

CJ341 Class Notes

Search Warrants & Seizure of Electronic Evidence

CJ341 – Cyberlaw & Cybercrime Lecture #17

M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management



1

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Topics

- Identifying Physical Location of Electronic Evidence
 - ❑ ECPA Effects on Data Acquisition
 - ❑ Collaboration from Third-Party Record-Holders
- Which Computers?
- Legal Limits on Searches
 - ❑ Federal Constitutional Limits
 - ❑ State Constitutional Limits
 - ❑ Statutes



2

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Identifying Physical Location of Electronic Evidence

- General Principles
- ECPA Effects on Data Acquisition
 - ❑ Coverage
 - ❑ Disclosure to Government Agents
 - ❑ Contents of Electronic Communications
 - ❑ Violations of the ECPA
- Collaboration from Third-Party Record-Holders
 - ❑ Finding the Records
 - ❑ Evaluating Utility of Records
 - ❑ Authenticating Records
 - ❑ Obtaining Records
 - ❑ Contacting ISP & Serving Papers



3

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

General Principles

- *Katz v US (1967)*: SCOTUS held that *publicly disclosed* information is *not* constitutionally protected
 - ❑ Includes voluntarily transferred info in hands of third parties
 - ❑ Thus third-party repositories limited by statute, not 4th amendment
- Restrictions include laws protecting
 - ❑ Bank records
 - ❑ Cable TV & video rentals
 - ❑ E-mail & other electronic communications



4

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

ECPA Coverage



- 2000: Updated Wiretap law (18 USC §2510-22)
- 2004: Added Stored Electronic Communications Privacy Act (SECA, 18 USC §2701-11)
- Protects contents of e-communications in storage by *service*
- Prohibits provision of communications to government agencies without strict controls

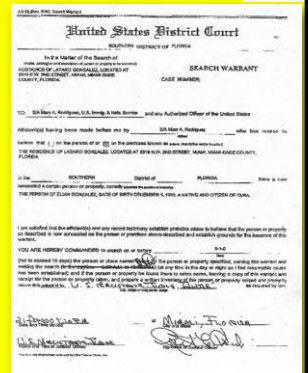


5

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Disclosure to Government Agents

- All records may be obtained through *warrant*
- Subscriber/customer records (identity, services) may also be obtained by *subpoena*
- Transaction history available through subpoena since U.S.A.P.A.T.R.I.O.T. Act passed
- E-mail may be retrieved by subpoena provided user given notice (up to 90-180 days delay)
- May use “§2703(d) court order” to access everything except unopened e-mail stored < 180 days



6

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

CJ341 Class Notes

Contents of Electronic Communications

- Agreement of *one* party in electronic communication suffices for legal disclosure
- Take that fact into account when you are writing e-mail
 - ❑ In general, when writing with employee userID, all e-mail must be considered equivalent to using company letterhead
 - ❑ All official e-mail may become evidence in a court of law
- *When writing informally using your own address, remember that everything on Internet is POTENTIALLY PERMANENT and may affect your future employment prospects*



7

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Violations of the ECPA

- Criminal liability
 - ❑ Up to 2 years in federal prison
- Civil liability
 - ❑ Damages & attorneys' fees
 - ❑ Government agent may be personally liable
- Suppression: NOT a remedy
- Good faith defense:
 - ❑ Government agent may
 - ❑ Rely on good faith application of warrant or subpoena
 - ❑ As absolute defense against civil or criminal charges stemming from actions



8

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Evaluating Utility of Records

- Records may not be available
 - ❑ Typically 30-60 day retention of log records
 - ❑ Dynamic IP addresses may make identification difficult for older evidence
- Some records may originate in public computers that are effectively anonymous
 - ❑ Business services (e.g., Kinko's)
 - ❑ Libraries, Internet cafés
 - ❑ Wireless services
 - ❑ Hijacked services
 - ❑ Anonymizers

But look for video camera recordings



9

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Authenticating Records

- Spoofing may disguise origin
 - ❑ Naïve users alter originating address
 - ❑ But headers show real IP addresses
- More sophisticated criminals add faked header lines
 - ❑ Must always analyze entire header
 - ❑ SamSpade does this (discussed in lecture 16)
- Open spam relay a danger
 - ❑ Logon to unprotected SMTP server
 - ❑ Send mail from someone else's system



10

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Obtaining Records

- Typically obtain search warrant
 - ❑ Better than subpoena
 - ❑ Can obtain any records at all
 - ❑ Avoids problem of more restrictive state laws that require warrant
- So why not use a warrant?
 - ❑ Might not have probable cause
 - ❑ Difficulty getting warrant across state lines



11

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Contacting ISP & Serving Papers

- Call ISP to be sure they have records you need
 - ❑ Discuss IP addresses with technical staff
 - ❑ Identify possible errors of analysis
 - ❑ Find out if there have been mergers or acquisitions
 - ❑ Identify possible IP sub-blocks owned/used by other entities
- Ask if ISP will accept warrant by fax
- Explain exactly what you need



12

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

CJ341 Class Notes

Search Warrants

- Which Computers?
- Legal Limits on Searches
 - ❑ Federal Constitutional Limits
 - ❑ State Constitutional Limits
 - ❑ Statutes



13

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

Which Computers?

