Industry Canada Industrie Canada

Bill C-27, the *Electronic Commerce Protection Act* (ECPA)

Presentation to the London Action Plan

October 2009

Canada

Table of Contents

Prime Minister's Announcement

- **Prime Minister Harper announced on September 25, 2008 intentions to table anti-spam legislation as part of the larger Protecting Consumers platform**

- **The Prime Minister said that with a new mandate, the Conservative Government will introduce a consumer protection plan including:**
  - Increased civil penalties for false and misleading advertising, and upon criminal conviction, tougher fines and prison terms.
  - Legislation to reduce Internet spam and to prohibit practices such as identity theft, the spreading of viruses, "phishing" and other forms of fraud.
  - Increased fines for dangerous, deceptive and destructive email, and for attempts to steal personal information.
  - Establishing a coordinating body to ensure the legislation is effectively enforced and to respond to consumers complaints.

Legislative Progress - Bills C-27 & S-220

- On May 7, 2008, and again on November 20, 2008 Liberal Senator Yoine Goldstein introduced his Private Member's Bill. In both cases, it was at second reading when Parliament was dissolved

- On February 3, 2009, Senator Goldstein re-introduced his legislation as Bill S-220, *An act respecting commercial electronic messages.*
  (It is currently with the Senate Transport & Communications Committee)

- Bill C-27, The *Electronic Commerce Protection Act* (ECPA) was tabled in Parliament on April 24, 2009 and is designed to reduce the most damaging and deceptive forms of spam and other conduct that discourage electronic commerce
  (It is currently with the House of Commons INDU Committee)

Main Elements of ECPA

ECPA 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:

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

support mechanisms such as:

- A National Coordinating Body
- A Spam Reporting Centre

Addresses a Wide Range of Concerns

ECPA prohibits:

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

ECPA - International Best Practices

- In developing a plan to address spam and related threats in Canada, the government studied international experiences in Australia, the U.S., the U.K. and Europe to understand which provisions were most successful in order to develop the most complete regime possible

- Every one of Canada's major trading partners addresses spam and related threats through an administrative regulatory regime. ECPA will allow for the three enforcement agencies to cooperate, share information and complete investigations in collaboration with our international partners

- By using a regulatory regime with prohibitions similar to those of our trading partners, international cooperation is facilitated and private rights of action concluded in Canada could also be pursued abroad

Viable, Comprehensive Compliance Regime

Regulatory enforcement would be undertaken based on expanding the mandates and using existing expertise of three agencies:

- **Canadian Radio-television and Telecommunications Commission (CRTC)**
  - Mandate to ensure the reliability, safety, and effective operation of telecommunications networks in Canada, including the Internet, C-27 will enable the CRTC to prohibit; the sending of unsolicited commercial electronic messages; altering transmission data without authorization; and installing programs on computer systems and networks without authorization
- **Competition Bureau**
  - Further to their mandate to ensure fair marketplace practices for businesses and consumers, C-27 will enable the Competition Bureau to effectively address false and misleading representations online and deceptive marketplace practices including false headers and website content
- **Office of the Privacy Commissioner (OPC)**
  - Responsibilities to protect personal information in Canada, C-27 will enable the Commissioner to effectively address the collection of personal information via access to computer systems without consent, and the unauthorized compiling or supplying of lists of electronic addresses

Legislative Remedies

Administration	Violation	Addressing
CRTC	ECPA includes violations respecting: • The sending of unsolicited commercial electronic messages • The use of telecommunications to alter transmission data and download programs to computer systems and networks without authorization	• Spam • Malware & Botnets • Network re-routing • Phishing (emails)
Competition Bureau	Amends the *Competition Act* to include violations respecting: • Misleading and deceptive practices/ representations, including false headers, subject lines, etc…	• False or misleading representations online (incl. websites and addresses)
OPC	Amends *PIPEDA* to include contraventions involving: • The collection and use of personal address information without consent by electronic or any other means • The collection of personal information by accessing, using, or interfering with computer systems	• Address harvesting • Dictionary attacks • Spyware (Personal Information)

Strong Penalties & Due Process

- The CRTC will use AMPs to ensure compliance with ECPA
- Amendments to the *Competition Act* allow the imposition of AMPs and other penalties
- S. 20(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. 20(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

The ECPA “Opt-in” Regime

ECPA 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 there is an “existing business relationships”, “existing non-business relationships”, or in other circumstances set out in regulations

The Private Right of Action (PRA)

- ECPA provides for a PRA for any violation
- The PRA would allow businesses, network providers and consumers to take civil action against anyone who violates ECPA
- 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 is expanded compared to the U.S. (which only allowed Internet Service Providers (ISPs) to pursue spammers) by allowing any person or enterprise to take action

International Cooperation

ECPA 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 ECPA 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 ECPA, 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 would support the ECPA 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
- Management of the Stop Spam Here website
- Directing research and measurement efforts (NCFTA, GCCR, UOIT)
- Analysis and reporting on emerging threats and trends (metrics)

Canada

A Comprehensive Response

ECPA incorporates the recommendations of the Task Force on Spam, elements of S-220, and anti-spam measures in place in other countries. 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