Third Party Doctrine

Fourth Amendment considerations of obtaining Digital Evidence

National Center
For Justice And The Rule Of Law

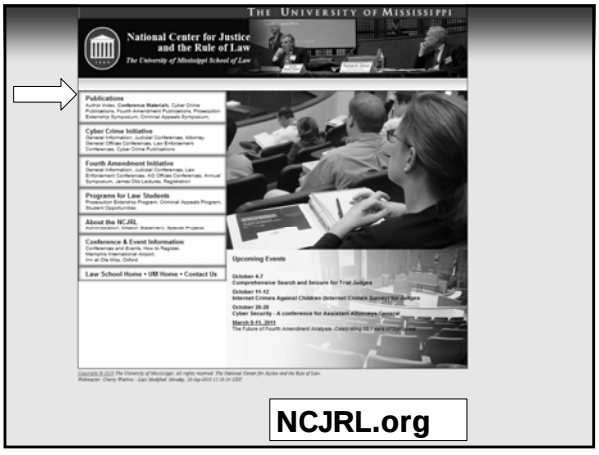
University of Mississippi
School of Law

Thomas K. Clancy
Director

www.NCJRL.org

Power points and other materials available at:

WWW. NCJRL.org



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

Cyber Crime and Digital Evidence Publications / Projects

lots **on line at www.NCJRL.org**

including:

Email delivered Cyber Crime Newsletter

Internet Victimization Symposium

Materials on computer-related crime

WEBINARS on Internet Technology

Web Browsing 101

Hiding Tracks on the Web

Interactive Media

Mobile Devices

Peer-to-Peer Technologies

Emerging Uses/Cutting Edge Technologies

recorded/ live at NCJRL.org

Grant-funded Judicial courses

- **Comprehensive Search and Seizure for Judges**
- **Searches and Seizures of Computers and Digital Devices**
- **Internet Crimes Against Children**

structure of 4th Amendment analysis

IN EVERY CASE, ...

1. Does the 4th Apply?

A. Gov't activity: "Search" or "Seizure"
B. Protected interest

2. Is it Satisfied?

[3. Remedies?]

analytical structure of applicability question

1. Protected interest is necessary but not sufficient condition
focus: *individual's* interest -- privacy

2. Must be gov't invasion – "search"– of that interest.
focus: *governmental actions.*

This session assumes step #2 and focuses on step #1.

protected interests

4th:

"The right of the people to be SECURE in their persons, houses, papers, and effects . . . ."

step #1: is object on list?

person, house, paper, or effect

step #2: quality protected?

does defendant have protected interest in that object implicated by gov't activity?

objects protected

only four objects protected: persons, houses, papers, and effects

step #1: is object on the list?

(ex) open fields – not on list

(ex) "house" -- includes apts, hotel rooms, businesses

step #2

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

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"

California v. Ciraolo, 476 U.S. 207 (1986)
Rakas v. Illinois, 439 U.S. 128 (1978)

1990s battleground

"standing" : Guests in houses

1. ***Olson***

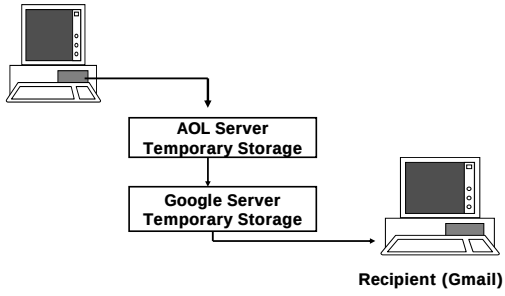
   -stayed overnight

2. ***Carter***

   - bagged cocaine for a couple hours

21st Century battleground

obtaining evidence



two fundamental considerations

1. **Content vs. Non-Content:**

   Fourth Amendment does not protect NON-content from gov't search

2. **location of search for content:**

   Where does one have reasonable expectation of privacy so as to be able to object when gov't obtains Content ?

type of information is gov't seeking

content:
the communication itself

non-content:
addressing information

Obtaining NON - content

- by "Search"
- Fourth Amendment DOES not apply

NON-content is not protected by Fourth Amendment

Pen register recorded numbers dialed by telephone

Smith v. MD, 442 U.S. 735 (1979):

- robber kept calling victim
- Amendment does NOT protect non-content
- no REP in numbers dialed
  - -- voluntarily conveyed info to 3rd party
  - -- assumed risk of disclosure

Pen Register / Trap & Trace: gets non-content

18 U.S.C. §§ 3121-3127

- get "dialing, routing, addressing, or signaling information"
- Not a search under 4th Amendment

  U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008)

  - to/from addresses
  - IP addresses of websites visited
  - volume of info to/from his account

Non-content Information

- Dialing, routing, addressing, or signaling information
- Basic customer or subscriber records
- Transactional information

same definitions as in SCA

Email Info with Pen/Trap

- get most e-mail header information
  - "To", "From"
  - IP address & port
  - For both source & destination
- But not
  - "Subject" line of e-mails
  - Content of downloaded file

Post-Cut Through Dialed Digits

- numbers dialed after call initially set up
- includes acct #s, pin numbers, ID #s, social security #, credit card #s

Content or Non-content?

