24/7 High Tech
Crime Network

Albert Rees
Computer Crime & Intellectual Property Section
Criminal Division, U.S. Department of Justice
24/7 Network

• “The G-8 24/7 Network for Data Preservation”

• Points of contact in participating countries that require urgent assistance with investigations involving electronic evidence

• About 48 participating countries, including:
  Brazil  Canada  Chile
  Jamaica  Mexico  Peru
Electronic Evidence

- E-mail
- Chat logs and instant messenger info
- Web-based email
- Web pages
- Data stored in computers
- Customer records
- And more…

THIS EVIDENCE CAN DISAPPEAR QUICKLY
Internet Service Providers (ISP)

- Essential link to the Internet
- Accessing the Internet through an ISP creates important records and other information
  - Customer records
  - Connection information
  - Stored data

THE ISP OFTEN HAS CRITICAL EVIDENCE
The ISP and Investigations

• Locating the ISP
  – An ISP’s servers may be anywhere in the world
  – Often in the United States

• Working with the ISP
  – Law enforcement point of contact
  – Requests from outside the country

• Data retention practices differ
  – ISP policy
  – A country’s laws

• Data preservation is key step in investigation
US Approach to Data Preservation

- Law enforcement contacts ISP & requests that any existing data be retained
- Contact can be by mail, e-mail, fax
- Contact can be 24/7
- Appropriate legal process to obtain data
  - Subpoena, court order, search warrant
  - Exception for emergencies
Why a 24/7 Network?

• Importance of timely response to cybercrimes

• Need to find and preserve electronic evidence
  – Data stored on computers and storage devices
  – Data and records kept by ISP

• Need to identify points of contact
  – Law enforcement organization with cyber expertise
  – Knowledge of local laws and procedures
24/7 Operations in the US

- Computer Crime & Intellectual Property Section (CCIPS), Department of Justice is the point of contact

- Each day one prosecutor takes 24/7 calls

- Duty mobile phone for calls after office hours
24/7 Process

• CCIPS receives call

• Requestor identifies assistance sought
  – Preserve records
  – Report online criminal activity in US affecting requesting nation
  – Shut down web site
    • Child pornography
    • Phishing
24/7 Process

• CCIPS determines if request indicates a violation of US law

• If US law is violated, CCIPS contacts appropriate US law enforcement
  – US law enforcement works with requesting law enforcement to obtain needed evidence
  – Evidence obtained & shared informally between law enforcement agencies
24/7 Process

• If no US law is violated
  – CCIPS can contact ISP to request record preservation
  – CCIPS informs requesting country of results of preservation request

THE 24/7 PROCESS IS AN IMPORTANT STEP, BUT IS NOT A SUBSTITUTE FOR FORMAL PROCEDURES
Providing Electronic Evidence Through Diplomatic Channels

- Convention on Cybercrime
- MLAT
- Letters Rogatory
- US obtains requested info by subpoena, court order or warrant & provides to requesting agency
CCIPS Ways to Expedite Preservation

- Identification of major ISPs in US
- Identification of legal points of contact at ISPs
- Many US ISPs have developed procedures on timely processing of law enforcement requests
24/7 Network Membership

- Contact point available 24/7
- English speaking
- Technical knowledge
- Knowledge about domestic laws and policies
24/7 Network Membership

• Capability
  – Knowledge of ISPs in country
  – Knowledge of legal points of contact at ISPs
  – Knowledge of cyber law enforcement agencies in country
    • Prosecutor
    • Police
24/7 Network Membership

• Capability
  – Knowledge of law enforcement authority to compel ISPs to
    • Preserve records
    • Provide records
  – Knowledge of procedures to provide information in accordance with international law

LARGE OFFICE NOT REQUIRED!
Joining the 24/7 Network

- Informal process
- Registration form
International Cooperation Is Necessary for Success

- Online criminals operate internationally
  - Electronic evidence can be anywhere
  - ISPs operate internationally

- Countries must work together to meet this challenge
  - Improved formal and informal mechanisms
  - Better person-to-person contacts
FOR MORE INFORMATION

Albert Rees

+1 (202) 514-1026

albert.rees@usdoj.gov