Fourth Amendment satisfaction

Evolving Issues: digital evidence

Thomas K. Clancy

Director

NATIONAL CENTER
FOR JUSTICE AND THE RULE OF LAW

University of Mississippi
School of Law

some evolving issues

warrant language related to

- **probable cause & broad seizures**
- **particularity of description of objects to be searched for and seized**
- **scope of permitted seizure**

Why do police {legitimately} want to seize / search computer?

1. ***it contains evidence***

   (ex) drug dealers' records

   (ex) who lives there, owns computer

2. ***it was used to commit the crime [instrument]***

   (ex) e Bay fraud (on-line auction house fraud)

   (ex) illegal trading of music, movies

   (ex) hacker's computer

   (ex) illegal Internet gambling business

3. *it's contraband, fruit of crime, criminally possessed*

contraband

* *child porn*
* *pirated software*
* *copyrighted materials*

fruits

**money from illegal transactions*

**computer bought with illegally obtained $*

criminally possessed

review of decisions to issue warrant: probable cause claims

Gov't:

merely establish search pursuant to warrant

Defendant Must Show:

1. no probable cause
2. no substantial basis for probable cause
3. good faith does not apply

No Probable Cause To Issue Warrant

***Only* Evidence Admissible at Hearing:**

"Four Corners"

1. **Affidavit submitted to magistrate who issued warrant.**

2. **Some states: oral testimony given by affiant to issuing magistrate that was *basis* for issuing warrant.**

"Substantial basis"

Proper question for motion court:

viewing affidavit as whole, *a substantial basis* for magistrate's determination that PC existed

Upton

* **deference afforded to issuing judge's determination**

* **PC *not* reviewed *de novo***

Good Faith Exception To Exclusion

***GENERAL RULE:* no exclusion**

exclusionary rule inapplicable to evidence obtained by officer acting in reasonable reliance on S/ warrant issued by detached & neutral magistrate, even if found NOT to be supported by PC

Leon

reasonable reliance:

