Cyber Crime Initiative

Link w/ national organizations, state-wide agencies to develop model projects to facilitate prosecution of persons engaged in computer-related crime.
Promotes awareness of search and seizure principles
National Judicial College conferences for state trial and appellate judges
Annual Symposium Address important search and seizure issues, published in the Mississippi Law Journal.
James Otis Lecture Annual lecture by noted scholar.
Computer Searches and Seizures Judicial and prosecutor training w/ NAAG and Mississippi State University

Publications at www.NCJRL.org

Prosecution Training
partner: National Association of Attorneys General
only national training program to help combat computer-related crime for AG Offices from all 50 states
23 conferences to date

Law Enforcement Training
partner: Mississippi State University
search and seizure of computers and other sources of digital evidence
Law Student Training
specialized courses, externship placements, and summer employment with prosecution-related organizations
Judicial Training

partner: National Judicial College

- search and seizure
- computer-related / digital search and seizure
- Internet Crimes Against Children

partner: Mississippi State University

- search and seizure of digital evidence

ICAC survey course of crimes

Survey: Technology Assisted Crimes Against Children

OCT 11-12, 2010 (Oxford)

4 day search and seizure course

Comprehensive Search and Seizure for Trial Judges

Reno -- May 24-27, 2010
OXFORD -- Oct 4-7, 2010
**digital evidence courses**

**Computer Searches and Seizures for Trial Judges**
- **OXFORD** -- Sept 9-10, 2010
- **OXFORD** -- Aug 25-26, 2011

**Technology-Assisted Crimes Against Children: Pretrial Motions Practice**
- May 20-21, 2010 (Reno)
- Spring, 2011 (Reno)

**appellate judge conferences**

**Foundational Fourth Amendment Principles and Annual Fourth Amendment Symposium**
- Oxford --- March 9-11, 2011

**Symposium: The Future of Fourth Amendment Analysis**
- Oxford - March 10, 2011

**Cyber Crime and Digital Evidence Publications / Projects**
- Lots on line at [www.NCJRL.org](http://www.NCJRL.org)

**including:**
- Email delivered Cyber Crime Newsletter
- Internet Victimization Symposium
- Materials on computer-related crime
Power points and reference materials available at:

WWW. NCJ RL.org

---

Overview of Fourth Amendment considerations in the digital world

1. Big picture of internet-related investigations and how to approach search and seizure analysis
2. Applicability issues
3. Two approaches to satisfaction

---

Federal vs. State guarantees

States free to interpret OWN constitution to provide more protections to individuals

- Increasing trend: PA, CT, OR, ....
- Contra CA, FL, ... prohibited from doing so

- Symposium, 77 Miss. L.J. 1 (2007) lots of info on developments ....
Article 14, MA Declaration of Rights

Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions.

All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

Massachusetts

The Framers' Intent: John Adams, his Era, and the Fourth Amendment, 86 Ind. L.J. __ (2010)

Annual James Otis Lecture

Amend. IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
digital searches and seizures

digital searches and seizures

the crime scene

new crimes & new techniques

computer at Target

- unauthorized access, damage, theft
- spam, viruses, worms
- denial of service attacks

computer as Tool

- fraud
- threats, harassment
- child pornography

computer as Container

- from drug dealer records to how to commit murder

just a murder!

- studied currents
- researched bodies of water
  - including San Fran Bay
- how to make cement anchors
- tide charts

had 5 home computers
applicability and satisfaction

IN EVERY CASE, ....

1. Does the 4th Apply?
   A. gov't activity: "Search" or "Seizure"
   B. Protected interest: liberty, possession, privacy

2. Is it Satisfied?
   "Reasonable"
   Warrant Clause requirements

   [3. Remedies?]

Digital Evidence Searches and Seizures

1. Is the Fourth Amendment applicable?
   inside the box vs. outside the box

2. Is it satisfied?
   two approaches to digital evidence

conceptual difficulties of applying traditional doctrines to digital evidence
"inside the box, outside the box"

part #1: Outside the box: network investigations
- Tracing electronic communications
  - E.g., finding IP (Internet protocol) address
- Identifying suspect and account

part #2: Getting to and inside the Box:
- Identifying who was at keyboard when crime occurred
- Locating computers to be searched
- Obtaining warrant or consent to search
- Searching and seizing evidence
- Forensic analysis
uncertain F/A applicability outside the box

non-consensual interception of communications, etc, over the Internet to another party

ease: email

possible analogies:

its like a letter in the mail
its like numbers dialed on a telephone
its like any info possessed by third party

statutory protections tend to supercede

Congress / states have enacted some statutory regulation of computer network investigations:

- Stored Communications Act
- Wiretap Act
- Pen Register / Trap and Trace
Vanlandingham tells police

- in Yahoo! chat room using screen name “dana_hotlips05,” chatted w/ “stevedragonslayer”

- “stevedragonslayer” invited him to watch web cam video of nude 6 to 9 year-old girls

- V-- informs “stevedragonslayer” he likes “young hard stuff”

- “stevedragonslayer” plays videos of young girls in explicit sexual acts

- gives police copy of chat room conversation
Police use ECPA to get Yahoo! subscriber info for screen name “stevedragonslayer”

- records: “stevedragonslayer” logged on to Yahoo! website from address 68.103.177.146

---------------------------------------------
- Electronic Communications Privacy Act ("ECPA") regulates disclosure of electronic communications and subscriber information
- IP (Internet Protocol) address is unique to specific computer at any one time

Yahoo records:

“stevedragonslayer” logged in on Yahoo website from IP address
68.103.177.146

what do you do next?

- go to: IP locator service
  http://www.geolo.com

IP address assigned to Cox Communications

- What do you do next?
  get disclosure order from Cox

- Cox informs that all the time reported by Yahoo, IP address was used by account of Steve Perrine
  11944 Rolling Hills Court
  Wichita, Kansas

- can get all subscriber info, including screen names, type and length of service, method of payment, etc
**Next steps:**

- PA -- contacts Kansas authorities

**KS:**
- Steve Perrine has prior state conviction for sexual exploitation of child / still on probation
- Wichita police obtain search warrant for Perrine's house

**Warrant executed:**
- seize computer computer
- observe firearms / drug paraphernalia
- get amended search warrant to seize those items
- forensic examination of Perrine's computer:
  
  **16,000 images of child pornography**

**Perrine's legal claims: the big picture**

- **ECPA**
  - violations: no suppression
  - stds for obtaining info & what info police can get

- **Fourth Amendment**
  - no protection for subscriber info
  - no protection: P2P shared files
  - search of house did implicate F/A:
    - apply standards for warrant issuance and execution
governmental responses: 
investigating on the internet / networks

three different legal frameworks for investigation

1. obtaining info that has no legal regulation
2. Fourth Amendment applicability
3. statutory regulation

using publicly available tools: no legal regulation

info available using advanced Internet tools

- NS lookup, Whois, Finger, Traceroute, Ping
- Domain names, IP addresses, networks, contact persons

protections mostly statutory for network investigations

Fourth Amendment protections for data held by networks or in remote locations is unclear

Statutory regulation:

- SCA
- Wiretap Act
- Pen Register / Trap and Trace
significant statutory considerations

1. type of surveillance
   - real time vs. stored info

2. type of information is gov't seeking
   - content vs. non-content

Real time vs. stored surveillance

two types of Network surveillance

1. **Real time**: monitoring of communications in transit

2. **stored records**: retrospective surveillance

Statutory regulation depends on type of surveillance