Fourth Amendment presentation

1. basic structure

2. acquiring digital evidence

THOMAS K. CLANCY
2022

today's materials

1. **power point slides**

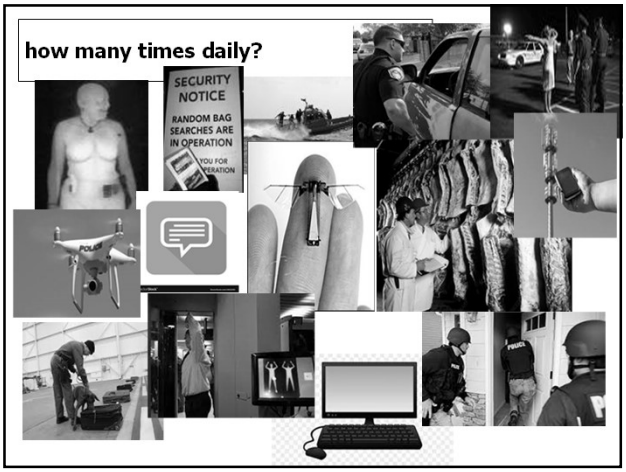
2. **Chapter 1, includes**

   - **4th Amend overview**
   - **section 1.5 – overview of computer searches**

     (does not include *Carpenter*)

3. **Chapter 12, section 12.2.2 – requirements for warrants to issue, including computer**

how many times daily?



Amendment IV

Reasonableness clause:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,

Warrant clause:

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.

Warrant clause:

does only one thing -- 3 requirements

no Warrants shall issue, but upon

- **probable cause,**
- **supported by Oath or affirmation, and**
- **particularly describing place to be searched, and persons or things to be seized**

Reasonableness clause:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,

- **fundamental right / promise**
- **limits on protection**
  - **only 4 objects protected**
  - **only a quality in each object: "secure"**
  - **only against two types of govt activity**
  - **only against "unreasonable"**

Three questions in each case

Ch. 1 for overview

1. **Does the 4th Apply?**
   - A. **Gov't activity: "Search" or "Seizure"**
   - B. **Protected interest: "secure" in 4 objects**
2. **Is it Satisfied?**
   - **"Reasonable"**
   - **Warrant Clause requirements**

[3. Remedies?]

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?

two sides of all Applicability issues:

1. **gov't side --**
   - **"Search" Defined**
   - **"Seizure" Defined**

2. **defendant side --**
   - **What Amendment Protects**
     - **each person, house, papers, effects**
     - **"Security" interest in each**
   - **Standing: Who is Protected**

two sided nature of applicability question

- **physical manipulation of bus passenger's carry-on luggage = gov't "search"**
- **But did it invade protected interest?**
  - **bag = effect**
  - **right to privacy invaded?**

Bond v. United States, 529 U.S. 334 (2000)

Satisfaction ?

Reasonableness clause

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,

Warrant clause

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.

Two aspects to question :

What is Reasonable?

1. **justification for initial intrusion**
2. **regulates scope of intrusion**

not discussed today ....

exclusionary rule

not **a constitutional right –**

sole basis:

deterrence of future police misconduct

Puerto Rico Constitution
Art. II section 10

- **The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated.**
- **Wire-tapping is prohibited.**
- **No warrant for arrest or search and seizure shall issue except by judicial authority and only upon probable cause supported by oath or affirmation, and particularly describing the place to be searched and the persons to be arrested or the things to be seized.**
- **Evidence obtained in violation of this section shall be inadmissible in the courts.**

Govt acquisition of Digital evidence

Does the 4th Apply ?

part A: need gov't activity:
"**Search**" or "**Seizure**"
(assumed today)

part B: that activity must intrude upon a
protected interest

digital evidence searches

4th Amendment Applicability:

- **Reasonable Expectations of Privacy defines protected interest in data**
- **Where evidence located is fundamental consideration**

Applicability:
reasonable expectation of privacy test

1. person exhibits **actual, subjective expectation of privacy**
2. society recognizes that expectation as
Justified / Reasonable / Legitimate

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

- If either prong missing, no protected interest

expansive views of digital privacy interests in recent cases

- **Riley v. Ca, 134 S. Ct. 2473 (2013)**
  changes search incident to arrest rule for digital devices – get a warrant!

