OBTAINING DIGITAL EVIDENCE

LEGAL ISSUES

This presentation was developed by the
Computer Crime and Intellectual Property Section
Criminal Division, United States Department of Justice
LAW AND DIGITAL EVIDENCE

- Computers and the Internet have opened new doors for criminal activity

- Challenges to law enforcement:
  - Identifying the perpetrator and extent of the crime
  - Volatility of electronic data
  - Need for fast and confidential investigations

- Criminal procedural law must adapt to meet these challenges
DISCUSSION

A FRAMEWORK FOR DIGITAL EVIDENCE

DIGITAL EVIDENCE PROCEDURES
INTERNATIONAL STANDARDS

• Cyber crime is a **worldwide** challenge

• **Domestic** laws establish procedures for obtaining digital evidence
  ○ Enable successful investigation and prosecution
  ○ Improve international legal cooperation
INTERNATIONAL STANDARDS

• A model: The Convention on Cybercrime
  ○ Crimes related to computers and the Internet
  ○ Provisions for investigating cyber crime
  ○ International legal cooperation
  ○ Protection of human rights and liberties
TYPES OF INFORMATION

• Content data
  o The substance, purpose, or meaning of a communication or other data

• Traffic data
  o Data generated by a computer relating to a communication

• Subscriber information
  o Information held by a service provider relating to a subscriber, other than content or traffic data
**WHAT DATA DO WE SEEK?**

- More conditions and safeguards as privacy interests increase

<table>
<thead>
<tr>
<th></th>
<th>Stored</th>
<th>Real-time Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic Data</strong></td>
<td>Privacy Interest</td>
<td>Privacy Interest</td>
</tr>
<tr>
<td><strong>Content Data</strong></td>
<td>Privacy Interest</td>
<td>PRIVACY INTEREST</td>
</tr>
</tbody>
</table>
DISCUSSION

A FRAMEWORK FOR DIGITAL EVIDENCE

DIGITAL EVIDENCE PROCEDURES
GENERAL CONSIDERATIONS

• Every legal system has different procedures and limitations on obtaining evidence

• Procedures generally include provisions to protect the confidentiality of an investigation

A CAREFUL BALANCE:

Law Enforcement Interests  ↔  Respect for Human Rights
PRESERVATION OF DATA

• Enables competent authorities to order the expeditious preservation of specified stored computer data

• May include partial disclosure of traffic data

• Prevents loss or modification of data
  ○ Intentional or accidental deletion or modification
  ○ Business practices
PRODUCTION ORDER

• Enables competent authorities to order:
  ○ A person to submit specified stored computer data
  ○ A service provider to submit subscriber information

• Different standards may apply to content data and traffic data
SEARCH AND SEIZURE OF STORED COMPUTER DATA

• Enables competent authorities to search and seize:
  ○ A computer system and its stored data
  ○ A data-storage medium (for example, drives, disks)

and to copy the data
REAL-TIME COLLECTION OF TRAFFIC DATA

• Enables competent authorities to:
  ○ Collect or record **traffic** data in **real-time**, by technical means
  ○ Compel a service provider to collect or record traffic data within its technical capability, or assist law enforcement

• Requires significant conditions and safeguards
INTERCEPTION OF CONTENT DATA

• Enables competent authorities to:
  ○ Collect or record **content** data in **real-time**, by technical means
  ○ Compel a service provider to collect or record content data within its technical capability, or assist law enforcement for investigations of serious offenses

• Requires significant conditions and safeguards
QUESTIONS?

A FRAMEWORK FOR DIGITAL EVIDENCE

DIGITAL EVIDENCE PROCEDURES