ELECTRONIC FRONTIER FOUNDATION eff.org

Global Perspectives on Cybercrime

Eddan Katz
International Affairs Director
Electronic Frontier Foundation

Thai Netizen Network Public Forum
Bangkok, Thailand
July 27, 2009

International Efforts to Harmonize Cybercrime

- Council of Europe (CoE): Conference on Criminological Aspects of Economic Crime - Strasbourg (1976)
- U.S. Justice Department: Criminal Justice Resource Manual (1979)
- First Interpol Training Seminar for Investigators of Computer Crime - Paris (1981)
- Organization for Economic Cooperation and Development (OECD): Committee for Information and Communications Policy (ICCP) Recommendations (1986)
- G-8 Senior Experts on Transnational Organized Crime: High Tech Subgroup (1998)
- Association of Southeast Asian Nations (ASEAN): Ministerial Meeting on Transnational Crime (AMMTC) (2004)
- International Telecommunications Union (ITU) Global Cybersecurity Agenda (2007)

Defining Cybercrime

- Computer Crime
  - "any illegal act for which knowledge of computer technology is essential for a successful prosecution." US DoJ
  - "any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data." OECD Rec.
- updating technical means of prosecuting existing crimes committed using a computer
- new crimes where computer is object of crime
- Internet Jurisdiction

Unauthorized Access

- define a computer system as a protected environment and make control of access to this environment a protected right
- normal operations and exceptions
  - Security Research
  - Quality Assurance
  - Lack of harm or damage
  - Legitimate Use
  - Anti-Competitive Behavior

Mens Rea: Guilty Mind

- automation of processing and transmission
- complex operation of computer systems
- computer as subject of crime
  - Worms - viruses that self-replicate
  - Trojan Horses - contain hidden malicious code
  - Logic Bombs - activate at specific time
  - Sniffers - network analyzers
- functionality of code lacks specific intent

Convention on Cybercrime

- Illegal Access - infringing security measures, intent of obtaining data
- Illegal Interception - interception, without right, by technical means, of non-public transmission
- Data Interference - damage, deletion, deterioration, alteration, suppression
- System Interference - inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing
- Misuse of Devices - production, sale, procurement for use, import, distribution, making available; designed or adapted primarily for offense
- Computer-Related Forgery - inauthentic data, intent to defraud
- Computer-related Fraud - causing of a loss of property to another person

CoE Cybercrime Convention Explanatory Report

- legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized. (38)
- must be the specific (i.e. direct) intent that the device is used for the purpose of committing any of the offences. (76)
- Liability arises for aiding or abetting where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. (119)
- there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision. (119)
- A service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person, because the term "acting under its authority" applies exclusively to employees and agents acting within the scope of their authority. (125)

Guidelines for the Cooperation between Law Enforcement and Internet Service Providers Against Cybercrime - Council of Europe (2008)

- written procedures, information sharing, culture of cooperation, formal partnerships (10-13)
- protect fundamental rights of citizens - civil, political, & human rights (14)
- enforcing domestic & international data protection & privacy (15)
- procedures, training, technical resources, designated personnel (17-21)
- standardizing requests, specificity and accuracy requirements (25-27)
- ISPs encouraged to report offenses. not obligated to monitor (42)
- ensure that customer data and personal information not disclosed (51-52)

Information Intermediaries

- Hosting Providers
- Internet Service Providers
- Domain Name Registrars
- Financial Intermediaries
- Auction Platforms and eCommerce actors
- Search Engines
- Participative Web Platforms
- Virtual Worlds
- Distributed Computing
- Social Networks

Privacy

- Notice/Disclosure/Collection
- Choice/Consent
- Access
- Security/Integrity
- Enforcement/Redress
  - mandatory disclosure of personal information
  - public-private space distinction
  - content of communications
  - specificity of warrant

Access to Knowledge

- Innovation
  - Open Infrastructure
  - Collaborative Production
- Development
  - Economic Growth
  - Individual Autonomy

Open Innovation

- End-to-End Principle
- Interoperability
- Creative Destruction
- Level Playing Field
- Collaborative Production
- Modularity
- Granularity
- Freedom to Tinker
- Distributed Responsibility
- Self-Organizing Community
- Reputation Economies
- Correctability

Domestic Economic Growth

- Translation
- Adaptability to Local Customs
- Network Effects
- Open Standards
- Skill Development

Thank you.

- Eddan Katz
  - eddan@eff.org