- Goal of tracing electronic communications:
 - ❑ Locate computer at origin of evidence of crime
 - ❑ Link to specific person
- Computers that may be involved
 - ❑ Victims' computers may be searched without warrant with permission
 - ❑ Publishers' computers not restricted if publisher is the victim
 - ❑ ECPA does not apply to suspects' computers

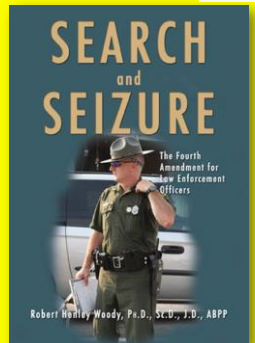


14

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

Federal Constitutional Limits

- Fourth Amendment
 - ❑ Reasonable expectation of privacy
 - ❑ Government action
- Legal Warrant
 - ❑ Probable cause
 - ❑ Neutral/detached magistrate
 - ❑ Reasonably precise
- Rules for Executing Warrant



<http://tinyurl.com/4jmcaz>

15

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

The Fourth Amendment Text

*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**.*

Bold emphasis added

16

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

4th Amendment Issues (1)

Reasonable expectation of privacy (EOP)

- Subjective expectation
 - ❑ Computer *in home* has *higher* EOP
 - ❑ Shared computer has *lower* EOP
 - ❑ Employer's computer: depends –
 - ✓ Policy?
 - ✓ Awareness?
 - ✓ Enforcement?
- Social acceptance or expectation of search



17

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

4th Amendment Issues (2)

- Government action
 - ❑ Searches by state law enforcement may transfer results to federal agencies
 - ✓ But federal authorities must not have been involved in a way that would require *suppression of evidence*
- Private citizens
 - ❑ Constitution does not affect search by private citizen *not acting as an agent of law enforcement*
 - ❑ Thus evidence usually admissible in court



18

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Tower-Pence & P. R. Stephenson. All rights reserved.

CJ341 Class Notes

Legal Warrant

- Probable cause
 - ❑ Evidence of a crime
 - ❑ Likelihood that evidence will be found in location to be searched
 - ✓ How do you know suspect used computer in home? Could have been elsewhere
 - ✓ May need *circumstantial evidence* such as time stamps, stakeout
- Neutral/detached magistrate
 - ❑ Who has authority for warrant location
 - ❑ Watch out for cross-state jurisdiction
- Reasonably precise
 - ❑ General description may lead to suppression
 - ❑ Best to mention computers & media *explicitly*



19

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

Rules for Executing Warrant (1)

- Knock and announce: identify as LEOs & explain purpose in entering premises
- Take items in plain view
 - ❑ But contraband and tools for crime may also be seized if they are visible and obviously incriminating



20

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

Rules for Executing Warrant (2)

- Good faith
 - ❑ Evidence seized under faulty warrant may be suppressed
 - ❑ But generally LEOs not prosecuted if acting under good faith in legality of (later overturned) warrant
- Remove computers for analysis off-site
- Prompt execution
 - ❑ Don't let evidence evaporate
 - ❑ Cannot hold warrant in abeyance indefinitely



21

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

State Constitutional Limits

- Some states more restrictive than federal rules
- Some do not allow good-faith exception to requirement for valid warrant
- Some may protect vehicles (and by implication portable computers) more than federal courts

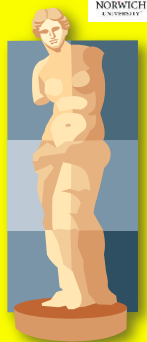


22

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

Statutes

- ECPA (as discussed above)
- *Zurcher v. Stanford Daily*
 - ❑ LEOs had warrant to search student newspaper's computer for pictures of political demonstration
 - ❑ SCOTUS ruled that 1st Amendment issues did not further limit warranted searches



This is not a statute.



23

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

Statutes: PPA

- PPA passed to further restrict warrants
 - ❑ Privacy Protection Act (42 USC §2000aa)
 - ❑ Passed in 2000
 - ❑ Any material intended for publication or broadcasting requires a subpoena
 - ❑ Exceptions
 - ✓ Contraband, fruits or tools for crime
 - ✓ Preventing imminent death or injury
 - ✓ Material held by target of investigation
 - ✓ Child pornography



And neither is this.



24

Copyright© 2013 M. E. Kobay, D. J. Byrne, J. Town-Pierce & P. R. Stephenson. All rights reserved.

CJ341 Class Notes

PPA & Steve Jackson Games

- March 1990: Secret Service raided Steve Jackson Games
 - ❑ Looking for info about BellSouth's emergency service
 - ❑ Had been posted on BBS
 - ❑ Seized entire computer for BBS
 - ❑ Held for months
 - ❑ Severely damaged company
- SJG sued under PPA & ECPA
 - ❑ Won trial
 - ❑ Awarded damages \$51K
 - ❑ Attorneys' fees \$250K
- Irony: BellSouth info was actually public & available for sale from company



25

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

**Now go and
study**

26

Copyright© 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.