Industry Canada Industrie Canada

The Global Internet Economy:

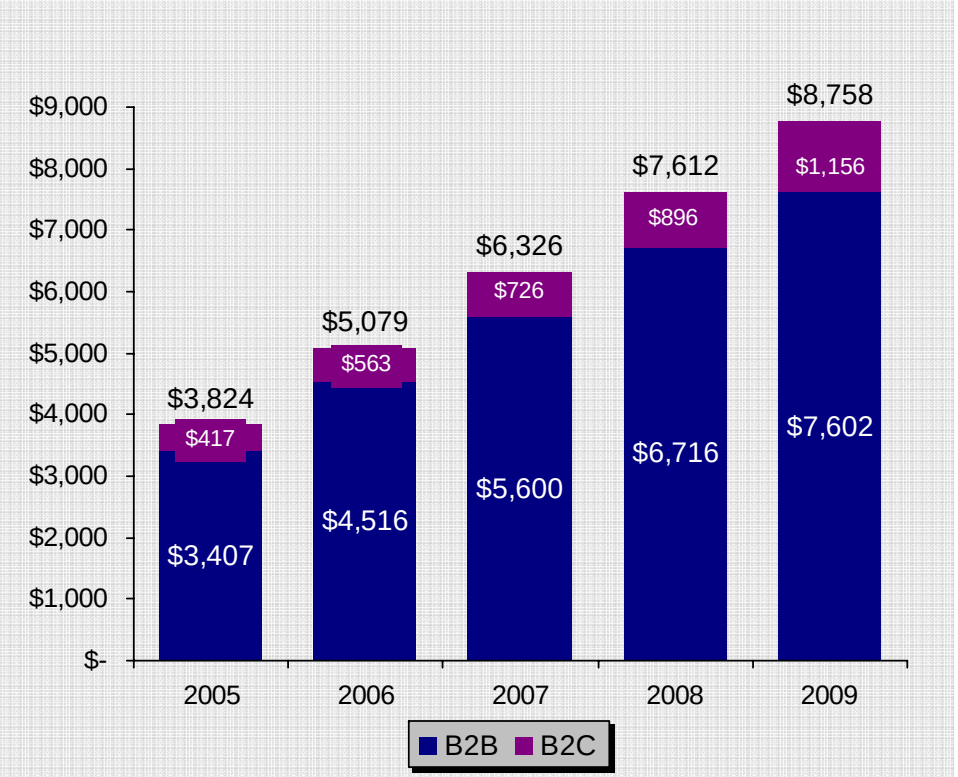
Public Policy Challenges and Responses

Richard Simpson
Director General
Electronic Commerce Branch
May 23, 2008

Canada

The Global Internet Economy

Worldwide E-Commerce Sales



- Worldwide e-commerce spending projected to grow at CAGR of 23%, exceeding $8.75 trillion in 2009
- The growth of B2B spending is comparably strong at CAGR of 22%, amounting to $7.6 trillion by 2009

Source: IDC, Worldwide Internet Usage and Commerce 2005-2009 Forecast update, April 2007

Canada's Stake in the Global Internet Economy

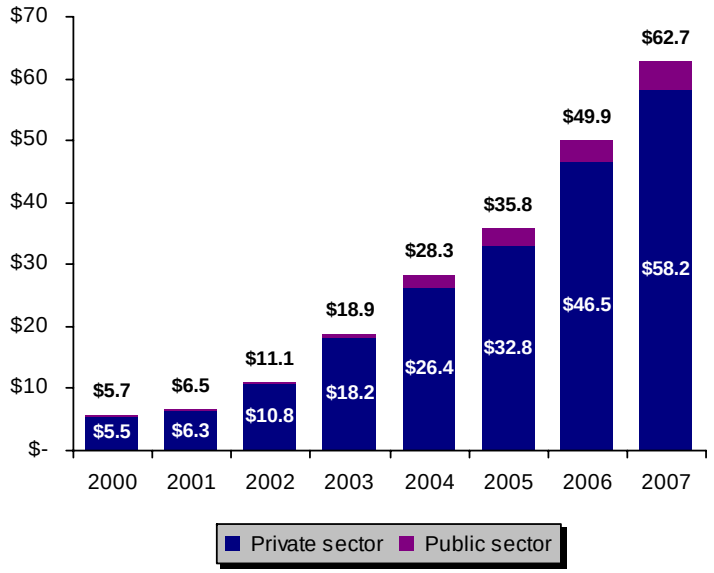
- Internet sales in Canada continued to grow in 2006 to $49.9 billion, up 40% from 2005

