Canada’s Anti-Spam Legislation

November 26th, 2013
• Compliance and Enforcement at the CRTC
• About Canada’s Anti-Spam Legislation (CASL)
• Enforcement of CASL
• Undertakings and Private Rights of Action
• CASL Regulations
• CASL Information Bulletins
• Next Steps
Compliance and Enforcement
C&E Role within the CRTC

A responsive regulatory organization that protects the interests of Canadians and enhances the value of our system of commercial communications.

Foster a culture of compliance and make a positive impact on Canada’s commercial communications system.

Prevent harm to consumers and to the Canadian economy as a result of a misuse of Canada’s communications systems.

Detect harm resulting from misuse of Canada’s communications systems quickly and accurately.

Respond to violations using the full range of authorities to mitigate risks to consumers and the Canadian economy.

Build Capacity to prevent, detect and respond to risks related to misuse of Canada’s communications system and to be a workplace of choice and centre for management excellence.

Canadians have access to a world-class communication system

Create Canadians have access to compelling creative content, from diverse sources, on a variety of platforms.

Connect Canadians have access to quality and innovative communication services at affordable prices.

Protect Canadians are protected from unsolicited commercial communications.

CRTC Strategic Framework

Management Excellence
Canada’s Anti-Spam Legislation
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 (CASL unofficial acronym)
Historical Background

- May 17, 2005: Task Force on Spam released a list of recommendations
- December 15th, 2010: Bill C-28 Received Royal Assent
- Summer 2011: Governor in Council and CRTC draft regulations posted for consultation
- March 28, 2012: Electronic Protection Regulations (CRTC) (Telecom CRTC 2012-183) were published, following a public process
- Part II of the GIC regulations once they are approved by both the Minister and the TBS.
## International Comparison

<table>
<thead>
<tr>
<th>Country</th>
<th>Anti-Spam Legislation</th>
<th>Enforcement Agency</th>
<th>Opt In / Opt Out</th>
<th>Private Right of Action</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>C-28 Canada’s Anti-Spam Legislation (CASL) (2010)</td>
<td>CRTC, CB, OPC</td>
<td>Opt In</td>
<td>Yes</td>
<td>$1M/violation for an individual; $10M/violation for any other person</td>
</tr>
<tr>
<td>United States</td>
<td>Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)</td>
<td>Federal Trade Commission (FTC)</td>
<td>Opt Out</td>
<td>Yes – but only by ISPs or state attorney generals</td>
<td>FTC Administrative Actions: $11,000 per violation</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Privacy and Electronic Communications (EC Directive) Regulations 2003</td>
<td>Information Commissioner’s Office (ICO)</td>
<td>Opt In</td>
<td>No</td>
<td>Magistrate’s court: £5,000 in England and Wales, £10,000 in Scotland; unlimited if trial before a jury</td>
</tr>
<tr>
<td>Australia</td>
<td>Spam Act 2003</td>
<td>Australian Communications and Media Authority (ACMA)</td>
<td>Opt In</td>
<td>No</td>
<td>$2200/violation up to $44,000/day for multiple violations; $11,000/violation up to $220,000/day for multiple violations for corporations</td>
</tr>
</tbody>
</table>
## Overview of CASL - Legislative roles