- In re Application, 515 F. Supp. 2d 325 (E.D.N.Y. 2007):

  "functional equivalent of the human voice"

URLs (uniform resource locators)

- Content or not?

www.biosupplies.com / mailorder / Anthrax.htm

host — path or "file path"

In re application, 396 F. Supp. 2d 45 (D. Mass. 2005):
same as post-cut through digit extraction

Legal requirements for Pen / Traps

- gov't can get order when 18 U.S.C. § 3123
  1. authorized attorney applies under oath for order and
  2. assert that "information likely to be obtained is relevant to an ongoing criminal investigation"
- no independent judicial determination of 2

In re application

Obtaining Content

- substance of communication
- **fundamental question:**

  does person objecting to search have reasonable expectation of privacy (REP) in info / data in location where it is found ?

information held by third parties

general rule: never have standing to challenge disclosure of information held by third party

ex: records of deposit at bank

***U.S. v. Miller,* 425 U.S. 435 (1976)**

only exception to date?

hospital records of medical tests of pregnant women indicating drug use given to law enforcement by hospital --- BUT premised on assumption woman did not consent to test

***Ferguson v. City of Charleston,* 532 U.S. 67 (2001)**

Traditional F/A doctrine: non-digital world

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**

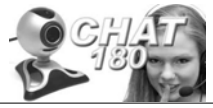
  Miller
- **such "risk" is "probably inherent in the conditions of human society"**

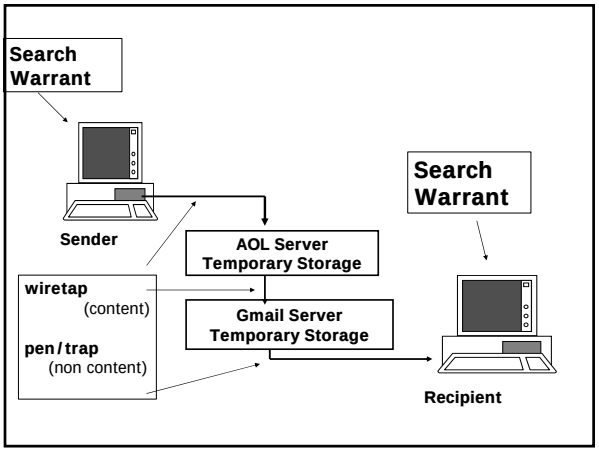
  Hoffa
- **vol. exposure to public eliminates F/A protection**

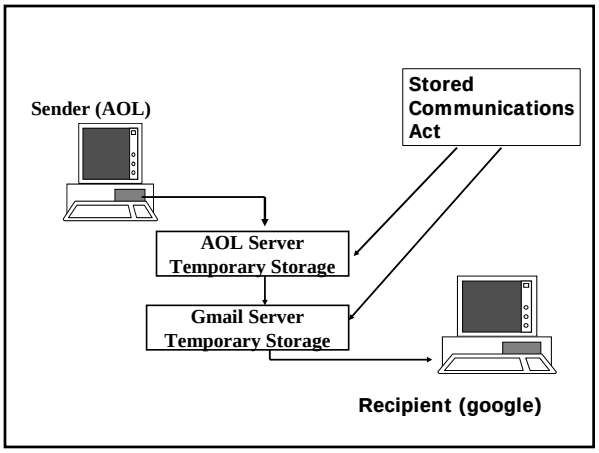
  Katz

21st century battleground !

assume risk / voluntary exposure ???







application of Fourth Amendment principles to --

1. Virtual worlds

2. cloud computing

3. web based data storage

4. email / data in transit

what are relevant considerations?

lower courts fairly uniform --

obtaining content --- No F/A protection

1. Email recovered from recipient

2. Internet chat rooms

3. Posting Info on a Website

doctrines:

- voluntary exposure
- assume risk

City of Ontario v. Quon, 130 S. Ct. 2619 (2010):
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?
3. Was search Reasonable ?