*** question of law -- *de novo* review**

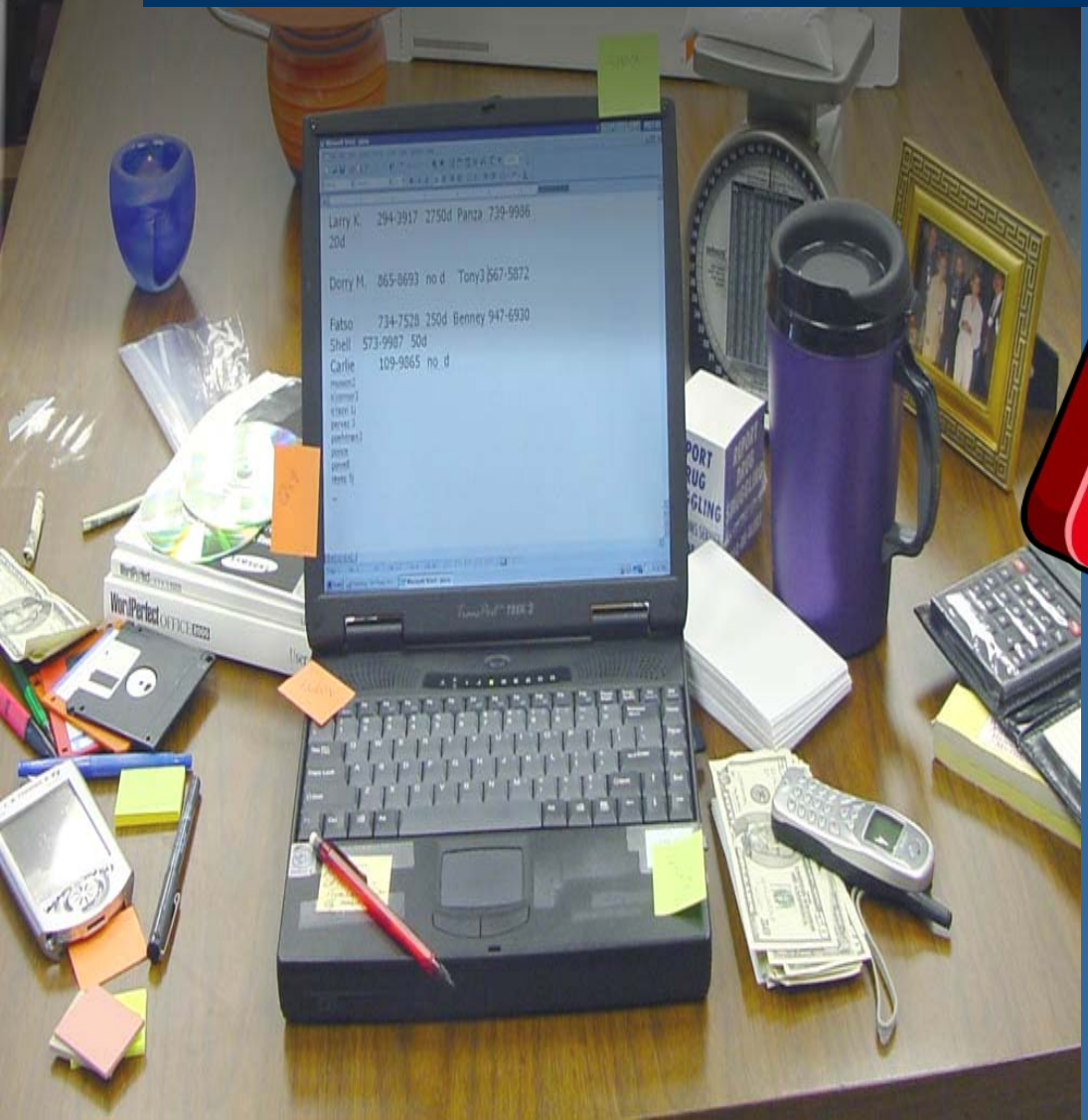
Establishing Probable Cause

Q#1: Why do police want to search the computer?

Q#2: What information supports that reason?

justification for broad seizures

the crime scene: what can be seized?



- laptop
- floppies
- manuals
- picture frame
- post it notes

establishing probable cause to search computer

Q#1: Why do police want to search computer?

**** it contains evidence***

(ex) drug dealers' records

(ex) who lives there, owns computer

(ex) communications over internet

**** it's an instrumentality of crime***

(ex) distribute child porn

**** it's contraband***

(ex) stolen property

Q#2: what information supports that reason?

sample affidavit includes --

1. **affiant's background and expertise [blank]**

2. **probable cause facts specific to case [blank]**

3. **facts about computers in general**

   * **role of computer in crime**
   * **seizing all equipment and off site search**

model: scope of seizure

Computer and Electronic Equipment, including the following:

a. Any and all information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer related equipment.

media includes network, servers, back-up tapes and diskettes, hard drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes and other media which are capable of storing magnetic coding.

b. Any and **all electronic devices** which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data.

devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives and other computer related devices.

c. Any and **all instruction or programs** stored in the form of electronic or magnetic media which are capable of being interpreted by a computer or related components.

The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware peripherals whether directly or indirectly via telephone lines, radio, or other means of transmission.

d. **Documents and other property** related to computers and their operation, including manuals, and any devices to access computers, such as **passwords** and **keys.**

ROLE OF THE COMPUTER – in general

Computer hardware, software and electronic files may be important to a criminal investigation in two distinct ways:

(1) may be contraband, evidence, instrumentalities, or fruits of crime

(2) may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

"In the instant case, the warrant application requests permission to search the described items because the affiant believes that the computer was involved in the crime as detailed above."

why need to seize all or most equipment
AND
search off site?

needs to be searched by qualified computer expert in lab because

1. Volume of evidence

*** millions of pages of data**

*** conceal evidence, including**

-- random order

-- deceptive file names

*** may have to examine all data**

-- sorting can take weeks

2. Technical Requirements

highly technical process -- need expert , controlled environment

no expert knows all systems -- cannot know needs before search

search is scientific procedure designed to:

* protect integrity of evidence
* recover "hidden," erased, compressed, encrypted, or password-protected files

computer evidence vulnerable to modification or destruction

*external sources
*destructive code imbedded in system ("booby trap"),

THEREFORE: must seize most / all of system, software, documentation, data security devices (including passwords) to accurately retrieve data

comprehensive data analysis

Searching computer systems require range of data analysis techniques

some cases -- targeted searches

others complicated because of

- **mislabeling**
- **hidden files**
- **encoding communications**
- **attempt to delete files**
- **other steps designed to frustrate searches**

MAY have to examine all electronic storage devices and areas

why seize documents?

