (RCMP, CCCS)
- International Counterparts
- Industry Associations (M3AAWG, CIRA, ICANN)
- Cyber Security Researchers
How You Can Help

• Talk to us – exchange best practices and engage our support.

• Evangelise your industry – encourage others to foster a compliant environment.

• Take steps to get abuse off your networks.

• Share info with us.
ONE DOES NOT SIMPLY
FINISH A PRESENTATION
WITHOUT TAKING QUESTIONS