- **Carpenter v. US, 138 S. Ct. 2206 (2018)**
  CSLI – need warrant to obtain from provider

  - **no "single rubric" to find REP**

traditional limitations on privacy still important for digital evidence

- **voluntary exposure / assumption of risk**
- **third party doctrine**
- **measuring REP generally**

Where data located is fundamental consideration

Do you have REP in data on --

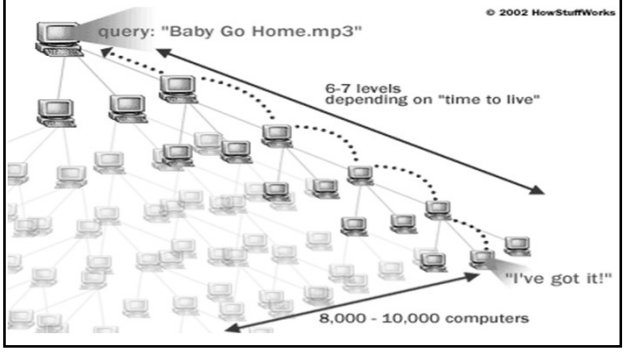
1. **own phone ?**
2. **phone of recipient ?**
3. **along the way:**
   – data w/service provider ?

part #1:
your own device ...

- Privacy not ownership is protected
  - case specific inquiry
- can loose it by failing to exclude others
  - info on screen
  - data in computer

Peer-to-Peer (P2P) Networks

file-sharing technology creates virtual networks



no REP in P2P

putting files in shared folder on own device ... " is like saying that he did not know enough to close his drapes "

U.S. v. Ganoe,
538 F.3d 1117 (9th Cir. 2008)

- case law is uniform

part #2: the recipient

sender has <u>no</u> REP in text message on recipient's cell phone

- **delivery created record of communication beyond control of sender**

Com. v. Delgado-Rivera,
168 NE3d 1083 (Mass. 2021) (collects cases)

- **post-Carpenter view – unanimous**

part #3: along the way (info with providers)

In 2017 –

- **130,000+ requests by law enforcement for digital evidence to just six tech companies**
  - **Google, Facebook, Microsoft, Twitter, Yahoo, Apple**

communicates with provider

information held by third parties

Traditional rule:

no standing to challenge disclosure of information held by third party

U.S. v. Miller, 425 U.S. 435 (1976)
(bank records)

Rationale:

Risk Analysis -- Voluntary Exposure

pen registers -- records numbers dialed by telephone

Smith v. MD, 442 US 735 (1979)

Two fundamental principles:

- **content vs. non-content distinction**
  - **#s NOT content**
  - **4th protects only content**
- **no REP in #s dialed**
  - **voluntarily conveyed info to 3rd party**
  - **assumed risk of disclosure**

Based on *Smith*, must distinguish between types of information gov't is seeking

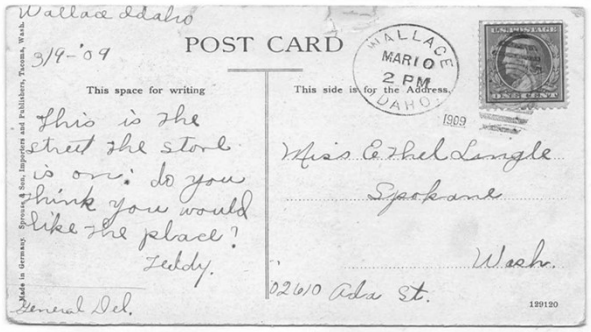
content: (protected)

- **communication itself**

non-content: (not protected)

- **dialing / addressing information**

protected?



pre & post Carpenter

Non-CONTENT = not protected

- **U.S. v. Forrester,** 512 F.3d 500 (9th Cir. 2008)
  - to/from email addresses
  - IP addresses of websites visited
  - total volume of info sent/received
- **U.S. v. Hood,** 920 F.3d 87 (1st. Cir. 2019)
  - subscriber info

social media warrant example

- shooting of Ellen
- goal: proving Joe was shooter
- Joe communicated via Instagram with Ellen on several occasions using his cell phone

what Instagram warrant sought

1. basic subscriber records: name; acct creation date; email address; sign up IP address
2. connection logs for account
3. list of accts user is "following"
4. list of accts "following" user

