Social and Economic Factors Shaping the Future of the Internet:
What the international community can do to protect the integrity of the Internet while facilitating e-commerce and global trade.

The Shrinking Globe – How the Internet has Brought us Together

The OECD's Committee on Information, Computer and Communications Policy, working with partners such as the *National Science Foundation's Global Environment for Network Innovations (GENI)*, plays an important role in identifying policies that assist countries and companies in protecting today's Internet and in laying the foundation for tomorrow's global networks. Governmental institutions, the private sector and civil society all have a role to play in determining how this highly evolved communication tool will further influence our society and how we live. The Internet's promise as an engine of growth is jeopardized by imperfect security protocols, unauthorized access to personal information, and on-line criminal activity. How governments address these and other issues will have a significant impact on the Internet's future power and potential for growth.

Some of the challenges governments face in sustaining the Internet's integrity and promise include network security attacks and data privacy breaches. The OECD serves as a neutral platform for governments to debate issues and seek common ground on Internet-related policies. Such efforts foster cooperation on several fronts including regional and global cooperation to find and prosecute criminal activity. The OECD also provides a valuable mechanism to link business, academic, and civil society interests in order to find the best possible ways to protect the Internet's integrity while at the same time balancing diverse interests. The advent of global communications necessitates cooperation among all concerned parties to cooperate and use many instruments -- including policy guidance, technical solutions, educational campaigns, and enforcement measures -- to combat online fraud, identity theft, and other threats yet to emerge.

Several examples of the OECD's valuable work on these issues include the 2006 Anti-Spam Toolkit, the 2002 Security Guidelines, the 1980 Privacy Guidelines, and ongoing work on identity management. The Anti-Spam toolkit consists of three key elements: (1) increased public awareness raising of the potential dangers of spam, (2) continued development of technical solutions to fight spammers, and (3) improved enforcement cooperation to enhance or implement local and international laws to prevent and stop spam. In its 2006 Spam Trends Report, Commtouch noted that spammers used millions of broadband connected computers to drive a 30% increase in spam. Spam is still a serious challenge to Internet users.

The OECD set a precedent in 1980 with its guidelines to protect privacy, and APEC established a solid privacy framework in 2004. Both are considered groundbreaking policy initiatives exemplifying regional cooperation on major issues impacting the growth of the Internet. They serve as primary references used by governments, civil society, corporations and the legal community to craft regional and country-specific privacy frameworks. In 2002, the OECD called for a new culture of security and revised its Security Guidelines to focus on increased awareness and protection of information systems and networks. Currently, the OECD is researching how governments and businesses can securely identify and authenticate users online while respecting privacy, and a workshop on identity management is planned for May 2006 in Norway.

Current Challenges to the Online Environment

The Internet has facilitated a convergence of technologies and applications that enables it to be accessed from anywhere, anytime, and from an increasing variety of devices. Companies continue to develop new applications and devices at breakneck speed. These are exciting developments that enable us all to communicate and conduct Internet transactions faster than ever. Unfortunately, this unprecedented accessibility paves the way for criminals to exploit the weaknesses inherent in open systems and networks. It has become clear to policy makers, enforcement officials and corporate executives alike that there is no one single challenge to the future of the Internet – though security and privacy are both key factors. Although OECD member countries treat security and privacy differently, all agree on the need to protect personal and business assets from intrusion and theft.

Security threats to the Internet are increasing. According to the 2006 Threat Report and 2007 Forecast of Trend Micro, a security software company, digital threats have increased by 163 percent and Web-based threats have increased by almost 15 percent in the past year. Spyware and adware are heightened, and some of it is evolving into malware. Gartner forecasts that by the end of 2007, 75 percent of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses. Trend Micro reports that on average, more than two-million different pieces of spam flood the Internet each month and more than 140,000 bots are flagged each month, which generates even higher amounts of individual spam messages. Without sufficient risk awareness, and safer online behavior, the future of the Internet could be in question. On privacy, there have been several high-profile compromises of personal information around the world. As a result, in the United States, industry and government have increased efforts to protect how personal information is stored, transmitted and used.