  (Statistics Canada, April 20, 2007)

- Canadian online advertising revenues totalled $1.01 billion in 2006, up 80% from $562 million in 2005

  (Interactive Advertising Bureau of Canada (IAB), April 2007)

Value of Canada's Total Internet Sales 2000-2007 (Billions)



Source: Survey of Electronic Commerce and Technology 2007, The *Daily, April 20 2007*, Statistics Canada

Online Threats are Growing

- Spam volumes remain high
  - 75 to 90% of email traffic is spam
  - represents hundreds of billions of messages
- New, more sophisticated and dangerous forms of spam continue to appear, and are increasingly the source of network damage and online fraud
- Now have a myriad of threats that go well beyond spam
  - phishing, botnets, spyware, computer viruses, & malware

Sources:

Messaging Anti-Abuse Working Group - MAAWG, 2nd Quarter, 2007; using 510 million mailboxes as a base

Sophos Security Threat Report, July 25, 2007

The Costs are Significant

- Growth of spam and related threats now a major drag on productivity and business competitiveness
- Costs to business and consumers estimated at $100 billion per year globally (Ferris Research, February 2007)
  - Phishing estimated at $850/incident and total damage to US economy is $630 million*
  - Spyware estimated at $100/incident and total damage to US economy is $2.6 billion*

* Source: Consumer Reports, State of the Net 2006

The Effects on the Internet Economy

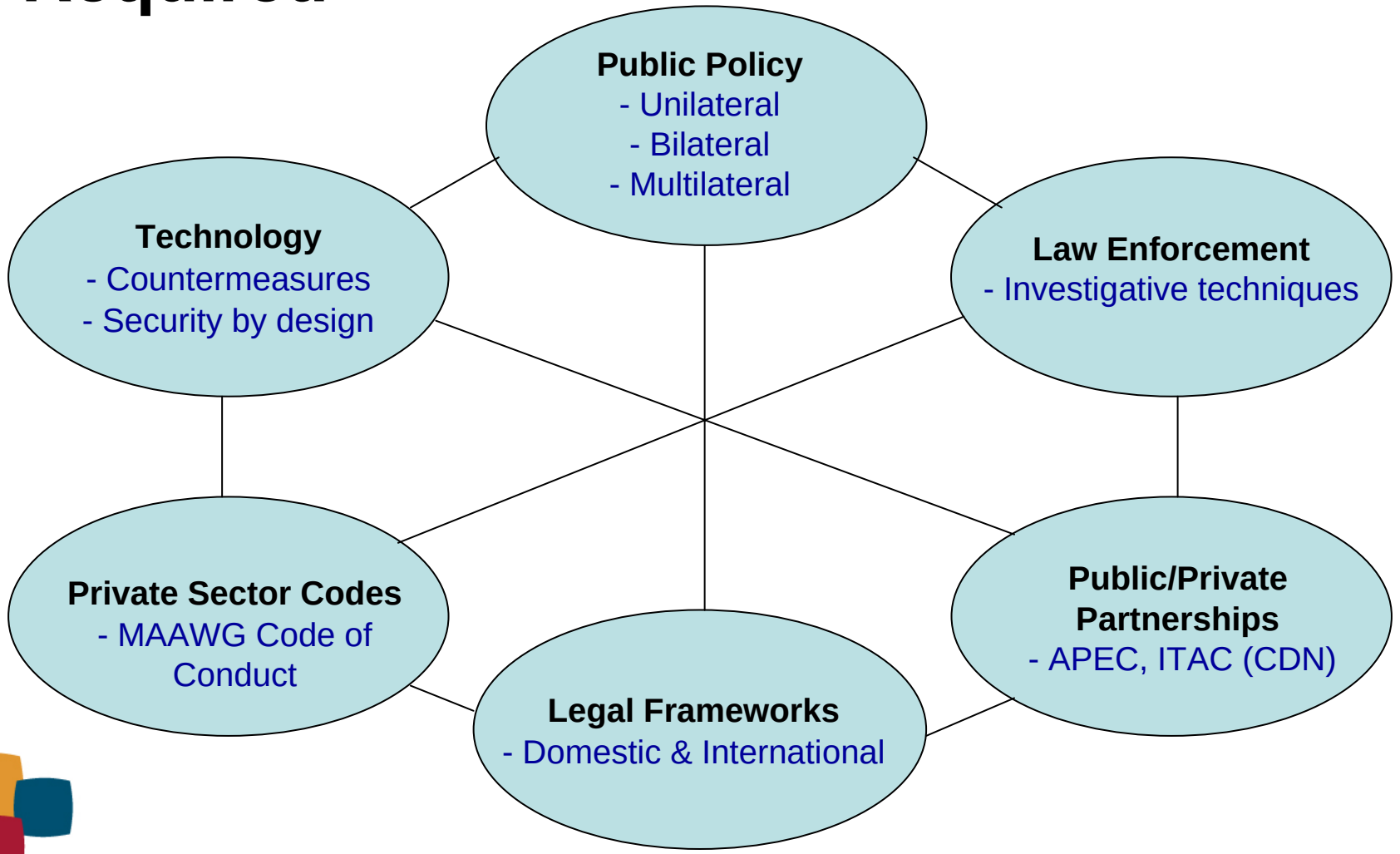
- An erosion of trust and confidence:
  - users changing their online behaviours due to security concerns
  - consumers losing trust in online banking and other services
  - business costs and concerns are mounting
- Internet is not reaching its full potential