All are non-content

statutes created hierarchy of privacy protections after *Smith*

Congress enacted some statutory regulation of computer network investigations:

- **Stored Communications Act**
- **Wiretap Act**
- **Pen Register / Trap and Trace**

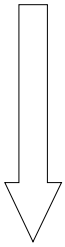
➢ **regulates non-content and content**

statutes create crimes for violation

- **ECPA rules apply to all gov't actors**
- **explains why simple subpoenas not used for most non-content**
- **explains references to federal statutes and details of facts in requests for court orders**

Compelled Production: 5 levels of process for stored data from some providers

- **Subpoenas**
- **Subpoenas *with notice***
- **"d" orders [§ 2703(d)]**
- **"d" orders *w/notice***
- **Search warrants**



more process = more info

"d" orders [18 USC § 2703(d)]

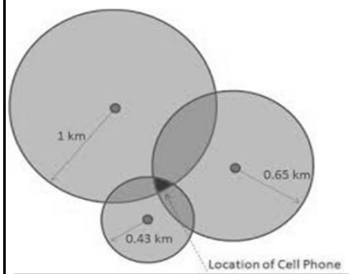
- used in *Carpenter*
- used in Google "Geofence Warrants"

"d" order requires:

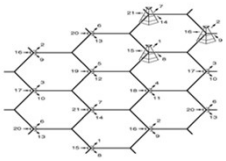
- specific and articulable facts that info sought is relevant & material to ongoing criminal investigation

---

obtaining information from cell phone providers



triangulation of 3 nearest towers



comparing signal strengths

- delays in receiving
- angles of receiving

Carpenter

co-conspirator confessed & gave cell phone to FBI showing Carpenter's #

- cell site location info (CSLI) obtained showing DEF near robberies
  - 127 days of his movements (MetroPCS)
  - 7 days requested, 2 days obtained (Sprint)

"It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."

scope of Carpenter REP holding

- **CSLI is "comprehensive chronicle of user's past movements"**
- **"near perfect surveillance" like ankle monitor**
- **like longer term GPS monitoring in *Jones***
- **case not about "person's movements at a particular time"**

Carpenter declines to speak about --

- **real time CSLI**
- **tower dumps**
- **conventional surveillance such as security cameras**
- **business records that incidentally reveal location**

third party doctrine still applies to:

- **telephone numbers**
- **bank records**

BUT not to CSLI:

- **qualitatively different category**
- **are novel circumstances**
- **"narrow decision" given "unique nature" of CSLI**
- **not truly shared – all phones generate CSLI**

basis of third party doctrine

dissents – flows directly from text

- **info not "yours"**
- **it's company's info**

Carpenter dissents:

Thomas – Katz is failure

- **"no plausible foundation" in text (citing Scalia)**
- **"The *Katz* test confuses the reasons for exercising the protected right with the right itself. A purpose of exercising one's Fourth Amendment rights might be the desire for privacy, but the individual's motivation is not the right protected." (citing Clancy)**

post-*Carpenter* questions

- **Is location info "content" or third category ?**
- **Does *Carpenter* create multifactor "qualitative" difference framework for data held by third parties?**

Post-*Carpenter* developments

Subscriber information = non content

NO REP in subscriber info, such as IP address

U.S. v. Hood,
920 F.3d 87 (1st. Cir. 2019)

(ex) pinging cell phones

- **less than 5 pings over 3 hours** – not search because not long term surveillance
  Sims v. State,
  569 S.W.3d 634 (Tex. Crim. App. 2019)

- **one ping** is search under MASS constitution
  Com. v. Almonor,
  120 N.E.3d 1183 (Mass. 2019)

- **not tracking devices** under Carpenter
  U.S. v. Ackies, 918 F.3d 190 (1st Cir. 2019)

emails with provider

- Kennedy in dissent in *Carpenter* observed:

  "modern-day equivalents" of "papers" or "effects" and protected even if held by third party

