ITU Model Cybercrime Law: Project Overview

October 2007

Jody R. Westby
<cybmail@itu.int>

ICT Applications and Cybersecurity Division
Policies and Strategies Department, BDT
International Telecommunication Union

The International Legal Landscape

- Cybercrime, Privacy & Cyber Security Are Global Issues
- 233 Countries Connected to Internet; 1.2 Billion Online Users
- Cybercrime, Privacy & Security of Information Infrastructure Important to National & Economic Security Interests & Public Safety
- Industrialized Countries Addressing; Developing Countries Lagging
- International Legal Framework Highly Inconsistent
- Cyber Security Investigations & Response Impacted by Legal Differences in Cybercrime Laws

Cybercrime Laws Protect Citizens

- Help Protect Freedom of Expression, Human Rights, & Other International Rights
- Enhance Statutory & Constitutional Rights (rights to privacy, protections on search/seizure & self-incrimination)
- Help Ensure Citizen Use of ICTs, Access To & Exchange Of Information
- Strengthen Consumer Confidence Against Fraud

Cybercrime Laws Important to Developing Countries

- Confidentiality, Integrity, & Availability of Data & Networks Central to Attracting FDI and ICT Operations
- Protect Integrity of Government & Reputation of Country
- Keep Country from Becoming Haven for Bad Actors, Repositories of Data
- Instill Market Confidence & Certainty Regarding Business Operations
- Provide Protection for Protected Information & Facilitate Cross-Border Data Flows

Cybercrime Laws Important to Developing Countries cont’d

- Protect Consumers & Assist Law Enforcement, Intelligence Gathering
- Deter Corruption & Fraud
- Increase National Security & Reduce Vulnerabilities
- Provide a Means for Prosecution and Civil Action for Cybercrimes
- Increase the Likelihood Electronic Evidence Will be Obtained

Computers Can Engage in Cyber Criminal Activities 3 Ways

- Can be Target of Offense: When Confidentiality, Integrity, & Availability of Data, Applications, Networks are Compromised
- Can Be Tool to Commit a Crime, Includes Fraud, Child Pornography, Conspiracy
- Can Be Incidental to a Crime But Have Significant Importance to Law Enforcement, Especially for Evidentiary Purposes

Consistent International Legal Framework is Emerging

- U.S., Europe, G8, OECD, Council of Europe are Global Leaders
- CoE Convention on Cybercrime
- EU Ministers of Justice adopted the Proposal for a Council Framework Decision on attacks against information systems on March 4, 2003.

Consistent International Legal Framework is Emerging cont’d

- G8
  - Ten Principles to Combat High-Tech Crime
  - Action Plan to Combat High-Tech Crime
  - 24/7 Point of Contact Network (45 countries)
- OECD Guidelines for the Security of Information Systems & Networks
- APEC Cyber Security Strategy, APEC-ASEAN Joint Workshop 2007

Areas Highlighting Need for Harmonization

- Definitions & Scope
- Jurisdictional Provisions
- Substantive Provisions
- Procedural Provisions
- International Cooperation

Definition & Scope

- Vary in Definition, Form, and Penalties
- Industrialized Nations' Laws Protect Computer & Communication Systems and Data Transiting & Residing In These Systems
- Cybercrime Laws Generally Apply To:
  - Use of computers & Internet for illegal purposes (viruses, hacking, unauthorized acts)
  - Crimes against communication systems
  - Crimes facilitated by the use of a computer
  - Wiretap, pen register, and trap and trace laws to protect privacy and facilitate investigations

Jurisdictional Issues

- Possible for Cyber Criminal to be Physically Located in One Country, Weave an Attack Through Multiple Countries & Computers, and Store Evidence on Servers in yet Another Country
- Victims May be All Over Globe, Jurisdiction Questionable
- Internet Borderless but Law Enforcement Must Stop at Borders
- Substantive & Procedural Laws of Countries May Conflict, Creating Evidentiary Issues
- Letters Rogatory & Multilateral Assistance Treaties (MLATs)
- Dual Criminality Requirements Very Problematic
- Needs to be Way to Secure Extradition; Extradition Treaties One Method

