SESSION PANEL

• David B. Elder, Counsel

• Wally Hill, Vice President, Government & Consumer Affairs

• Scott Smith, Director, Intellectual Property & Innovation Policy
SESSION OVERVIEW

1. CASL After Three Years

2. CASL Enforcement Experience After Three Years

3. Business View After Three Years

4. Questions and Discussion of CASL “Issues” after Three Years
LEGAL NOTICE

The information contained in this presentation is provided for general informational purposes only and should not be construed as legal advice from Stikeman Elliott, the Canadian Marketing Association, or the Canadian Chamber of Commerce.
CASL TURNS THREE!

1. CASL Timeline
2. Vital Stats
4. July 1, 2017 (Private Right of Action)
5. July 1, 2017 (Parliamentary Review)
6. Ongoing CASL Concerns
CASL TIMELINE

- **CASL Passed**: Dec. 2010
- **Industry Canada Regs Finalized**: Dec. 2013
- **CRTC Regs Finalized**: July 1, 2014
- **Computer program provisions in force**: Jan. 15, 2015
- **Parliamentary Review Prescribed after 3 years**: July 1, 2017
- **Mar. 2012 CRTC Regs Finalized**
- **July 1, 2014 CEM provisions in force**
- **July 1, 2017 PRA in force, EBR transition ends**
- **Jan. 15, 2018 Transitional computer provisions expire**
VITAL STATS

Consequences
• Govt Spam Reporting Centre established: fightspam.gc.ca
• 5-6k complaints/week - over 900,000 complaints to date
• Number of enforcement cases to date: 7
• Total amount of fines: over $2,200,000
• Average amount of fine: $316,000
• Brand impacts

Results
• 63% increased open rates post-CASL
• 50% increased click-over-open rates post-CASL
• 5.5% increase click-through rates post-CASL
• Average unsubscribe rates 20% lower before CASL for volume clients.

(Source: Inbox Marketer Benchmark Study)
JULY 1, 2017 (TRANSITIONAL PROVISIONS)

• Implied consent for existing customers were given a duration of three years if:
  
The sender had a relationship with the recipient prior to July 1, 2014 and, as part of that relationship, the sender and recipient had communicated through CEMs.

• On July 1, 2017, these transitional implied consents will expire. Businesses need to prepare for change and transition the data files.
MANAGING CONSENT TYPES

- Know what consents you have and who you can mail to
- Know what the expiration of these consents are

<table>
<thead>
<tr>
<th>Email</th>
<th>Source</th>
<th>Opt-in Date</th>
<th>Consent Type</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:user@name.com">user@name.com</a></td>
<td></td>
<td>01/03/2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:sample@test.com">sample@test.com</a></td>
<td><a href="http://www.corporate.com/Jun2013-sale">http://www.corporate.com/Jun2013-sale</a></td>
<td>04/06/2013</td>
<td>Implied</td>
<td>30/06/2017</td>
</tr>
<tr>
<td><a href="mailto:help@me.com">help@me.com</a></td>
<td><a href="http://www.corporate.com/contactus">http://www.corporate.com/contactus</a></td>
<td>14/04/2015</td>
<td>Implied 6 months</td>
<td>13/10/2015</td>
</tr>
<tr>
<td><a href="mailto:foo@bar.com">foo@bar.com</a></td>
<td><a href="http://www.corporate.com/subscribe">http://www.corporate.com/subscribe</a></td>
<td>30/11/2015</td>
<td>Implied</td>
<td>29/11/2017</td>
</tr>
<tr>
<td><a href="mailto:test@example.com">test@example.com</a></td>
<td>POS - Store #1234</td>
<td>17/07/2016</td>
<td>Express</td>
<td>no expiry</td>
</tr>
<tr>
<td><a href="mailto:new@example.com">new@example.com</a></td>
<td><a href="http://www.corporate.com/subscribe">http://www.corporate.com/subscribe</a></td>
<td>01/01/2017</td>
<td>Express</td>
<td>no expiry</td>
</tr>
</tbody>
</table>
REQUEST CONSENT UPDATE

To:
Subject: Join our Email Consent List
We are reaching out to let you know that in accordance with Canada's Anti-Spam Legislation (CASL), which came into effect July 1, 2014, we require your consent to continue sending you email communication.