The Importance of a Safer Internet

- A safe and secure Internet is essential in order to:
  - Maximize the social and economic benefits of the Information society
  - Assure proper functioning of critical information infrastructures
  - Build trust and confidence in e-business and e-government

- Given the global and interconnected nature of the Internet:
  - International cybercrime policy and law enforcement remains a significant challenge
  - International cooperation is multi-layered: legal, policy, and technological
  - Governments, civil society, public and private stakeholders are working together under the auspices of international fora such as OECD, G8, APEC, UNCITRAL, UNCTAD, OAS, ISO, ITU, and the IGF to build a safer and more secure Internet.

Integrated Global Approaches are Required



Three-tier Cyber Defence Strategy

1. Strong criminal law and effective law enforcement are important **BUT**
2. Robust domestic and international frameworks outside of the criminal law sphere are critical to enhance the power of the Internet as an economic driver and economic medium
3. Voluntary measures (i.e. private sector codes of conduct) that aim to protect the Internet economy should be encouraged

Law Enforcement and National Security

The Council of Europe's *Convention on Cybercrime*

- First international treaty on crimes committed via the Internet
  - Copyright infringement
  - Computer-related fraud
  - Child pornography
  - Violations of network security
- Seeks to harmonize national laws across signatories to facilitate international cooperation and improve investigative techniques
  - 43 signatories including non-European countries such as Canada, Japan, and the United States, 21 countries have ratified

International Response

- Ground rules for the Internet economy:
  - **Legal**
  - **Policy**
  - **Regulatory**
- Instruments that: (1) protect privacy; (2) strengthen information security; and (3) combat network threats
  - **OECD *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Information* (1980)**
  - **OECD *Security Guidelines* (2002)**
  - **APEC *Cybersecurity Strategy* (2002)**
  - **OECD *Recommendation and Guidance on Electronic Authentication* (2007)**

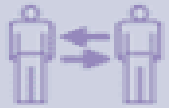
Private Sector Self-Protection and Empowerment

Messaging Anti-Abuse Working Group

COLLABORATION

How do we work together as an industry to jointly combat abuse?

- Develop an ISP code of conduct
- Develop a trusted inter-carrier network for messaging
- Develop and share industry best practices



TECHNOLOGY

What architectural frameworks and technology options are required to best combat abuse?

- Define a reference architecture and network standards for combating messaging abuse, including reduction of spoofing and prevention of identity forgery

POLICY

How do we effectively engage with policy makers?

- Build effective interfaces to key standards and legislative bodies

Forward Plan

- APEC Tel Min 7 Meeting (April 2008)
- OECD Ministerial on the Future of the Internet Economy (June 2008)
- WSIS Action Line C5: Building Confidence and Trust in the Use of ICTs – facilitated by ITU

Conclusions

- Three-Tier Cyber Defence Strategy
  1. Stronger criminal laws and enforcement
  2. Effective Ground Rules for the Internet Economy
  3. Private Sector Self-Protection and User Empowerment
- Businesses and Governments need to continue to work together


Canada