- **majority agreed with Kennedy**

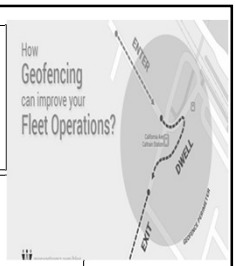
social media "content" after *Carpenter*

REP trends seem to be …

- **public post – no REP**
- **private posts only to "friends":**
  - **– acct holder has REP in content**
  - **-- gov't needs warrant**
- **undercover agent becomes "friend" – can view post w/o implicating Fourth Amendment**
- **"friend" shows police post – 3rd party doctrine applies**

Geo-fencing

virtual perimeter for real-world geographic area



- **Targeted marketing**
- **parents tracking children**
- **employers to locate employees**
- **political campaign events**

Propellant Media

Geofencing Marketing (Location Based Advertising) - Propl

GEO-FENCE "warrants" by Google

map

typically issued pursuant to 18 USC 2703(d)

date & time

location coordinates

Date & Time Period (including timezone):
July 2, 2015 at 10:15 a.m. through July 2, 2015 at 11:30 a.m. Central Time Zone.

Target Location:
Geographical area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:

Point 1: 33.441261°, -94.035497°
Point 2: 33.441245°, -94.033217°
Point 3: 33.439851°, -94.035537°
Point 4: 33.439833°, -94.033234°

Please see the **Target Location Reference Image 1** below.

three step process

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Google shall provide responsive data (as described in Attachment A) pursuant to the following process:

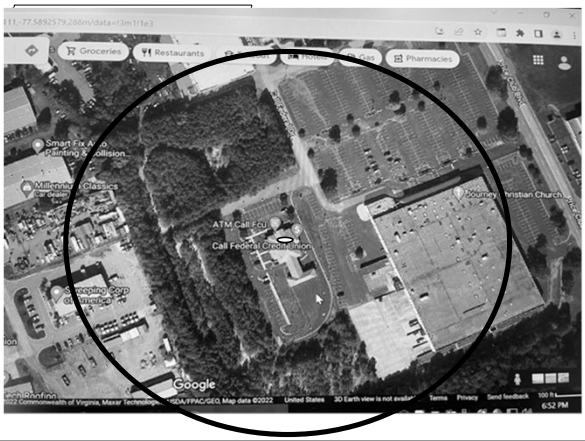
1. Google shall query location history data based on the Initial Search Parameters (as described in Attachment A).
2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").
3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the Target Location, were not within the Target Location for a long enough period of time, were moving through the Target Location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.
4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google Provide identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each identified device ID.

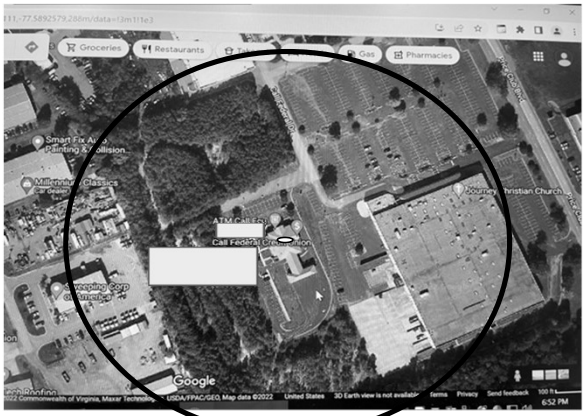
#1 anonymized data

#2 law enforcement narrows

#3 follow-up request

This is really a subpoena -- NOT a warrant





geofence analysis

- **to issue, even if "subpoena," must comply with particularity requirement**

at motion to suppress:

- **is one time GPS location enough to give individual REP in data?**
  - **if YES, need warrant**
  - **if NO, DEF has no standing at motion**

- **Geofence "warrants" have multiple problems**
  - **based on less than probable cause**
  - **scope -- particularity requirement**
  - **three bites of "warrant" to search**
  - **private parties do not get to negotiate scope**

geofence analysis –if a "warrant"

- **Geofence "warrants" have multiple problems**
  - **based on less than probable cause**
  - **scope -- particularity requirement**
  - **three bites of "warrant" to search**
  - **private parties do not get to negotiate scope**
  - **does defendant have standing to challenge scope as to other people?**

Phone Apps

Washington Post article spring 2019 by G. Fowler

5400+ tracking notices sent by apps on his cell phone in one week to marketing companies, other 3rd parties

