Fourth Amendment issues: part 1

applicability and satisfaction issues in Internet Child Pornography cases

Thomas K. Clancy
Director
National Center for Justice and the Rule of Law
The University of Mississippi School of Law

part I

- framework of Fourth Amendment analysis
- when does one have a reasonable expectation of privacy in data?
- some recurring issues in Child Pornography cases

part II

- seizing and searching mobile devices

Funding!

NCJ RL is funded in part by a grant to the National Center for Justice and the Rule of Law by the Office of Juvenile Justice Delinquency and Prevention, US DOJ.

Points of view / opinions are those of the presenters and do not represent the official position of the U.S. Department of Justice.
National Center for Justice and the Rule of Law

Conferences
Training
Projects
Publications

Cyber Crime Initiative
Link w/ national organizations, state-wide agencies to develop model projects to facilitate prosecution of persons engaged in computer-related crime.

Fourth Amendment Initiative
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

25 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
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

---

**Cybercrime Newsletter**

**JANUARY-FEBRUARY 2010**

**TABLE OF CONTENTS**

- FEATURES
- UN FIGHTING CYBERCRIME
- IN THE COURTS
- SUPREME COURT NEWS
- LEGISLATIVE NEWS
- NEWS YOU CAN USE
- FREE TRAINING

Like to feature articles written by you. Please con-
tact us with information, prepared articles and com-
ments about this newsletter. There are:

**SUPREME COURT TAKES 4TH AMENDMENT TEXTING CASE**
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
1. Does the Amendment apply?

A. need Government Intrusion: "Search"
   assume government is examining digital evidence on computer

B. Intrusion must invade protected interest:
   reasonable expectation of privacy of suspect

Privacy: main interest protected

"The principal object of the Amendment is the protection of privacy . . . "
Soldal

Gov't Activity: "SEARCH"

Reasonable expectation of privacy test

1. person exhibits actual, subjective expectation of privacy

2. society recognizes that expectation as Justified / Reasonable / Legitimate

   Smith v. Maryland, 442 U.S. 735, 740 (1979)

   If either prong missing, no protected interest
partial list -- NO R.E.P.

Prison Cells
Handwriting
Facial Characteristics
Movements Outside
Open Fields
Bank Records
Trash
VIN numbers
Field testing of suspected drugs

NO PROTECTED INTEREST -- F/ A does NOT apply --

How to find "legitimate" expectation of privacy?
look to:

1 real property law

2 personal property law

3 "understandings that are recognized or permitted in society"


"inside the box, outside the box"

The Box
Outside the box: network investigations
when does person have REP in data in computer?

case law has examined variety of situations:

1. person’s own computer
   - info on screen
   - data in computer

2. work and gov’t computers
   - monitoring and other policies that affect REP
   - who has access to computer?

Traditional F/A doctrine

No F/A Protection from 3rd Party Disclosures to Gov’t

Rationale: Risk Analysis -- Voluntary Exposure

- misplaced belief to whom voluntarily confides will not reveal secret
  Miller
- such “risk” is “probably inherent in the conditions of human society”
  Hoffa
- vol. exposure to public eliminates F/A protection
  Katz

voluntary disclosure

assume risk that third party will disclose information, item to gov’t
Peer-to-Peer (P2P) Networks
file-sharing technology --- creates virtual networks
criminal activity:
- Copyright Infringement
- Computer Hacking
  - Worms -- Viruses -- Theft of information
- Child Exploitation and Pornography

Law Enforcement Response
search file sharing networks for known child porn images
Questions:
- “Search” w/in meaning of 4th Amendment?
- Does user connected to Internet via P2P have reasonable expectation of privacy in files in shared folders?

no REP in P2P
U.S. v. Ganoe, 538 F.3d 1117 (9th Cir. 2008)

"To argue that Ganoe lacked the technical savvy or good sense to configure Lime Wire to prevent access to his child pornography files is like saying that he did not know enough to close his drapes."
connecting computer to local network

US v. King, 509 F.3d 1338 (11th Cir. 2007)

connected own laptop in dorm room to military base network
knew activities on network subject to monitoring
airman looking for music found porn on King’s computer
after report, investigator located King’s computer on network
  • found porn file
  • additional CP files
REP?

hard drive contents “akin to items stored in the unsecured areas of a multi-unit apartment building or put in dumpster” accessible to the public

same principles applied --- No F/A protection against

1. disclosure of subscriber info by ISPs

2. Email recovered from recipient


3. Internet chat rooms

   doctrines:
   voluntary exposure
   assumption of risk

4. Posting Info on a Website

Quon: some answers?

- cop sent text messages to wife, mistress via gov’t issued pager
- agency reviewed printouts obtained from provider to determine if needed more capacity for police business

issues:

1. Quon have REP in messages?

2. Wife / mistress have REP in messages?
Formal Written Policy
- explicitly said user had no REP
- could audit, monitor, or log all activity
- not for personal use
- Quon aware of and signed

"Informal Policy"
- Lt. Duke: you pay overages, will not audit

Should Quon be treated differently than Wife / mistress?