The International Trade Administration's (ITA) Role

The Commerce Department is a champion of innovation and encourages the development of technologies and policies to protect personal information and curb harmful network intrusions. ITA is a bureau of the Commerce Department, which seeks to promote overall trade and investment by strengthening industry competitiveness at home and abroad, and works to ensure fair trade practices. ITA views the Internet as a major contributor to information and communications technology (ICT) growth across sectors, and dedicates resources to research and export analysis of the ICT industry, and supports a formal high-tech trade advisory committee.

In support of the President's trade and competitiveness agenda to develop stronger public-private partnerships, ITA strives to build effective coalitions and ensure that organizations are communicating about threats and cooperating where possible to avoid creating loopholes for rogue players to exploit. A recent example was ITA's market development cooperator grant with the Better Business Bureau Online (BBBOnline) to promote trust online.

ITA places a high priority on its role in the OECD Working Party on Information Security and Privacy where we seek consensus on policy guidance to support an accessible and safe Internet, utilizing globally agreed to approaches to privacy and security. ITA also plays a leading role in the Asia Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group and encourages multilateral collaboration to further the goals of global cooperation on Internet policies.

Cooperation to Foster a Safer Internet

Following are some examples of work being done in the United States and international fora outside of the OECD to promote a safer Internet:

- **U.S. Efforts to Protect Personally Identifiable Information**. To realize the Internet's promise to contribute to economic growth, the United States has made preserving the Internet's integrity a top priority. In May 2006, President Bush established an Identity Theft Taskforce. Secretary of Commerce Carlos Gutierrez is a member of the Taskforce. The Taskforce has issued interim recommendations on identity theft prevention and how to improve government handling of sensitive personal data, authentication methods, victim assistance, and law enforcement. The Federal Trade Commission will host a workshop on authentication and identity theft in April to further explore solutions.

- **U.S. SAFE WEB ACT**: On December 22, 2006, the President signed in to law the US SAFE WEB ACT, which will better enable the United States and our foreign counterparts to cooperate effectively to combat spam, spyware, and Internet fraud and deception. The US SAFE WEB Act aims to protect consumers from cross-border fraud and deception by broadening reciprocal information sharing and investigative cooperation across borders.

- **U.S.-EU Safe Harbor**: The Department of Commerce leads the Administration's efforts to implement the U.S. – EU Safe Harbor Framework, which allows U.S. companies to meet the requirements of the EU's Directive on Data Protection when transferring personal data across the Atlantic. This is critical because it ensures lawful and uninterrupted transfers of personal information worth billions of dollars.

- **Council of Europe Convention on Cybercrime (CoC)**: The Council of Europe's Convention on Cybercrime, ratified by the United States in 2006, seeks a common international policy to protect society from cybercrime, by investigating and prosecuting criminals. The Convention fosters a step in the right direction for law enforcement cooperation against phishing, hacking, zombies, identity fraud and other threats to the Internet and e-commerce.

- **Computer Emergency Response Teams (CERTs)**: To combat security challenges, CERTs around the world are working hard to protect Internet related infrastructures, and their efforts should be coordinated and supported. The Department of Homeland Security created the United States Computer Emergency Readiness Team in September 2003 to protect the nation's Internet infrastructure by coordinating defense against and response to cyber attacks with Federal agencies, the private sector, the research community, State and local governments, and international entities.

Ideas for Future Action

In conclusion, here are some additional steps the international community should consider to strengthen the Internet's integrity, enhance security, and facilitate global access to information.

1. Review the Convention on Cybercrime in partnership with the private sector with a view towards implementation.

2. Educate users on Internet best practices as well as online threats; what to look for, what to avoid, and how to fix it if it goes wrong.

3. Create educational programs geared towards business needs that factor in (1) the responsibilities of all stakeholders, (2) cross-border cooperation and (3) the development of improved technical solutions to protect privacy and security.

4. Support industry innovation to create and improve technical solutions; do not stifle developments with burdensome or undue regulations.

5. Continue multilateral and bilateral cooperation to craft and implement policies designed to offer protections against online threats and prosecute rogue operators.

6. Encourage voluntary adoption of relevant guidelines published by the OECD and APEC on privacy, security, and spam, as well as related best practices published by government, industry and civil society.

7. Initiate public-private partnerships to build trust in online transactions.

8. Offer technical assistance programs to develop legal frameworks which combat on-line fraud.