- **YELP sent notice every 5 minutes**
- **What they were sending**
  - **location info, GPS coordinates**
  - **IP address, info about phone (serial #, model, etc)**
  - **other personal ID information**

Emerging issue: police buying APP location info

- **Apps collect location info -- advertising IDs have "unique numbers assigned to each device"**
- **APPs sell "anonymized" info to broker and Fog Data Science obtains and then creates "pattern of life" from data**
- **police buy data and exploit to find suspect by studying patterns of behavior**

See **Electronic Frontier Foundation for more**

Question#2: 4th Amendment satisfied?

SCT adopts warrant-based approach for digital evidence

- **search incident arrest: can seize device but to search ...**

  "Get a warrant"

  Riley

- **CSLI – need warrant to obtain from provider**

  Carpenter

most common DIGITIAL searches going forward

- **get a warrant !**
- **consent**
- **exigent circumstances**

Warrants for digital evidence:

split in lower courts on what needs to be in warrant

- **does warrant have to specifically ask to search a digital device for the evidence sought? (drafting issue)**
- **does warrant have to authorize manner in which device is analyzed? (execution issue)**

- **the problem is plain view**

drafting issue

- **majority: simply identify items sought**
  - **no principled distinction between digital & paper records**
- **minority: drafting must specify that digital device is to be searched**
  - **Digital fundamentally different than writings**

E.g., U.S. v. Payton, 573 F.3d 859 (9th Cir. 2008)

Warrant Clause issue

What should be in the warrant for digital evidence ?

- ***see*** **treatise sec. 12.2.2. (in materials)**

Warrant clause:

. . . 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.

non –digital world

US Supreme Court

- **rejects view: warrants must specify manner of execution**
- **"manner in which a warrant is executed is subject to later judicial review as to its reasonableness."**

U.S. v. Grubbs, 547 US 90 (2006)
Dalia v. U.S., 441 U.S. 238 (1979)

most courts -- reject preauthorization in warrant for search protocols

U.S. v. Galpin,
720 F.3d 436 (2d Cir. 2013)

- **search protocols not required**
- **look instead to actual search methods used**

special approach – a few courts

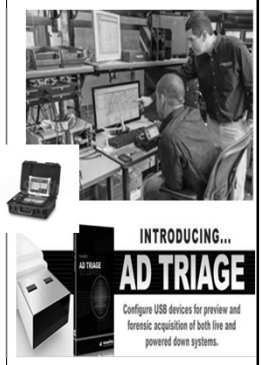
prior approval of search execution in warrant application

- **technology based or legal limitations in warrant itself**
- **examples:**
  - **word searches**
  - **date limitations**
  - **types of files**

forensic analysis: mobile and back at lab

How to regulate scope of search (exam)?

- **majority – search must be "reasonable"**
- **"special approach" -- unique limits for data exams**

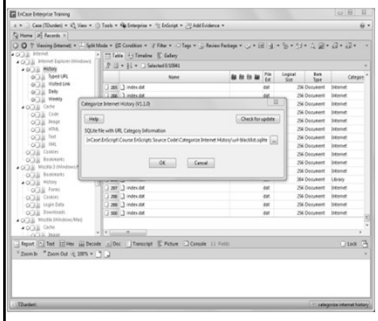


"Reasonableness" approach example -- execution unreasonable

U.S. v. Schingloff,
901 F.Supp.2d 1101 (C.D. Ill. 2012)

- **warrant for passport fraud**
- **FTK forensic search settings included looking for Child Pornography**
- **chose to search for CP but not authorized by warrant – suppression granted**

EnCase – forensic tools by Guidance Software
(acquired by OpenText)



www.youtube.com/watch?v=NYuhlyY2MRU

(18 minute youtube demo)

extended discussion in ---

- **Clancy, The Fourth Amendment: Its History and Interpretation**
  (3rd edition 2017)
  - **you have chapter 1, and sec.12.2.2.**
- **Clancy, Cyber Crime and Digital Evidence**
  (4th edition 2022 -- soon)

cap-press.com to order

Thomas K. Clancy

662-832-5244

clancy.thomas.k@gmail.com