OUR MISSION

• To promote the two concepts that make up our title
  o “Justice” — equality, equity, and fairness
  o “Rule of Law” — requirement for certain procedures and principles to be followed in each case to reach a correct result

FUNDING

• This project is supported by grants by the Bureau of Justice Assistance, U.S. DOJ, and by Mississippi State University

- Points of view or opinions in these training sessions are those of the authors and do not represent the official position of the U.S. Dept. of Justice
MATERIALS

- **Handouts:**
  - Structure of Fourth Amendment Analysis
  - Current Supreme Court cases (periodically updated online)

- **Online Materials:**
  - Computer Searches & Seizures (article online)
  - Power point presentations and materials available at www.NCJRL.org

www.NCJRL.org

FOURTH AMENDMENT INITIATIVE

Promotes awareness of search and seizure principles

- Conferences for state judges
- Computer searches and seizures
- Annual symposium / published lectures

Publications at www.NCJRL.org
ANNUAL FOURTH AMENDMENT SYMPOSIA
2002: Technology
2003: Race & Ethnicity
2004: “Tools” to Interpret
2005: Computer Searches and Seizures
2006: Role of Objective v. Subjective Intent
2007: Independent State Grounds
2008: Border Searches -- digital and physical
2009: “Great Dissents”
2010: Fourth Amendment Rights of Children
2011: The Future of the Fourth Amendment

CYBER CRIME & DIGITAL EVIDENCE PUBLICATIONS & PROJECTS
Lots accessible online at www.NCJRL.org
Including:
• Email delivered Cybercrime Newsletter
• Internet Victimization Symposium
• Materials on Computer-Related Crime

UPCOMING EVENTS
• Oct. 2 – Webinar - Hiding Tracks: Proxy Servers and Private Networks
• Oct. 30 – Webinar - Location Tracking Technologies
• Nov. 27 – Webinar - Peer-to-Peer Offenses: BitTorrent Investigations
WHAT IS CYBER CRIME?

- No consensus definition for cyber crime
- Basically, it is any crime in which a computer or other digital device plays a role; any crime involving digital evidence

DEFINING CYBER CRIME
BY FUNCTION

• The digital device is used as either:
  – *(1) Container* – digital device contains evidence of criminal activity
  – *(2) Tool* – digital device is used to commit a crime
  – *(3) Target* – digital device is the target of the crime

DEFINING DIGITAL EVIDENCE

- Information that is stored or transmitted in binary form that may be relied upon in court.
  – Where digital evidence may be found:
    • Computers
    • Hand-held devices with “embedded computer systems”
    • Digital cameras
    • Personal digital assistants (PDAs)
    • Mobile phones
    • Servers, including: Internet service providers, FTP and web servers, email servers, & local area network (LAN) servers
    • Online activities
OBTAINING DIGITAL EVIDENCE

• Types of Digital Evidence:
  – User created: text, address books, bookmarks, databases, images, video/sound, web pages, hidden files
  – Computer created: email headers, metadata, activity logs, browser cache, history, cookies, configuration files, printer spool files, swap files, surveillance taps

DIGITAL EVIDENCE EXAMPLE

• Scott Peterson - Five computers revealed Peterson’s Internet searches as he planned his criminal behavior

DIGITAL EVIDENCE EXAMPLE

• State v. Carroll, 778 N.W.2d 1 (Wis. 2010) – state charged the defendant with felony gun possession and as evidence they used a picture found on his cell phone showing him holding a semi-automatic weapon

*Not the real photo from the case*
DIGITAL EVIDENCE CHALLENGES

• Requires specialized equipment and personnel training;
• Technology is constantly developing and criminals rapidly adapt to these changes;
• Interstate and international aspects raise jurisdictional issues

DIGITAL EVIDENCE PROTECTIONS

What happens when we press the send button?

Do we have a protected interest?

INSIDE THE BOX v. OUTSIDE THE BOX

What is stored on your computer: Documents, Pictures, Outlook Emails, Internet Cache, etc.

What is not stored on your computer: Online email accounts, Internet shopping accounts, Social networking accounts, Cell site location data, Website contents, etc.
THE FOURTH AMENDMENT

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

THE FOURTH AMENDMENT

IN EVERY Case:
1. Does the Fourth Amendment apply?
   - Government activity "search" or "seizure"
   - Protected interest: liberty, possession, privacy
2. Is it satisfied?
   - Was search/seizure reasonable?
   - Warrant Clause Requirements?
3. [Remedies]

WHEN DOES A PERSON HAVE A R.E.P. IN DATA ON A COMPUTER?

Case law has examined a variety of situations
1. Person’s Own Computer
   - Info on screen
   - Data in computer
2. Work & Government Computers
   - Monitoring and other policies that affect R.E.P.
   - Who has access to computers
FEDERAL v. STATE GUARANTEES

• States are free to interpret OWN constitution to provide more protections to individuals
• Increasing trend
• See 77 Miss. L.J. 1 (2007) (info on developments)

DEVELOPING ISSUES

Do established rules apply to digital evidence containers?
• Should file names or types limit the scope of a search?
• Do technological search programs make the file cabinet analogy inadequate?
• Does the nature or amount of material make computers different from other containers?
• Should there be limitations based on search execution procedures with warrants for digital evidence?

OUTSIDE THE BOX FRAMEWORK

• Uncertain whether Fourth Amendment applies outside the box
• Ex: The non-consensual acquisition of email
  o Possible analogies:
    - Letter in the mail
    - Numbers dialed on a telephone
    - Telephone conversations
    - Information possessed by third party
STATUTORY PROTECTIONS

• Statutory provisions tend to be primary protection for outside the box data
• Congress has enacted some statutory regulations that apply to computer network investigations
  – Stored Communications Act
  – Wiretap Act
  – Pen Register / Trap and Trace
DAY 1: INSIDE THE BOX

- Introduction to Digital Evidence & Computer Forensics
- Private Search Doctrine
- Reasonable Expectations of Privacy
- Satisfying the Fourth Amendment
- Warrantless Searches & Seizures

DAY 2: OUTSIDE THE BOX

- The Internet & Network Technologies
- Typical Investigations Involving Digital Evidence
- Fourth Amendment & Statutory Framework Regulation
- Technology Framework – Tracking Technologies
- Legal Framework – Tracking Technologies

QUESTIONS?

Don Mason
Associate Director
National Center for Justice and the Rule of Law
662-915-6898
drmason@olemiss.edu
www.ncjrl.org