The FBI: Security and Privacy

Global Forum 2006

Special Agent Robert Flaim
Federal Bureau of Investigation

Presentation Goals

- How the FBI balances privacy with security in investigating cyber crime:
  - Privacy: US legal requirements when conducting investigations
  - Security: The use of technology to keep the Internet secure

USA Legal Requirements

- Based on 4th Amendment of U.S. Constitution “right to privacy”
- Electronic Communications Privacy Act: 18 United States Code (U.S.C.) 2701 – 2712

Investigative Legal Tools

- 2703 (f) Preservation Request
- Federal Grand Jury Subpoena
- 2703(d) court orders
- Search Warrants
- Trap and Trace/Pen Register
- Consensual Monitoring
- Title III – Wiretap

FBI Cyber Division

- Primary goal - to enhance the FBI's capability to protect the US against cyber based attacks and high tech crime
- Cyber Squads active in all 56 FBI field offices

Cyber – Traditional Crimes

- Cyber Crime Investigations
  - Child pornography
  - Phishing, spam
  - Terrorism
  - Fraud
  - Slave trade
  - Theft of Intellectual Property (IPR)
  - Stalking
  - Sale of drugs or other contraband

Cyber – Internet Crimes

- Computer Intrusion Investigations
  - Distributed Denial of Service (DDoS) attacks
  - Malicious code (viruses, worms, trojans)
  - Botnets and Pharming
  - Malicious intrusions into computers/networks
  - National Security Threats
    - Cyber Terrorism

Use of Technology

- The FBI uses many of the same publicly available technologies to identify, capture, and prosecute the criminals the criminals use, such as:
  - Domain & IP WHOIS queries
  - DNS
  - VOIP
  - Web sites, forums
  - Encryption
  - Google
  - And many others

Technology Use Example

WHOIS

WHOIS

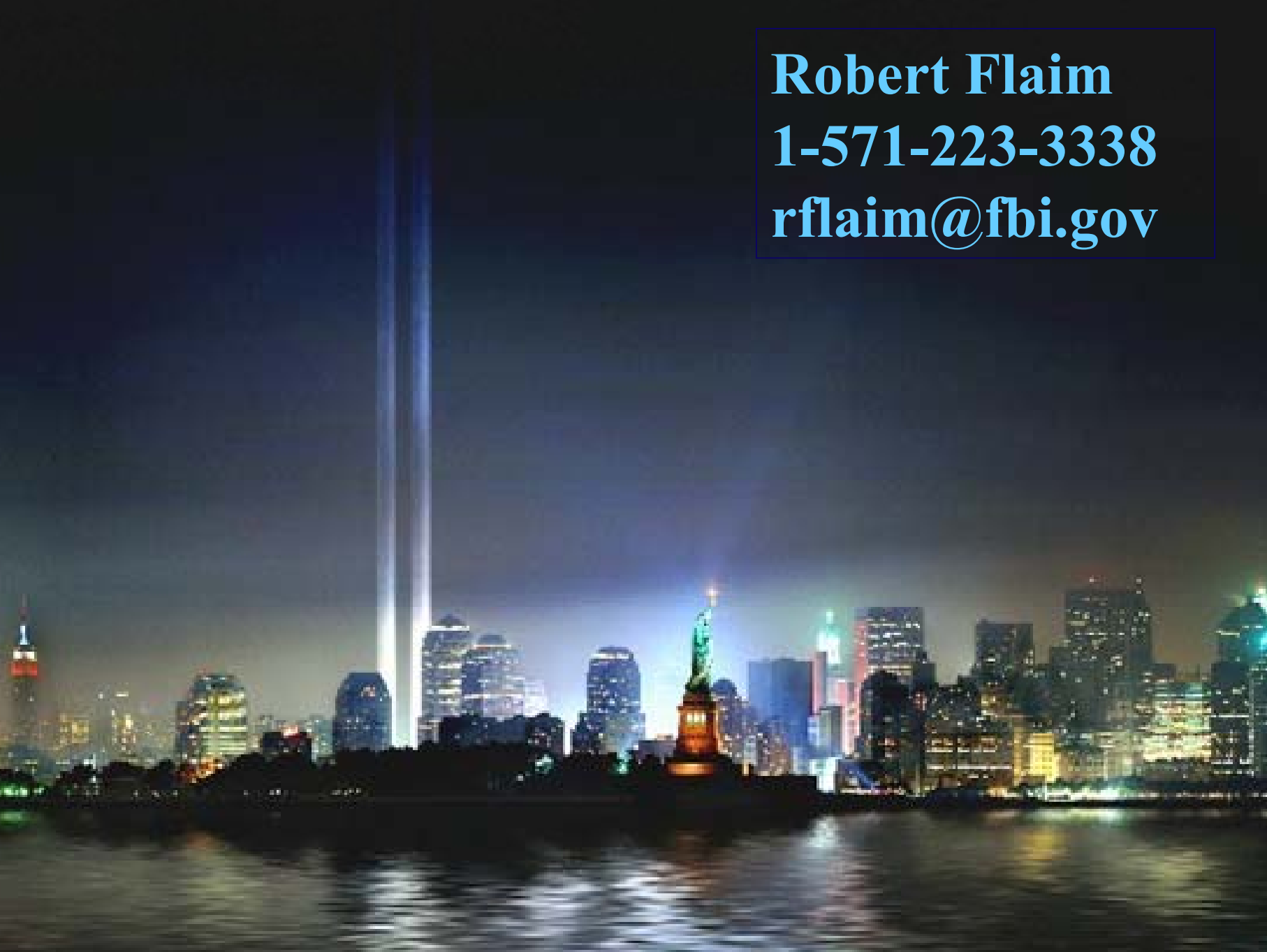
- IP and domain name WHOIS information is an integral tool for all cyber investigations
- These tools provide gap analysis, target profiling, and sometimes even - identification
- **Speed and accuracy in getting the data is key**

WHOIS - Investigative Use

- 9/11 and Anthrax Investigations
- International criminal investigations: mytob, norway/spain murder case
- Multiple kidnappings
- Child pornography
- Many other including phishing, botnets, pharming, IPR, Internet gambling, and Internet fraud related investigations

ICANN Luxembourg 2005

- International Law Enforcement session
- Reps from Australia, Spain, Malawi, UK, Japan, Interpol
- Importance of accessible and accurate WHOIS



Robert Flaim
1-571-223-3338
rflaim@fbi.gov