"all documents and other property related to computers and their operation, including manuals, and any devices to access computers, such as passwords and keys"

why:

* how to run computer, software programs
* how to access data
* assist in establishing ownership and/or operator

* passwords often written in manuals, notebooks, post-it notes, etc.

"THEREFORE necessary to seize all written material that is in close proximity of the computer system(s) being seized"

model warrant seeks to justify very broad search:

- all manuals
- all notes, etc
- all hardware, including storage devices
- all documentation
- all software

Does it make a sufficient showing?

can police seize *all* computer equipment and storage media to search off site?

U.S. v. Hill, 459 F.3d 966 (9th Cir. 2006)

- must demonstrate *factually* need in each case

- must explain why cannot describe objects of search more specifically

"seize the haystack to find the needle"

but what's the remedy for overbroad seizure?

Fourth Amendment -- **particularity requirement**

Warrant must particularly describe ---

"place to be searched, and the persons or things to be seized."

Test:

does it enable officer to identify w/ *reasonable certainty* items that issuing magistrate has authorized to seize?

Garrison

Two varieties of Searches: Equipment; Data

questions to ask:

Are police seeking data or hardware?

How is object sought described in the warrant?

computer as stolen property

looking for specific property -- be as specific as possible

possibilities:

* brand name, model
* serial number
* identifying name tags

(ex) "First Page Beeper Services"

(on company's equipment)

* generic statement:

"and all other equipment belonging to ___ "

OK if part of list of specified items

generic search for Computer Equipment
-- instrumentality of crime

generic descriptions of items to be seized usually OK

Suffices to say ---

this is **not** the "special" approach

“computer equipment”

“equipment” …. [used in X crime]

[ex] warrant: "any and all computer software and hardware,

computer disks, disk drives

sufficiency of description: equipment

U.S. v. Herendon, 501 F.3d 683 (6th Cir. 2007)

- probation provision to check: **"computer and any software at any time for Internet capacity and activity"**
- can search all storage areas, including peripheral drives
- "computer" is **"commonly understood to include collection of components involved in computer's operation"**

State v. Stapleton, 924 So. 2d 453 (La. Ct. App. 2006)

Warrant provided authority to search computer for

"information concerning plans to build indoor marijuana cultivating devices"

During execution officer looked floppy disks

Scope violated?

"common sense scope of warrant" included floppy disks

State v. Hinahara, 166 P.3d 1129 (N.M. Ct. App. 2007)

Warrant authorized search for

.... computers, video tapes, computer diskettes, CDs, DVDs, photographs, and magazines containing child pornography

Police examined hard drive -- Scope violated?

common sense reading of affidavit ... reference to computers and computer disks sufficient to guide officers to seize hard drive

sufficiency of description: Data searches

majority view: Data in computer storage = document

warrants for “writings” or “records” include computer files

"documents in any form, including electronic and other formats, relating to the crime of _____ {specify crime}"

recent case:

U.S. v. Giberson, 527 F.3d 882 (9th Cir. 2008)

warrant to search for—

"records and documents" to show ownership of property, aliases, making false IDs, employment

execution --

saw computer, printer, documents near by evidencing producing false IDs

held -- seizure OK

warrant described items to be seized as particularly as could be expected given nature of the crime and evidence govt possessed at time it was issued

Commonwealth v. Huntington, 924 A.2d 1252 (Pa. Super. Ct. 2007)

warrant did not provide definitions of computer-related terms

- e-mail addresses
- screen names
- IP addresses
- Yahoo Groups
- cybertip
- IP tracker logs

trial court granted suppression -- lack of probable cause

affirm or reverse?:

terminology employed is sufficiently well-established that we cannot agree that it constitutes incomprehensible technical jargon