Possible analogies as to the Women:
- its like letter in mail
- its like numbers dialed on telephone
- its like any info possessed by third party

Child pornography:
Distinct category of prohibited speech

  - does not have to meet obscenity test

* Osborne v. Ohio, 495 U.S. 103 (1990)
  - permissible to ban mere possession of CP

  - has to be a real kid
Federal Crimes

- Production
- Sending/Distributing
- Receipt
- Possession
- Viewing
- Pandering

probable cause: some recurring issues

- in general
- membership in CP websites
- use of profile information
- staleness

claim: NO PROBABLE CAUSE TO ISSUE WARRANT

Only Evidence Admissible at Hearing:

1. Affidavit submitted to magistrate who issued warrant.

2. MS: oral testimony given by affiant to issuing magistrate that was basis for issuing warrant.
Key inquiry on PC:

issuing judge must be supplied w/ sufficient information to support independent judgment that PC exists

The more information put in statement of probable cause, more likely warrant issued and motion to suppress denied!!!

What Probable Cause Means

PC = fair probability that contraband or evidence will be found

totality of circumstances examined

PARTICULARIZED: --- must be able to point to specific location and have info relating to that particular place to be searched.

OBJECTIVE: -- point to identifiable facts about place and be able to state why those facts support PC to search.

PC statements in CP cases

Search warrant must establish:

1. Is image sexually explicit?

   Give as much detail as possible and / or attach image

2. Does image depict real child?

   Affiant’s statement --- image appears to be real child is sufficient

   E.g., U.S. v. Love, 516 F.3d 580 (7th Cir. 2008)
   (estimated age of person depicted)
Justice Stewart

“*I know it when I see it.*”

Jacobellis v. Ohio, 378 U.S. 184 (1964)

“Child Pornography”

- visual depiction (photo, film, video, digital)
- of sexually explicit conduct

1. using minor (under 18) engaging in the conduct
   or
2. digital or computer-generated image that is, or is indistinguishable from, a minor
   or
3. created or modified to appear that identifiable minor is engaging in act

18 U.S.C. § 2252A CP Prevention Act

“Sexually explicit conduct”

- Sex acts
  - Actual or simulated
    - sexual intercourse (genital-genital, oral-genital, anal-genital, or oral-anal, between persons of same or opposite sex)
    - bestiality
    - masturbation
    - sadistic or masochistic abuse
  or
- “Lascivious exhibition” of genitals or pubic area
“Lascivious Exhibition”

- Nudity not required
  
  *U.S. v. Knox*, 32 F.3d 733 (3rd Cir. 1994)

- Six factors + others appropriate to case
  
  
  *U.S. v. Hill*, 459 F.3d 966 (9th Cir. 2006)

“Lascivious Exhibition”

- Test: Six non-exclusive factors: *Dost*
  
  - Focal point -- genitals or pubic area?
  
  - Setting sexually suggestive?
  
  - Child in unnatural pose or inappropriate clothing?
  
  - Child fully or partially clothed, or nude?
  
  - Suggest coyness or willingness to engage in sexual activity?
  
  - Intended to elicit sexual response in viewer?

recent cases discussing sufficiency of description of “lasciviousness” in warrant application

*United States v. Hill*,
459 F.3d 966 (9th Cir. 2006)

*United States v. Genin*,
594 F. Supp. 2d 412 (S.D. N.Y. 2009)

Excellent summary of case law

- append pics
- detailed descriptions of activity
probable cause to believe "mere" member of website has CP on computer?

considerations:

- does site have both legal / illegal materials? -- if so, less likely probable cause exists

- what if site has only illegal materials?
  - most courts: mere membership = probable cause
  - some courts: not enough -

  *U.S. v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (collects cases)

additional info beyond membership

- site focus is clearly CP

- evidence of actual downloading of child porn

- automatic transmission as part of site's services

- use of suggestive screen names / email addresses
  - (ex) Littlebuttsue ; Littletitgirly

more PC evidence ....

- prior convictions for sex offenses involving children or child porn

- possession of child erotica

  *U.S. v. Hansel*, 524 F.3d 841 (8th Cir. 2008)
nexus: is suspect a collector?

- need some evidence suspect is collector
  
  Ellis v. State, 971 A.2d 379 (Md. App. 2009)  
  (affirming striking profile material from warrant affidavit)

- all of previous slides indicate maybe collector

- PLUS assertion by affiant what collectors do is sufficient  
  See U.S. v. Paull, 551 F.3d 516 (6th Cir. 2009)

internet child pornography collectors

- no typical profile ----

- Store images on computer media

- Collect as many images as they can

- Tend to organize collections

- Keep collection for long time

Why CP Retained Long Periods

- Initial collection difficult to obtain – illegal

- Social stigma

- Images used for trading, or as currency

- Emotional value

- Addiction?

- Kept in secret and secure places
  - in private homes, for example
overcoming staleness
judicial recognition collectors keep CP long period of time

- U.S. v. Morales-Aldahondo, 525 F.3d 115 (5th Cir. 2008)
  (3 years since last download)
- U.S. v. Perrine, 518 F.3d 1196 (10th Cir. 2008)
  (111 days after chat room images displayed on web cam)
- State v. Felix, 942 So. 2d 5 (Fla. App. 2006)
  (about 6 months after email sent)
- Mehring v. State, 884 N.E.2d 371 (Ind. 2008)
  (collects authorities)

Overcoming Staleness

statements in affidavit RE:

- Deleted files - ability to recover
- Protracted activity / continuing conduct, rather than one-time download
- Info from ISP when account last accessed

nexus to home: where are the pictures?

"common sense" suspect has them in home

- it's a place of privacy
- it has access to internet

E.g., State v. Samson, 916 A.2d 977 (Me. 2007)