***See* memo on line for summary**

police pager policies

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

Quon: NO answers

- "case touches issues of far reaching significance"
- concern: "broad holding" on REP "might have implications for future cases that cannot be predicted"

Therefore:

1. assumed Quon / women had REP
2. search reasonable

dicta on REP analysis -- *possible* factors

- Duke's statements change in policy?
- did Duke have "fact or appearance" of authority to change / guarantee REP
- should public/ private employees be treated differently
- gov't had interests to review messages:
  - performance evaluations
  - litigation on lawfulness of police actions
  - comply w/ open records laws

- Rapid changes in communication
- many employers expect / tolerate personal use
- **employer policies "especially" when "clearly communicated"**
- some state statutes require employers to notify when monitoring electronic communications
- uncertain evolution of **workplace norms** / law's treatment

- Cell phone / text messaging pervasive -- hence:
  - one view:

    "essential means or necessary instruments for self-expression, even self-identification"

  - another view:

    due to ubiquity / affordability employees can buy own

Scalia, concurring

- Applicability discussion "unnecessary" & "exaggerated"
- rejects "implication" about electronic privacy that Ct should decide less –

  The-times-they-are-a-changin' is a feeble excuse for disregard of duty.

- **courts/ litigants likely to use dicta as "heavy-handed hint about how they should proceed"**

The Court's standard

"is (to put it mildly) unlikely to yield objective answers"

Sotomayor concurring in *U.S. v. Jones,* 132 S CT 945 (2012)

Privacy does not equal secrecy

- **reconsider 3rd party doctrine: "ill suited to the digital age"**
- **people reveal great deal of info to 3rd parties to carry out mundane tasks**
  - **phone numbers dialed / text to cellular providers**
  - **URLs visited**
  - **e-mail addresses to ISPs**
  - **books, groceries, and medications purchased online**

Sotomayor concurring

- **Doubts people accept warrantless disclosure to Gov't list of Web sites visited in last week, or month, or year**
- **Does not assume all info voluntarily disclosed to some member of public for limited purpose is, for that reason alone, disentitled to F/A protection**

Smiling Bob meets the 6th Circuit

Is email obtained from ISP protected by Fourth Amendment?

Warshak #1,

532 F.3d 521 (6th Cir. 2008) (en banc)

QUESTION not ripe:

privacy expectations

- **"may well shift over time"**
- **"shifts from internet-service agreement to internet-service agreement"**
- **requires knowledge about ever-evolving technologies**

variety of agreements

Service providers ....

- **will "not ... read or disclose subscribers' e-mail to anyone except authorized users"**
- **"will not intentionally monitor or disclose any private email message" but "reserves the right" to do so in some cases**
- **right "to pre-screen, refuse or move any Content that is available via the Service"**
- **e-mails will be provided to government on request**
- **other individuals will have access to email / can use information**
- **no REP in any communications**

U.S. v. Warshak (#2),
631 F.3d 266 (6th Cir. 2010)

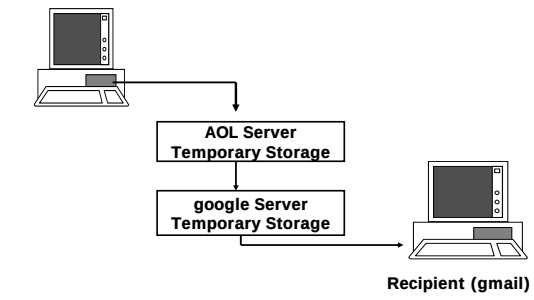
SCA subpoena on less than probable cause violates 4th Amend

- analogy to letters / phone calls
- ISP = post office / telephone company

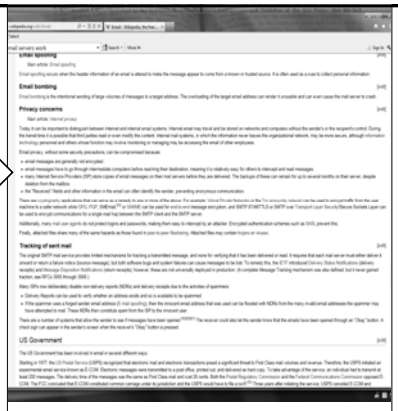
- **subscriber agreement: limited access only to protect ISP**

- **not holding: subscriber agreement will *never* be broad enough to snuff out REP .... if ISP intends to "audit, inspect, and monitor" emails, might be enough**

Where email can be read



wikipedia



solutions?

data in transit *or* stored

stored data

Compelling Content Production: warrants

Search Warrant: gets everything !

- ***may*** **always be needed when content sought**
- **safer course: Get warrant for *any* content**

The Fourth Amendment

Its History and Interpretation

Thomas K. Clancy

$70 on Amazon

ISBN-10: 1-59460-412-6
ISBN-13: 978-1-59460-412-6

www.cap-press.com/books/1795

Cyber Crime and Digital Evidence: Materials and Cases

- **LexisNexis (2011)**
- **ISBN: 9781422494080**

Power points other materials available at:

WWW. NCJRL.org

- **tclancy@olemiss.edu**