

Security of Information Systems and Networks

Remarks of

Marc Rotenberg, President
Electronic Privacy Information Center
Washington, DC

APEC-OECD Workshop
Seoul, Korea
5-6 September 2005

Ladies and gentlemen, distinguished guests, fellow participants, thank you for the opportunity to provide a perspective from civil society on the work of the OECD and APEC on the Security of Information Systems and Networks. I thank the organizers of this important conference for bringing together experts, government officials, and representatives of civil society. I thank the co-chairs of the workshop: Peter Ferguson, Chair, Working Group of Information Security and Privacy, OECD and Dr. Inuk Chung, Chair, APEC TEL Working Group. And I thank the OECD, which has played a leading role in efforts to promote international policy frameworks for information technology that enable innovation and economic growth while respecting fundamental human rights.

Civil society has a particular interest in ensuring that the policies developed by the OECD member countries and the APEC market economies respect such interests as Article 12, on the protection of privacy, and Article 19, on freedom of expression, that are found in the Universal Declaration of Human Rights of the United Nations.

We believe that one of the central challenges facing government in our modern era is to ensure that the adoption of new technology improves the human condition broadly understood. Economic growth is an important indicator of the success of a modern economy. But a modern society should consider also literacy, health care, education, and a wide range of other indicators that help assess the value of investment in technology

In the area of information technology, there has always been a particular concern about the impact that new systems to automate databases will have on personal privacy. Records about our personal lives are now routinely recorded in digital formats and stored in information systems. The risk of misuse of personal information has been an ongoing concern for over thirty years. But the dramatic disclosures of identity theft in the United States, a crime now estimated to cost more than \$50 b to the US economy, has recently made clear the scope of the problem.

The OECD played a critical role in 1980 in the development of the Privacy Guidelines in seeking to ensure that information technology that enabled the transborder flows of personal information would safeguard personal privacy. The OECD Privacy Guidelines made clear that organizations that collect and use personal information should safeguard the information and ensure that it is not misused. The OECD Privacy Guidelines further established that individuals that provide personal information are entitled to certain rights, such as the ability to inspect and correct information. That framework has contributed to the development of important privacy laws and practices around the world.

In this context, the recent efforts of the OECD and the APEC to set out safeguards for the transborder flows of personal information in the APEC region and to apply OECD Framework for Computer Security represent the next chapter in the effort to develop appropriate policy frameworks for our modern information economies. We appreciate the work of the OECD and APEC delegates who participated in this process.

For this gathering, I will focus on the Framework for Computer Security. The Computer Guidelines consist of nine principles that aim to increase public awareness, education, information sharing, and training that can lead to a better understanding of online security and the adoption of best practices. The Guidelines are:

- *Awareness.* Participants should be aware of the need for security information systems and networks and what they can do to enhance security.
- *Responsibility.* Participants are responsible for the security of information systems and networks.
- *Response.* Participants should act in a timely and cooperative manner to prevent, detect, and respond to security incidents.
- *Ethics.* Participants should respect the legitimate interests of others and recognize that their action or inaction may harm others.
- *Democracy.* The security of information systems and networks should be compatible with essential values of a democratic society.
- *Risk Assessment.* Participants should conduct risk assessments to identify threats and vulnerabilities to their information systems.
- *Security Design and Implementation.* Participants should incorporate security as an essential element of information systems and networks.
- *Security Management.* Participants should adopt a comprehensive approach to security management.
- *Reassessment.* Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, measures, and practices.

Although the Guidelines are voluntary, they represent a consensus among OECD governments resulting from discussions that also involved representatives of the information technology industry and consumer advocates. OECD members, industry, and other participants will draw on the Guidelines in establishing policies, measures, and training programs for online security.

Civil society worked in support of the OECD computer security guidelines when they were first considered in 1992 and again when they were reviewed and reissued in 2002. In particular, we underscored the importance of the Ethics and the Democracy principles. We believe it is important, as the OECD has emphasized elsewhere, that policy frameworks for information technology respect important political and social values.

We also recognized in the development of the OECD Security Guidelines that there was a significant evolution of information technology throughout the last decade. In the early 1990s, the focus was on computing systems. By the end of the decade, the focus shifted to systems connected by networks. The revised Security Guidelines reflect this change.

At the same time, we did not favor the adoption of the phrase “A Culture of Security.” The phrase is inconsistent with the broader aims of the OECD. We are glad that this phrase has been modified somewhat in the United National General Assembly Resolution that speaks of a “Creation of a Global Culture of Cyber Security.” Still, we believe that the long-term challenge to maintaining the security and stability of our networks will require a “Culture of Transparency and Respect for Participants in the Information Society.” All of the principles of the OECD Framework for Computer Security would fit neatly under this heading.

The need for openness in the development of computer security policy was made clear at a meeting earlier this year in Madrid, hosted by the Club de Madrid. The International Summit on Democracy, Terrorism, and Security brought together leading technical experts, government officials, and representatives of civil society to address the challenge of security during a period of ongoing concern about future terrorist acts. The conference concluded with the release of the Madrid Agenda, which is "an agenda for action for Governments, institutions, civil society, the media and individuals. A global democratic response to the global threat of terrorism."

At the closing plenary session, UN Secretary General Kofi Annan urged governments to safeguard human rights and the rule of law. A special session on Democracy, Terrorism and the Internet issued a declaration, “The Infrastructure of Democracy” that urged governments to understand that an open Internet, like democratic government, provides the best response to future acts of terrorism.

We hope that the OECD countries and the APEC economic will continue to view the challenge of computer security in the larger context of transparency, respect for the individual, and the protection of human rights.

Finally, the recent hurricane in the United States and the tsunami in Asia last year remind us that the reliability of communications systems should remain a central concern for network managers and policy makers. Dependable communication systems can help ensure effective response to catastrophes and minimize human tragedy. A broad

understanding of network security requires recognition that there are many different types of threats to communication networks. We should not assume that all threats are man-made. The ability to respond to natural disasters is still a critical priority

We look forward to continuing to work with the OECD member countries and the APEC member economies on emerging policy issues concerning information technology. The participation of civil society in these projects will promote broader public support for the efforts of government and the private sector, and will help ensure that the outcomes address our common concerns.

REFERENCES

The Public Voice Website

<http://www.thepublicvoice.org>

EPIC, "Privacy Law Sourcebook: United States Law, International Law, and Recent Developments" (EPIC 2005) <http://www.epic.org/bookstore/> [Includes the texts of the OECD Privacy Guidelines and the OECD Cryptography Guidelines]

EPIC, "Privacy and Human Rights: An International Survey of Privacy Laws and Developments" (EPIC 2004)

"The Infrastructure of Democracy: Strengthening the Open Internet for a Safer World," March 11, 2005, available at http://thepublicvoice.org/news/infra_dem.html

OECD Guidelines for the Security of Information Systems and Networks (2002) http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html