Click Here to Join the Canadian Institute Email List

As our thank you, we will send a voucher that is valid for up to $250 that can be used towards any conference in 2017.

To view a complete listing of our events, you can also visit our website at http://www.canadianinstitute.com
CONSENT UPDATE STRATEGIES

– Pre-header copy between mid-April to mid-May
  • The action of the click will = express consent. Landing page can acknowledge confirmed consent e.g. “Thank you for confirming your consent. We are happy to have you as part of our email community!”
    • We would like to confirm your interest in receiving our emails after June 30, 2017. Yes, you have my consent
    • We would like to confirm your interest in receiving our emails after June 30, 2017. Yes, I am interested.

– Recommendation for pre-header copy starting mid-May
  • More urgent call to action, prompting a yes or no action
    • You must confirm your consent to continue receiving emails from us after June 30, 2017.
    • Yes, I want to continue receiving our emails.
    • No, I want to unsubscribe.

(Courtesy of Inbox Marketer)
PRIVATE RIGHT OF ACTION TAKES EFFECT

- Effective July 1, 2017, PRA will provide fertile ground for class action lawsuits given the statutory damages.
- CASL provides that a recipient of an offending CEM can seek compensatory damages and **statutory damages up to $200** for each contravention; up to $1M for individuals and $10M for businesses.
PARLIAMENTARY REVIEW AFTER 3 YEARS

- July 1, 2017 marks earliest date the Government of Canada can commission the House of Commons Standing Committee on Industry, Science and Technology (INDU) to begin a review of CASL.
ISSUES FOR PARLIAMENTARY COMMITTEE

• Overall Effectiveness of CASL
• Impact for eCommerce, businesses
• Scope of the law - What is a CEM? Spam?
• Private Right of Action (PRA)
• Section 6.6 clarification
• Unsubscribe challenges
• EBR - with no purchase; personnel changes
• Reasonable records of consent?
• Third Party Referrals - single messages
• Social Media coverage
INVESTIGATION & ENFORCEMENT

- CRTC has been active with respect to enforcement/investigations re CEMs and malware
- Tools:
  - Preservation demands
  - Notice to produce
  - Warrants
- “visits” and requests for info
- “Honeypots”
- For computer programs, initial focus on malware/botnets?
# CASL ENFORCEMENT SUMMARY

<table>
<thead>
<tr>
<th>Organization</th>
<th>Alleged Non-Compliance</th>
<th>Process</th>
<th>AMP</th>
</tr>
</thead>
</table>
| CASL ENFORCEMENT | - Sent CEMs without consent  
|                  |   - Unsubscribe not functioning properly  
|                  |   - Ignored unsubscribe requests  
|                  |   - Unknown number of messages                                                      | Notice of Violation | $1,100,000.00    |
| PlentyOfFish     | - Deficient unsubscribe mechanism:  
|                  |   - Not clearly and prominently set out  
|                  |   - Could not be readily performed  
|                  |   - Unknown number of messages                                                      | Undertaking         | $48,000.00       |
| porter           | - Inadequate proof of consent  
|                  |   - Incomplete contact information in messages  
|                  |   - No unsubscribe link in messages  
|                  |   - Unsubscribe not set out clearly and prominently  
|                  |   - More than 10 days to unsubscribe  
|                  |   - Unknown number of messages                                                      | Undertaking         | $150,000.00      |
| ROGERS           | - Non-functioning unsubscribe could not be readily performed  
|                  |   - Address used to unsubscribe not valid for 60 days  
|                  |   - Some unsubscribe requests not honoured  
|                  |   - Unknown number of messages                                                      | Undertaking         | $200,000.00      |
| Kellogg's        | - Sent CEMs without consent  
|                  |   - Unknown number of messages                                                      | Undertaking         | $60,000.00       |
| Blackstone Learning | - Sent CEMs without consent  
|                  |   - No proof of consent provided  
|                  |   - 9 campaigns totaling 383,668 messages                                          | Notice of Violation| $640,000.00      |
|                  |                                                                                      | C&E Decision 2016-428 | $50,000.00      |
| William Rapanos  | - Sent CEMs without consent  
|                  |   - Didn’t include or provide contact details  
|                  |   - No functioning unsubscribe mechanism                                           | Notice of Violation| $15,000.00       |
|                  |                                                                                      | L&E Decision 2017-40 |                 |
GOING AFTER THE SOURCE
ANATOMY OF A TYPICAL INVESTIGATION