Substantive Provisions

- Illegal Access
- Illegal Interception
- Data Interference
- System Interference
- Misuse of Devices, Passwords
- Computer-Related Offenses (forgery, fraud, child pornography, © infringements)
- Aiding & Abetting
- Corporate Liability

Procedural Provisions

- Laws Can Restrict Government Access to Real-Time Interception of Communications & Traffic Data (Wiretaps); Content is Protected More Than Traffic Data
- Laws Can Also Restricts Access to Stored Electronic Data
- Be Aware of Constitutional Protections & International Law
- Requirements Vary: Upon Court Order, Search Warrant, Subpoena

Procedural Provisions cont’d

- Actual Search & Seizure of Data Requires Skill
- Important to Follow Rules of Criminal Procedure, Protect Chain of Custody to Prove Integrity of Data, and Preserve it for Transport
- Best Practice Guides Available from U.S. Government, State Governments, Prosecutors, American Bar Association, Canada, & London Internet Exchange (LINX)

International Cooperation with Law Enforcement

- Cyberspace Has No Borders, But Law Enforcement, Diplomats, & Investigators Do
- Interpol and Europol are Important Global Links
- Interpol & Europol Do Not Investigate: Passes Requests from Country to Country
- Interpol has National Central Bureaus in Each Country

International Cooperation with Law Enforcement cont'd

- Staffed by One of More Law Enforcement Agencies
- Interpol Actively Involved in Information Technology Crime (ITC) Through "Working Parties" of Experts
- Collection & Preservation of Evidence May be Difficult; Evidence May Be Useless in Court

Judicial & Statutory Common Protections for Live Interceptions

- Approval Should Be Obtained from Independent Official (Judge) Based on Written Application and Manifested in Written Order
- Approval Should Be Granted Only Upon Strong Factual Showing of Reason to Believe That the Target of the Search is Engaged in Criminal Conduct & Less Intrusive Methods Not Adequate
- Each Surveillance Order Should Cover Only Specifically Designated Persons or Accounts; Generalized Monitoring Should Not Be Permitted

Judicial & Statutory Common Protections for Live Interceptions cont'd

- Rules Should Be Technology Neutral
- Scope & Duration of Interception is Limited to Only What is Necessary to Obtain Evidence
- In Criminal Investigations, Those Who Have Been Subject of Interception Should be Notified When Investigation Concludes (Whether Charged or Not)
- Personal Redress or Suppression of Evidence at Trial is Provided for Violations

Model Cybercrime Law Project

- American Bar Association Privacy & Computer Crime Committee (Section of Science & Technology Law)
- Produce Draft Law & Explanatory Comments
- Same/Similar Format as UNCITRAL Model Laws (Electronic Commerce & Electronic Signatures)
- ITU to Make Available to Developing Countries to Help Them Establish Legal Frameworks

Participants

- Multidisciplinary
  - Industry, Policy Experts, Academicians, Government Personnel, Technical Experts, Attorneys)
- International (Canada, Germany, India, Israel, Latvia, Japan, Mexico, Nigeria, Sri Lanka, UK, US)
- No Cost to Participate, Open to Interested Persons

Approach

- Develop Matrix of Provisions of Laws (Council of Europe + 10 Developed Nations)
- Comparative Analysis of Laws
- Working Groups by Topic Areas
- Teleconferences (Skype) & Email
- Drafting Model Law & Explanatory Comments
- Review & Editing Across Working Groups
- Completion Date: March 1, 2008

Overall Goal:

Develop Model Cybercrime Law that Will Promote Global Harmonization & Assist Developing Countries In Establishing Legal Frameworks for Cyber Security

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/itu-d/cyb/
- Cybersecurity Resources and Activities
  - www.itu.int/ITU-D/cyb/cybersecurity/
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
  - www.itu.int/ITU-D/cyb/events/
- Cybersecurity Publications
  - www.itu.int/ITU-D/cyb/publications/

More Information cont'd

- ABA Privacy & Computer Crime Committee Publications
  - International Guide to Combating Cybercrime
  - International Guide to Privacy
  - International Guide to Cyber Security
  - Roadmap to an Enterprise Security Program
- FREE to people in developing countries: Send email to westby@mindspring.com
- ITU Cybercrime Model Law Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

International Telecommunication Union

Helping the World Communicate