<table>
<thead>
<tr>
<th>Administration</th>
<th>Violation</th>
<th>Addressing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CRTC</strong></td>
<td>The legislation includes violations respecting:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sending of commercial electronic messages (CEMs) without consent</td>
<td>• Spam (s.6)</td>
</tr>
<tr>
<td></td>
<td>• alter transmission data in the course of a commercial activity without consent</td>
<td>• Botnets (s.8)</td>
</tr>
<tr>
<td></td>
<td>• Installing a computer program in the course of a commercial activity without consent</td>
<td>• Malware (s.8)</td>
</tr>
<tr>
<td></td>
<td>Amends the <em>Competition Act</em> to include violations respecting:</td>
<td>• Network re-routing (s.7)</td>
</tr>
<tr>
<td></td>
<td>• Misleading and deceptive practices/representations, including false headers, subject lines, etc…</td>
<td></td>
</tr>
<tr>
<td><strong>Competition Bureau (CB)</strong></td>
<td>Amends <em>Personal Information Protection and Electronic Documents Act (PIPEDA)</em> to include contraventions involving:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The collection and use of personal address information without consent</td>
<td>• Address harvesting (steal email contacts)</td>
</tr>
<tr>
<td></td>
<td>• The collection of personal information by illegally accessing, using, or interfering with computer systems</td>
<td>• Dictionary attacks (Systematically guessing email addresses to spam)</td>
</tr>
<tr>
<td></td>
<td>Amends <em>Personal Information Protection and Electronic Documents Act (PIPEDA)</em> to include contraventions involving:</td>
<td>• Spyware (Personal Info)</td>
</tr>
</tbody>
</table>
The legislation addresses the recommendations of the Task Force on Spam with a comprehensive regulatory regime that uses economic disincentives instead of criminal sanctions to protect electronic commerce and is modelled on international best practices. The regime includes:

- New Violations
- A Private Right of Action (PRA)
- Administrative Monetary Penalties (AMPs)
- Domestic and International Cooperation
- Extended Liability (follow the money)

Support mechanisms such as:

- A National Coordinating Body
- A Spam Reporting Centre
Main Elements (cont’d)

The legislation provides for:

• Public Right of Action (PRA) for any violation
  – The PRA would allow affected persons such as businesses, network providers and consumers to take civil proceedings against those alleged to have committed contraventions of the Act. In addition to actual damages, courts may award significant sums to successful applicants.

• Domestic and International Cooperation
  – Coordination and consultation between the three enforcement agencies responsible for compliance
  – Information sharing and consultation between the three agencies and their international equivalents

• A variety of investigative and enforcement tools
  – Preservation Demand; Notice to Produce; Search Powers; Restraining Order; Direct and Vicarious Liability; Undertakings; Notice of Violation
CRTC Enforcement Process

Gather Information

Organize/Analyze

Compliance and Enforcement

Sources
- Complaints
- Honeypot Data
- Industry Filings
- International Agencies

Sorting/Categorization

SPAM Reporting Centre (SRC)

CB

CRTC

Triage

Tool Choice

Results
- Joint Action
- Investigation
- Warnings
- Notices of Violation/Administrative Monetary Penalties
- Injunction
- Undertaking
- Negotiated Settlement
- Alerts
- Education
The legislation provides for a variety of investigative and enforcement tools:

- Preservation Demand (s.15)
- Notice to Produce (s.17)
- Warrant (search & seizure) (s.19)
- Restraining Order (cease & desist) (s.26)
- Injunction (s.41)
- Undertaking (s.21)
- Notice of Violation (s.22)
- Administrative Monetary Penalty (AMP) (s.20)
Consequences of a violation

• **Administrative Monetary Penalties (AMPs)**
  - maximum penalty for individual = $1,000,000 / violation
  - maximum penalty for an organization = $10,000,000 / violation

• **Extended Liability**, including:
  - vicarious liability
  - director/officer liability
Conformity Continuum

Prevent

Objective:
- Increase consumers’ ability to recognize, avoid and report conduct that violates the rules and regulations
- Increase industry ability and willingness to voluntarily comply with the rules and regulations

Means:
- Public education, awareness and outreach
- Promotion of internal compliance measures
- International co-operation
- Consultations with various stakeholders

Detect

Objective:
- Assess compliance through surveillance and intelligence gathering activities to ascertain the need to engage in enforcement action

Means:
- Review and analysis of complaints and trends
- Assessment of risks
- Information sharing
- Investigation techniques

Respond

Objective:
- Ensure appropriate, timely and effective responses to violations

Means:
- Preliminary measures
- Voluntary measures
- Involuntary measures

*The appropriate tool to use in a particular situation will depend on the factual context.
Partnership Approach

Non-Profit Organizations

Mail Service Providers

Government Organizations & Alliances

Telecom Service Providers

Reputation and Security Vendors

Email Service Providers & Marketers
What is Success?