- Request for information
- Response
- Follow-ups and Response (repeat as necessary)
- Invitation to discuss findings/settlement
- Agreement
- Review and finalization of undertaking agreement
- Execution
- Payment of AMPS
- Media release
OTHER INVESTIGATION/ENFORCEMENT MODELS

- Preservation/Production Order
- Surprise visit
- Entry Warrant (with Police) - seizure
- Direct Issuance of NOV
- Right to make representations to CRTC
- Commission decides on b.o.p. whether violation committed
- May impose NOV penalty, may reduce or waive penalty, or may suspend payment of penalty subject to any conditions necessary to ensure compliance
TYPICAL UNDERTAKING

1. Applies to broader corporate family
2. Agreement to comply in future
3. Agreement to cease offending practice(s)
4. Payment of AMP
5. Creation/update of corporate compliance program
6. Confirm when done
7. Review on annual basis - provide written report on request
Enforcement Advisory - Notice for businesses and individuals on how to keep records of consent

Commission staff has published this advisory, directed to businesses and individuals in Canada sending commercial electronic messages (CEMs) as part of their commercial activities.

Commission staff notes that under section 13 of Canada’s anti-spam legislation (CASL), the onus is on the person who alleges they have consent to send a CEM (typically, the person who sends the CEM) to prove that they have proper consent, either implied or express, to send each message. Commission staff has observed that some businesses and individuals are unable to prove they have obtained consent before sending CEMs. The purpose of this Enforcement Advisory is to remind those involved, including those who send CEMs, of the requirements under CASL pertaining to record keeping.

How can the sender keep track of consent?

The onus of proving consent always remains with the person(s) sending, causing or permitting the sending of CEMs. This is the case even if the sender is relying on an existing business or non-business relationship that was created prior and post July 1, 2014 (the implementation date of CASL).

As such, good record-keeping practices can help the sender:
- Identify potential non-compliance issues
- Investigate and respond to consumer complaints
- Identify the need for corrective actions
- Demonstrate that these corrective actions were implemented
- Establish a due diligence defense in the case of a violation of CASL

Senders of commercial electronic messages should consider keeping a hard copy or an electronic record of, among others:
- All evidence of express and implied consent (e.g., audio recordings, copies of signed consent forms, completed electronic forms) from consumers who agree to receive CEMs.
RECORD-KEEPING TIPS

• All evidence of express and implied consent (audio, forms, electronic forms)
• Date, time, originating telephone number/IP address, etc.
• Best evidence rule: CRTC prefers direct evidence; organization-created record likely insufficient
• All unsubscribe requests and resulting actions
• Documented methods through which consent collected (particularly important where oral consent)
• CASL compliance policies and procedures
LESSONS LEARNED

1. May help to revise practices quickly (or may not)
2. Only partial disclosure of case against you
3. Complainants assumed to be truthful - onus on company to disprove
4. Some have settled where not clear violation committed
5. Predilection for AMPs
6. Unclear what weight, if any given to due diligence
7. Unclear how AMPs calculated - may be being recalibrated
8. Warrants are intense, disruptive - watch privilege issues closely
9. Warrants most likely re malware investigations
10. Beware continuing application of privacy laws
BUSINESS VIEW AFTER THREE YEARS
Global spam volume as percentage of total e-mail traffic from 2007 to 2015
# Most Spam Messages Originate in the US

Top ten countries from which spam originated in 2015

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>15.2%</td>
</tr>
<tr>
<td>Russia</td>
<td>6.2%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>6.1%</td>
</tr>
<tr>
<td>China</td>
<td>6.1%</td>
</tr>
<tr>
<td>Germany</td>
<td>4.2%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>4.0%</td>
</tr>
<tr>
<td>France</td>
<td>3.2%</td>
</tr>
<tr>
<td>India</td>
<td>3.0%</td>
</tr>
<tr>
<td>Argentina</td>
<td>2.9%</td>
</tr>
<tr>
<td>Brazil</td>
<td>2.9%</td>
</tr>
</tbody>
</table>

Source: Kaspersky Lab
We’re nervous and worried about the gravity and potential cost of violations...

