

Defending Cybercrime Cases: Search & Seizure Issues



CJ341 – Cyberlaw & Cybercrime Lecture #25

M. E. Kabay, PhD, CISSP-ISSMP
<mailto:mekabay@norwich.edu>
 V: 802.479.7937
 Assoc Prof Information Assurance
 School of Business & Management

P. R. Stephenson, PhD, CISM, CISSP, FICAF
<mailto:pstephen@norwich.edu>
 V: 802.498.4923
 Chair, Department of Computing
 School of Business & Management

Julie Tower-Pierce, Esq
<mailto:jtpit@hpit.net>
 Adjunct Prof Justice Studies
 School of Social Sciences

1

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Topics

- Intro
- Fourth Amendment
- Federal Statutes



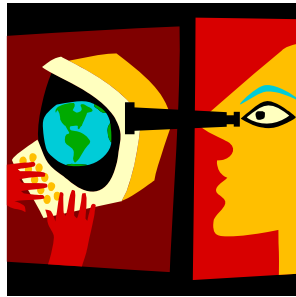
2

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Intro



- Technology + Computer Crime = Significant legal issues around privacy
- Concerns pertaining to:
 - Personal privacy
 - Intrusion into private lives
 - Surveillance



3

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Fourth Amendment Review



- Protection from unreasonable government search & seizure:

"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."

- Requires warrant for search by LEO or other government agent(s) [not owners] where individual has reasonable expectation of privacy
 - Warrant must be based on *probable cause*
 - Exceptions to warrant requirement may apply
 - ✓ E.g., plain view, consent, exigent circumstances



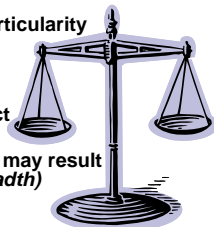
4

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Searching & Seizing Computers



- Fourth Amendment right is personal
 - Only claim expectation of privacy when one owns, possesses, or controls
 - E.g., 1992: *US v. Taylor*. Defendant lacked standing to challenge search of co-defendant's computer because no evidence of ownership or possessory interest presented
- Particularity requirement
 - Search warrant must describe with particularity place and items to be searched
 - Goal of 4th Amendment is to prevent widespread searches
 - ✓ Computer searches = balancing act
 - ✓ Broad search may be useful for evidence collection, but too broad may result in evidence suppression (*overbreadth*)



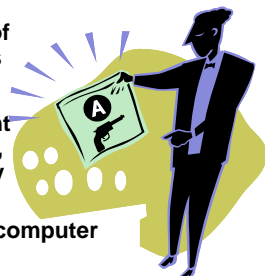
5

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Searching & Seizing Cont.



- **Suppression:** Defendant can move to suppress evidence if improperly obtained or where warrant requirements disregarded ("*Motion to Suppress*")
- **2001: *In re Grand Jury Subpoena Duces Tecum*.**
 - Court found subpoena for all computer disks overbroad because ...
 - ...no need to subpoena *all* of defendant's computer disks
- **Intermingled Document Rule:**
 - When irrelevant and relevant documents so intermingled, broader search warrant may be required (*US v. Tamura*)
 - Rule has been extended to computer searches

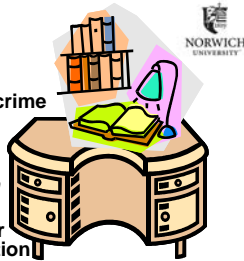


6

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

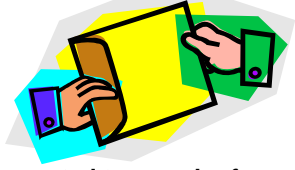
Warrant Exceptions: Plain View

- Warrantless seizure of evidence of a crime lawfully obtained if in plain view
- 1999: *US v. Carey*: no plain view exception where police opened computer files *not clearly specified in the warrant*
 - ❑ Police warrant specified search for files related to drug sales/distribution
 - ❑ Police couldn't find drug related files, but observed files titled with sexually suggestive names, and opened those files, which contained child pornography
 - ❑ Defendant convicted of possessing child pornography, appealed
 - ❑ Prosecution used "file cabinet" analogy
 - ❑ Court found no plain view exception because contents were seized, not just the files
 - ❑ *Images not in plain view*



