



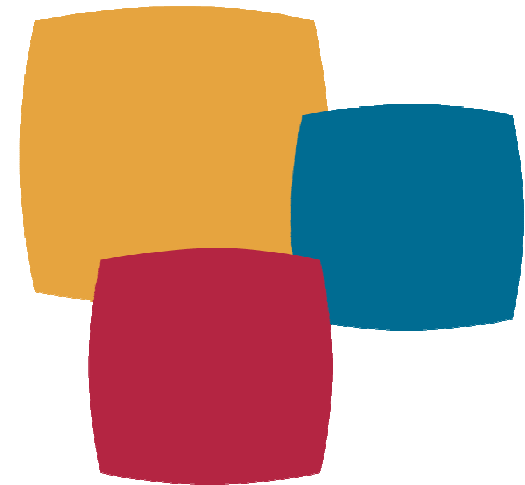
Industry  
Canada

Industrie  
Canada



# Canada's Anti-Spam Legislation

March 2011



**Andre Leduc**  
Senior Security Policy Advisor  
Industry Canada  
[Andre.Leduc@ic.gc.ca](mailto:Andre.Leduc@ic.gc.ca)  
[www.ecom.ic.gc.ca](http://www.ecom.ic.gc.ca)

Canada 



# Table of Contents

- Legislative Process
- Main Elements of the legislation
- Compliance Regime
- Consent
- Private Right of Action
- International Cooperation
- Spam Reporting Centre
- Anti-spam Coordinating Body





# Legislative Progress

- The *Electronic Commerce Protection Act (ECPA)* was tabled in Parliament on April 24, 2009 and was designed to reduce the most damaging and deceptive forms of spam and other conduct that discourage electronic commerce
- ECPA was passed by the House of Commons and was before the Senate Transport & Communications Committee when Parliament was prorogued in December 2009
- Bill C-28 was tabled on May 25<sup>th</sup> of 2010 (virtually the same bill as before with a few technical amendments)
- C-28 received Royal Assent on December 15<sup>th</sup>, 2010
- Coming into force of the legislation is expected to occur in fall of 2011





# Main Elements of the Legislation

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)
- International Cooperation
- Extended Liability (follow the money)

Support mechanisms such as:

- A National Coordinating Body
- A Spam Reporting Centre





# New Violations

The legislation prohibits:

- The sending of unsolicited commercial electronic messages (s.6)
- The unauthorized altering of transmission data (s.7)
- The installation of computer programs without consent (s.8)
- False and misleading representations online (including websites and addresses) (s.75)
- The use of computer systems to collect electronic addresses without consent (s.82(2))
- The unauthorized access to a computer system to collect personal information without consent (s.82(3))





# The Consent Regime

The legislation is based on an “opt-in” consent regime, which stipulates that no electronic message can be sent without:

- **Express Consent**
  - can be determined when the organization presents an opportunity for the individual to express positive agreement to a stated purpose. Unless the individual takes action to "opt in" to the purpose — in other words, says "yes" to it — the organization does not assume consent.
- **Implied Consent**
  - arises where consent may reasonably be inferred from the action or inaction of the individual and is also further determined in section 11 regarding “existing business relationships” and “existing non-business relationships”. Implied consent also covers situations of conspicuous publication or disclosure.





# Legislative Remedies

Administration	Violation	Addressing
<b>CRTC</b>	The legislation includes violations respecting: <ul style="list-style-type: none"><li>• The sending of unsolicited commercial electronic messages</li><li>• The use of telecommunications to alter transmission data and download programs to computer systems and networks without authorization</li></ul>	<ul style="list-style-type: none"><li>• Spam</li><li>• Malware &amp; Botnets</li><li>• Network re-routing</li></ul>
<b>Competition Bureau</b>	Amends the <i>Competition Act</i> to include violations respecting: <ul style="list-style-type: none"><li>• Misleading and deceptive practices/ representations, including false headers, subject lines, etc...</li></ul>	<ul style="list-style-type: none"><li>• False or misleading representations online (incl. websites and addresses)</li></ul>
<b>OPC</b>	Amends <i>PIPEDA</i> to include contraventions involving: <ul style="list-style-type: none"><li>• The collection and use of personal address information without consent by electronic or any other means</li><li>• The collection of personal information by illegally accessing, using, or interfering with computer systems</li></ul>	<ul style="list-style-type: none"><li>• Address harvesting</li><li>• Dictionary attacks</li><li>• Spyware (Personal Information)</li></ul>





# Strong Penalties & Due Process

- The CRTC will use AMPs to ensure compliance
- Amendments to the *Competition Act* allow the imposition of AMPs and other penalties
- S. 21(4) notes that the maximum penalty per violation is \$1 M in the case of individuals and \$10 M in the case of any other person
- Prior to administering penalties, the CRTC must consider factors as described in (s. 21(3)), most of those factors are also to be considered in assessing the statutory damages under the Private Right of Action
- The Act is a regulatory regime designed to encourage compliance but also carries stiff penalties for violations





# The Private Right of Action (PRA)

- The legislation provides for a PRA for any violation
- The PRA would allow businesses, network providers and consumers to take civil action against anyone who violates the legislation
- Experience from other countries, such as the U.S., demonstrate that PRAs can be an effective tool in deterring detrimental conduct to online commerce and complements regulatory enforcement measures in the public domain
- This PRA would allow any person or enterprise to take action against spammers. This is expanded compared to the U.S. which only allowed Internet Service Providers (ISPs) to pursue spammers





# International Cooperation

The legislation provides for:

- Coordination and consultation between the three enforcement agencies responsible for compliance
- Information sharing and consultation between the three agencies and their international equivalents
- A broadly defined Canadian link which stipulates that the legislation would apply to electronic messages sent to, through or from Canada
- Disclosure of information from organizations to the enforcement agencies with regards to any of the violations





# Spam Reporting Centre

- In support of the legislation, the government would establish and operate a Spam Reporting Centre to:
  - Allow harmful Internet messages to be sent to a central facility by individuals and businesses
  - Analyze and refer major threats to relevant authorities for action
  - Store and analyze spam and related computer threats for evidentiary and enforcement purposes
  - Support cooperative work with partner agencies such as the Competition Bureau, the CRTC and the OPC and assist the three enforcement agencies with investigations and prosecutions
- The Spam Reporting Centre will ensure full and effective access to the database for all enforcement agencies.





# Anti-Spam Coordinating Body

- In its May 2005 report, the Task Force on Spam recommended the creation of a focal point or coordination centre, within government, to coordinate Canada's anti-spam work (recommendations #21 and #22).
- A coordinating body at Industry Canada will support the legislative regime by providing:
  - Effective policy oversight
  - Monitoring and reporting on the efficacy of the legislation
  - Supporting international cooperation (*London Action Plan, Organization for Economic Cooperation and Development, Messaging Anti-Abuse Working Group*)
  - Working with the private sector on joint anti-spam efforts
  - Overseeing operation of the Spam Reporting Centre
  - Analysis and reporting on emerging threats and trends (metrics)





# A Comprehensive Response

- The new law will be:
  - Fair and effective at addressing detrimental conduct,
  - Comprehensive and broad in its approach,
  - Swift in its application,
  - Complete and thorough by capitalizing on existing expertise and using a multifaceted enforcement approach
  - Conducive to international cooperation
- Furthermore,
  - Increased user awareness and education would allow the Internet community, especially consumers and SMEs, to take further steps to protect themselves
  - An effective Spam Reporting Centre would provide business and consumers a focal point for reporting spam and related threats

