"Social and Economic Factors Shaping the Future of the Internet" Workshop, January 31, 2007

Richard Simpson, Director General, Electronic Commerce Branch, Industry Canada

Position paper for the International Dimension Session, addressing the question:
How do different governments view their role in balancing the needs and interests of users, service providers, industry, online content creators, and encouraging an environment that enables innovation, investment and growth?

The Role of Government

Governments seek to accelerate their country's transition to the network economy for the benefit of their citizens, with due respect to the values and the cultures of the country. This requires serving multiple stakeholder needs and ensuring that all their citizens have access to advanced telecommunications and information infrastructures and the ability to participate in the networked economy. They do this by creating a legal and policy environment that serves the public interest and fosters innovation, investment, productivity and economic growth.

Canada's public policy for the information economy has been based on an approach that:

- is inclusive, participatory and enabling;
- relies on multi-stakeholder partnerships and private sector initiatives; and
- is trans-national in scope.

In the early 1990's the Canadian federal government appointed the **Information Highway Advisory Board Council (IHAC***)* to advise on the policy measures needed to develop the Information Highway in Canada. In addition to providing a wide range of policy recommendations, IHAC laid out a blueprint for building an information society in Canada. The IHAC process also helped government develop a deeper understanding of "public access", and in turn influenced the design of pioneering programs such as the Community Access Program and SchoolNet from 1993 to 1999.

The **Canadian e-Business Initiative (CeBI)** was a voluntary, private sector-led partnership that aimed to further Canada's e-business success by focusing on productivity, leadership and innovation. CeBI helped to create the right environment for e-business in Canada by advocating e-business adoption and use, advising on tax and investment rules, branding strategies for Canada as a tech-savvy country, and benchmarking Canada's performance in the digital economy. CeBI produced a series of annual e-report cards grading Canada's progress in SME e-business adoption.

In 2004, the Government of Canada established the **Task Force on Spam** to consult Canadians on how to best achieve the objective of curtailing the growth of unsolicited commercial e-mail. The Task Force became a catalyst for combined private and public sector initiatives which addressed aspects of the spam threat, such as network management guidelines. Its final report, *Stopping Spam: Creating a Stronger, Safer Internet*, contained a range of recommendations, including more rigorous law enforcement, public education, policy development and legislation.

In 2005, the government appointed the **Telecommunications Policy Review Panel (TPRP)** to advise on the modernization of Canada's telecommunications policy framework. The Panel recommended that government should rely primarily on market forces to achieve telecom policy objectives, that it use well-targeted government measures in cases where the market has failed or is likely to do so, and that government measures be efficient and proportionate to their objectives. It recognized that federal, provincial and municipal governments may need to continue playing a role in fostering advanced network connectivity in areas where market forces have failed to operate effectively, as in the case of broadband access for isolated communities. The Panel also recommended benchmarking against other countries and their policies to continue to reap the potential economic and social benefits of evolving communication technologies.

During the past year government conducted multi-stakeholder consultations on framing a **digital content strategy** for Canada. In recognition of existing digital content initiatives in many sectors and jurisdictions across the country, the consensus was that a distributed strategy involving public-private partnerships for a digital Canada could maximize Canadian content preservation and public access and use. Demands were also made for government to provide enhanced access to content it controls or funds.

In conclusion, as a consequence of the convergence of networks and services to the Internet, the emergence of new societal expectations and the increasing global pressures for competitiveness, governments need to revisit their country's legal and policy environment ever more frequently.

<u>Trust and Confidence in a Borderless World</u>

Privacy protection in an online marketplace that is essentially borderless represents a major public policy challenge.

In the 1998 OECD Ministerial "Declaration on the Protection of Privacy on Global Networks", governments strongly endorsed the application of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, issued in 1980. The guidelines are technology neutral and can be widely used and applied in a variety of social and cultural contexts. National governments have effectively translated the guidelines into their own legal frameworks for online privacy protection, assigning specific responsibilities to public and private sector organizations. The Canadian approach consisted in balancing the need for a private sector-led, self-regulatory model with e-commerce and privacy legislation that built consumer and business confidence in the new medium. Enforcement efforts require continual reinforcement due to conflicts of jurisdictions and rapid technological change.

Privacy in "ubiquitous societies", brought about by pervasive computing and telecommunications, is an even greater challenge for policy makers. Ubiquitous networking or wireless data transfer and networking for anyone, any place and whenever, using different devices has become common place and is taken for granted. Surveillance cameras and sensors can be anywhere, and people increasingly depend on their always-on mobile phones with Swiss-knife functionality to keep in constant touch with others. Data trails and data can be retained indefinitely. The OECD has undertaken a review of the applicability of its privacy guidelines for sensor-based and linked technologies, and already some best practices and recommendations are emerging to help the designers of sensor based networks and the organizations that operate such networks ensure adequate privacy protection.

International Partnering

Cross-border law enforcement for online security, privacy and consumer protection depends on governments adopting better mechanisms for international cooperation. While international legal frameworks exist, governments need to develop effective methods for information sharing and for cross-border privacy law enforcement. Policy standards for sanctioning the misuse and abuse of the Internet are also needed. Canada has signed several bilateral and multilateral agreements for cross-border law enforcement cooperation, and it participates in both APEC and OECD efforts to further develop such frameworks.

Protecting the integrity of the internet also requires greater inter-governmental coordination. Key members of the international community, including the United Nations, the Council of the European Union, APEC and ASEM have recognised or used the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002). Many governments have developed effective national policies to address information system security threats and vulnerabilities. For example, the Government of Canada has increased its capacity to predict and prevent cyber-security attacks against its networks. It has also set up a national task force, with public and private representation, to develop a National Cybersecurity Strategy. At the international level, the Canadian Security Establishment maintains close intelligence relationships with peer organizations to address critical network threats and combat cybercrime.

In short, shaping the future of the Internet can best be achieved through multi-sector, multi-level and multilateral international cooperation, with the support of all governments.

Electronic Commerce Branch
Industry Canada

January 2007