

Cyber Security

*What does the Private Sector expect
from Governments?*

A Transatlantic Perspective

U.S. Embassy/RAND Europe Conference

The Hague

Jeffrey F. Pryce

Steptoe & Johnson LLP

9 April 2001

Outline

- General Principles of Regulation
- Challenges of Cyber-Security
- Prevention and Response
- Crime and Punishment

Favored U.S. Principles regarding Internet Regulation

- Minimalist, libertarian; presumption against govt direction/intervention.
- Industry-Led.
- Technology-neutral.

White House Framework for Global Electronic Commerce

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.

White House Framework (II)

4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.

2000 Panetta FRAMEWORK FOR SECURITY AND TRUST IN CYBERSPACE

- Private sector leadership.
- Government as a model citizen.
- Public-private partnership.
- Preserving fundamental values, even as technology changes.

Protecting Against Attacks on the Web

- Prevention.
 - Security measures; Firewalls; InfoSec procedures/technology; PKI; etc.
- Response.
 - Warning; Information Sharing and Analysis. IT-ISAC.
- Deterrence.
 - Finding and Prosecuting Attackers.

ISAC

Information Sharing and Analysis
Centers

ISACS

- Information Sharing and Analysis Center
- Industry leadership
- Support from U.S. Government
 - PDD-63
 - Independent, but cooperative relationship
- Established by Critical Sectors
 - Information Technology
 - Financial Services
 - Other Critical Infrastructure

Information Technology ISAC (IT-ISAC) Background

- Initial planning before Dec 1999
 - ITAA, Cisco/AT&T/KPMG
- Consensus reached Jun 2000
- Contractor selection Sep 19, 2000
- Incorporated Dec 20, 2000
- Announced Jan 16, 2001

IT-ISAC: Founding Members

- **AT&T**
- **Cisco Systems**
- **Computer Associates**
- **CSC**
- **EDS**
- **Entrust**
- **Hewlett-Packard Co.**
- **IBM**
- **Intel Corporation**
- **KPMG Consulting**
- **Microsoft**
- **Nortel Networks**
- **Oracle Corporation**
- **RSA Security**
- **Securify, Inc.**
- **Symantec Corporation**
- **Titan Systems Corp.**
- **Veridian**
- **VeriSign/Network Solutions**

IT-ISAC Mission

Report, respond to, and exchange non-proprietary information concerning electronic threats, attacks, and protective measures, and to establish a mechanism for “systematic and protected sharing coordination of information” regarding:

- Incidents and attacks
- Threats
- Vulnerabilities
- Solutions and countermeasures
- Resolutions
- Best security practices

Objectives

- Serve as focal point for coordination, cooperation, and sharing within IT community and between IT and other private sector and government electronic security activities
- Facilitate timely sharing of non-proprietary information
- Provide for systematic and protected sharing of sensitive information within IT sector
- Provide for coordination of IT sector efforts
- Encourage systematic sharing and coordination of cyber security practices

Crime:

Problems of Cyber-Space

- Information Sector
 - Attacks against computers.
- Law Enforcement
 - Challenges of finding and prosecuting criminals -- of all kinds -- who use computers.

Types of Crimes

- Cyber-Crime proper:
 - Crimes against Computers and Information Systems
- Ordinary Crime, making use of information systems
 - Fraud
 - Illicit content
 - Copyright

International Responses

Issues – Process and Forum.

1. Participation

a. Sector Participation:

- Law Enforcement
- Industry
- Civil Society

b. Regional, Global, Individual?

2. Transparency - Open or closed?

3. Scope

Issues – Vehicle for Action

- A. Analysis, foundational consensus-building.
- B. Guidelines, Best Practices
- C. Mechanisms for Cooperation
- D. Treaty
 - binding/enabling

Issues – Potential Subjects of Treaty Regulation

- Substantive Criminal Regulation.
 - i. Crime against Computers
 - ii. Computer-related Crime
 - iii. Criminal Copyright
- Data Interception and Preservation.
- Legal Assistance, Law Enforcement Cooperation.

Council of Europe (CoE) draft Convention on Cyber-Crime

CoE Draft Treaty

- Substantive Criminal Offenses.
 - i. Crime against Computers
 - ii. Computer-related Crime - Fraud, Content
 - iii. Criminal Copyright
 - iv. Aiding and Abetting
 - v. Corporate Liability
- Data Interception and Preservation.
- Mutual Legal Assistance, Law Enforcement Cooperation.

Project

- Some intended benefits:
 - Harmonization
 - Improving International assistance and cooperation
- Industry Interest in supporting law enforcement:
 - As Citizens
 - As Victims

Industry Concerns

- Breadth, scope, unintended consequences
 - Criminalization of legitimate activities
 - Intermediary Liability
- Surveillance - Costs, burdens, balance.
- Imposition of regulatory overlay on Internet
 - Legislative “pull”
 - Interpretation and Implementation

Art. 1 - Service Provider

“service provider’ means:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service.”

Art. 2 - Illegal Access

- Each Party shall ... establish as criminal offences ... when committed intentionally the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

“Without Right”

- “...without restricting how Parties may implement the concept in their national law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under national law.” [d.25 fn 7]

Illegal Access - fn 6

- Articles 2-5 are not intended to criminalise legitimate and common activities inherent in the design of networks, ... such as ... sending electronic mail without it having been first solicited by the recipient; accessing a web page or ftp (“file transfer protocol”) server that has been configured for public access; ... [d.25 fn 6]

Computer-related Fraud and Forgery

- Ordinary crimes, with use of computer added as element.
- Duplication.
- Technology-neutrality.

3d Party/Service Provider Liability

- Aiding and abetting (Art. 11)
 - Criminal liability for intentional failure to remove criminal material when “duly notified”
- Corporate Liability (Art. 12)
 - Action by a Leading Person
 - Lack of Supervision or Control

Private Assistance to Law Enforcement

- Parties shall empower authorities to compel service provider, within its existing technical ability, to collect and record (or assist authorities)
 - traffic data (art 20)
 - content data (art 21)
- Preservation of computer data for “adequate period of time”

Some issues

- Breadth and Impact of Substantive Crimes
- Intermediary Liability.
- Operational burden, lack of reimbursement.
- Privacy implications.
- Lack of due process provisions:
 - Independent review;
 - Procedural Regularity and Certainty;
 - Accountability and Protection from Liability.

Commentary on CoE Draft Convention

a. Industry:

- ITAA; US Chamber of Commerce; ad hoc coalition
- ICC; WITSA

b. Computer Experts:

- Purdue statement.

c. Civil Society:

- Global Internet Liberty Campaign

d. EU Data Privacy Authorities

- Opinion adopted March 22, 2001

e. CoE Parliamentary Assembly

- Hearing March 6; Opinion being adopted

Prognosis

- **Need for better analysis of Problems, dialogue and understanding**
- **Broader cross-sectoral and transatlantic dialogue in early stages**
- **Consensus by June difficult**

EU Process

- January 22 Communication on Info-Sec and Computer-Related Crime
- March 7 public hearing
- EU forum
- Early Process Indicia
 - Participation
 - Transparency
 - Scope

Conclusions

- Lay foundation on dialogue, cooperation
- Participation; Open process; broad scope
- Balance
- Careful drafting and narrow tailoring
- Habits more important than Legislation
- Security Critical to Internet; e-Commerce
- Internet-friendly regulatory paradigm crucial

Further Information

Jeffrey Pryce
Steptoe & Johnson LLP
1330 Connecticut Ave, NW
Washington DC 20036
+1 (202) 429.8121
jpryce@steptoe.com