Warrant Exceptions: Consent

- Can challenge consent
 - ❑ Was it given?
 - ❑ Scope of consent
 - ✓ Reasonable person standard
- *US v. Turner*: *defendant* consented to search of apartment for evidence of sexual assault.
 - ❑ Police viewed nude woman photo on computer and searched hard-drive without warrant and found child pornography
 - ❑ Applying the reasonable person standard, court concluded that *search was beyond scope of consent*



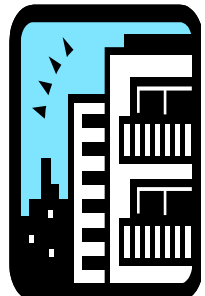
Consent (cont'd)

- Consent to *seize computer* does not necessarily = *consent to search*
- But see *US v. Al-Marri (2002)*
 - ❑ FBI seized laptop pursuant to consent of defendant, a computer science graduate student, and indicated that they wanted to bring it back to FBI offices to "take a look"
 - ❑ Defendant later asked for computer back at FBI offices, told "no" but didn't protest
 - ❑ Court found *defendant consented to search*



Warrant Exceptions: Authority to Grant Consent

- Defendant can challenge consent on grounds of *no authority* for consent
 - ❑ Third party (e.g., parent or roommate gives consent to search of computer)
 - ❑ Analysis turns on *access and control*
 - ✓ Does third party have joint access or control over computer?
- Limits to authority
 - ❑ E.g., co-user can't consent to search of *password-protected files* belonging to another user, but *can* give consent to search of the computer



Searches & Attorney-Client Materials

- Search of business computers sometimes leads to seizure of *privileged attorney-client material*
- "Taint procedures" used to minimize risk
 - ❑ Warrant to seize materials
 - ❑ Materials sorted based on potential existence of privilege
 - ❑ Potential privileged documents then sent to *independent attorney or judge*
- *US v. Lin Lyn Trading*: Yellow notepad containing privileged notes between lawyer and defendant seized (contained incriminating statements by defendant).
 - ❑ Found *unlawful seizure* and irreparable injury from government possession of notepad



Electronic Communications Privacy Act (ECPA)

- Interception of Electronic Communications
- Government can intercept electronic communications with judicial approval
 - ❑ Showing of probable cause
 - ❑ Consent
- ECPA allows *suppression of unlawfully intercepted wire or oral communications*
 - ❑ Does not automatically provide same for *electronic communications*
 - ❑ Defendant must move for suppression



Accessing Stored Electronic Communications



➤ Stored Wire and Electronic Communications Act

- Prohibits unauthorized access to stored electronic communications
- Gov't must follow specific procedures before accessing stored communications
 - ✓ E.g., obtaining warrant for *unopened* e-mail



13

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Obtaining Basic Subscriber Information



- U.S.A.P.A.T.R.I.O.T. Act expands gov't access
 - E.g., service provider can *voluntarily* provide info to gov't without recourse if reasonably believes emergency of death or serious injury
- Gov't can compel turn-over of *subscriber info* or electronic communication *transaction records* in connection with terrorism or intelligence activities
- Defendant can argue against disclosure
 - Unduly burdensome
 - Excessively voluminous
- More about U.S.A.P.A.T.R.I.O.T. in *Lecture 28*



14

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Privacy Protection Act



➤ PPA Restricts gov't from engaging in intrusive searches or seizures of materials of:

- Media
- Public Communications
- First Amendment activities
- Gov't must use *subpoenas* (distinguish from *warrants*)
 - No surprise searches permitted
 - No search of standalone computers
- Remedies
 - No suppression of evidence collected in violation of PPA
 - Civil damages only



15

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

DISCUSSION



16

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.