There’s still some vagueness in the bill that leaves a fair margin for interpretation...

This is encroaching on our basic freedoms...Reaching out to communicate with someone seems like a basic right, and a basic human function...

Seems like I can't find someone's email and send them a message about a potential product, service or opportunity. That pretty much shuts down commerce in Canada!
In a study of 500 businesses

- 10% stopped email marketing all together
- 30% curtailed marketing lists
- 48% believe they are no longer competitive with US counterparts.
Amount of spam received after Canada’s Anti Spam Legislation (CASL) introduction according to consumers in Canada as of August 2015

- Received the same amount of spam: 29.5%
- Did not receive less spam: 29.4%
- Received more spam: 5.4%
Perception of retailer promotional emails and ads among email users in the United States in 2014, by gender

- Find it useful when retailer sends me emails featuring recommended products based on what I’ve previously purchased: 78% Female, 83% Male
- Find it useful when a retailer sends me emails featuring recommended products based on what I’ve looked at online, but not purchased: 72% Female, 71% Male
- Find it useful when I see online ads featuring images of products I previously viewed on a retailer’s website: 67% Female, 72% Male
- Like it when retailers personalize my emails by using my name in the subject line or the body of email: 66% Female, 71% Male
- Find it useful when a retailer recommends products on the pages of its website while I’m shopping: 63% Female, 73% Male
Subscribers' typical actions when they are no longer interested in a company's permission e-mails as of 2011

- Click the link to "unsubscribe" - 67%
- Delete e-mails when they arrive - 17%
- Click on the "spam" or "junk" button - 8%
- Nothing, just ignore the e-mails - 6%
- Set up a filter in my e-mail program - 2%
THIRD PARTY MESSAGES

• Consent for 3rd party messages - who owns the consent?
• Reconciling CASL and PIPEDA - are business email addresses personal? What happens when you share with a third party?
“CONSPICUOUS PUBLICATION”

- “implied consent “ (s. 10(9)(b)) must have records to prove that the publication was “not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages”.

“best practice” in this regard would be to capture a record (such as a screenshot) of the publication in each case?
UNSUBSCRIBE

- No clear answer on what constitutes a “step” in the process
- 10 day window, 60 day active link, general failures of system.
- Demonstrable auditing and monitoring of functionality required
OUTSOURCED MESSAGING FUNCTIONS

• The CRTC will not accept the view that outsourced messaging functions are not the responsibility of an organization.
• Organizations are likely accountable for the failures of service providers, unless they can demonstrate due diligence.
• Organizations must clearly address CASL compliance in their service contracts and monitor and audit the compliance of their service providers.
**DUE DILIGENCE**

- **What is considered due diligence?**
  - adequate written policies
  - adequate on-going training
  - contemporaneous record-keeping
  - active monitoring and enforcement
  - responsiveness to complaints, problems and to inquiries from the CRTC

- **Due diligence is not a one-time activity;**
  - on-going, day-to-day activity
  - organizations will have to practice and document to rely on it as a defense.

- **Approach is not consistent with the statutory language of s. 33:**
  - “Every rule and principle of the common law that makes any circumstance a justification or excuse in relation to a charge for an offence applies in respect of a violation to the extent that it is not inconsistent with this Act.”
GOAL TO "HELP ACHIEVE COMPLIANCE"

- Encouraged to voluntarily disclose mishaps
- Carefully assess the risks of taking up this invitation
- Must also consider preservation of privilege and third party liability due to CRTC’s ability to share information

“Hi, I’m Hugo — I’ll be your compliance officer.”
MISLEADING MESSAGES

• Competition Bureau provisions biggest concern under PRA
SMART SPAM

- 25% of compromised computers were smart devices, including home routers, webcams, home entertainment centers, burglar alarms, and yes—refrigerators.
QUESTIONS AND DISCUSSION