Direct
- Increased compliance with legislation
- Change Canada’s reputation as spam haven
- Reduction in infected electronic devices

Indirect
- Adoption of Best Common Practices (BCP’s)
  - Enable / encourage many new Best Practices in the industry
- Cost savings for Business and Consumers
- Reduction in Consumer losses
- Increased Consumer protection, empowerment, and confidence in the e-marketplace
Undertakings and Private Rights of Action
Elements of an Undertaking

• An alleged violator may enter into an undertaking as per Section 21 of CASL

• Entry into an undertaking is subject to approval from a designated person

• The undertaking:
  – Must identify every violation committed under Sections 6 to 9
  – May require payment of a given amount and/or other conditions

• Undertakings
  1. When a Notice of Violation has not yet been issued
  2. When a Notice of Violation has been issued, it will be ended
As per Section 47(1) of *CASL*, a person who alleges that he or she is affected by an act or omission that breaches the key provisions of:

- Sections 6 to 9 of *CASL*
- Section 5 of *PIPEDA* (collection/use of personal information)—subsection 7.1(2) or (3) of that Act
- Section 52 or 53 (false/misleading representations) or 74.011 (deceptive marketing) of the *Competition Act*

may apply to a court for an order of compensation

- Limitation period of 3 years
- A court may not impose statutory damages against a person who has already entered into an undertaking with reference to the same violations
CASL Regulations
CASL Regulations

• CASL Contemplates two categories of regulations:
  – Governor in Council regulations (managed by Industry Canada)
  – CRTC regulations (for which the Commission is responsible)

• Both sets of regulations were published in the Canada Gazette for a 60 day comment period

• Consistent with normal practice, comments on the CRTC regulations were sought by way of a public CRTC Notice of Consultation with the concurrent 60 day consultation period launched via the Gazette

• All regulations will come into force at the same time as the legislation, subject to Governor in Council approval
The final CRTC regulations were made on March 28, 2012.

The Regulations relate solely to the CRTC’s mandate under C-28, namely, Section 6 to 8.

They include:

- Reg 2: Information to be included in CEMs
- Reg 3: Form of CEM
- Reg 4: Information to be included in a request for consent
- Reg 5: Specified functions of computer program
Information Bulletins
The CRTC has published the following two information bulletins to help Canadian businesses better understand CASL and facilitate compliance:

1. Certain provisions of the Electronic Commerce Protection Regulations (CRTC)
   (Compliance and Enforcement Information Bulletin CRTC 2012-548)

2. The requirement to obtain express consent under CASL when using Toggling
   (Compliance and Enforcement Information Bulletin CRTC 2012-549)
Information to be included in a CEM (Reg 2)

- Sender(s) must be identified
  - Including Affiliates
- CEMs must include the sender’s mailing address
  - Definition
  - Valid for 60 days
Form of CEM (Unsubscribe Mechanism) – (Reg 3)
Information to be included in a request for consent – (“sought separately”) – (Reg 4)
Specify functions of computer programs (Reg 5)
Use of Toggling Information Bulletin

• What is Toggling?

You are about to purchase Product A for $10.00.

I agree to receive Company Inc.'s newsletter containing news, updates and promotions regarding Company Inc.'s products. You can withdraw your consent at any time.

Please refer to our Privacy Policy or Contact Us for more details.

You are about to purchase Product A for $10.00

I agree to receive Company Inc.'s newsletter containing news, updates and promotions regarding Company Inc.'s products. You can withdraw your consent at any time.

Please refer to our Privacy Policy or Contact Us for more details.

ALL PRODUCTS 40% off for a limited time only!

Enter your email below to receive Company Inc.'s newsletter containing news, updates and promotions regarding Company Inc.'s products. You can withdraw your consent at any time.

Please refer to our Privacy Policy or Contact Us for more details.
Next Steps
Next Steps

• Awaiting the Governor in Council (GIC) Regs
• Coming into force of the Act and regulations on a day fixed by the GIC
• Spam Reporting Center and Labs required for implementing CASL will be ready at time CASL is in force
Questions?