

How the Constitution Protects your Cell Phone and Laptop Encryption Key

Abraham Kang, JD Lincoln Law School of San Jose
Principal Security Researcher
HP Fortify

Security in
knowledge





Disclaimer

- ▶ This is not legal advice.
- ▶ This is an academic analysis of the legal issues surrounding cell phones, passwords/encryption keys, and GPS logs.
- ▶ If you need legal advice please seek council in a licensed attorney.



Reasons Why I Love America

- ▶ Opportunity
- ▶ Freedom
- ▶ The Constitution
- ▶ So many other things but I don't have time to list them all...



Goals

- ▶ Understand how the 4th Amendment applies to searches of your cell phone and its GPS data
- ▶ Understand how the 5th Amendment applies to compelled disclosure of passwords and encryption keys

4th Amendment

- ▶ 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.
- ▶ Protects against unreasonable searches and seizures.



Reasonable Suspicion vs. Probable Cause

- ▶ Professor Joe Kennedy of University of North Carolina Law School gave a great analogy:
- ▶ Reasonable Suspicion
 - ▶ Poop
- ▶ Probable Cause
 - ▶ Steaming Poop

4th Amendment Analysis

- ▶ State Action
- ▶ Was there a search?
 - ▶ REOP in place searched
 - ▶ Subjective Expectation of Privacy (SEOP)
 - ▶ Society is willing to acknowledge that EOP as reasonable
 - ▶ Closed containers usually have REOP (must physically contain)
 - ▶ No REOP when data given to 3rd party or public (untrusted ear, iCloud)
- ▶ Does Plaintiff have Standing to sue?
 - ▶ Interest in item seized or place searched
- ▶ If there was a search was there a warrant based on P/C procured by a neutral and detached magistrate.
 - ▶ Pat downs are not searches (Terry v. Ohio)

Exceptions to Searches Requiring Warrants

- ▶ Search Incident to Lawful Arrest(-People v. +Nattoli— Akimbo, +US v. Park no safety or evidence concerns)*
 - ▶ Officer safety and preservation of evidence (search within wingspan)
 - ▶ You are arrested when:
 - ▶ By force or fear and your will to leave is over come
- ▶ Automobile Search Exception*
 - ▶ Car is searchable if officer has P/C (reasonable belief that person pulled over has **committed a crime, like DWI in Diaz**, evidence of the crime exists in the car) and car is mobile
- ▶ Border Searches*
 - ▶ Lesser standard than probable cause to search (In re Boucher)
- ▶ Exigent circumstance (Pursuit, Remote wipe irrecoverable)

* allows search of **closed containers if officer believes evidence may be found in them (US v. Finley -- Phones == container, US v. Park – Phone != container)**

— Exceptions to Searches Requiring Warrants (Continued)

- ▶ Plain View Doctrine (Arizona v. Hicks – Stereo)
 - ▶ Evidence has to be seen, smelled, or heard
 - ▶ Lawful vantage point
 - ▶ Plain view
 - ▶ Immediately apparent probable cause that evidence is fruit, instrumentality, or contraband of crime
 - ▶ Consent*
- ▶ Voluntary, Intelligent and Knowing
- ▶ Michigan Police
- ▶ Inventory Search*- ▶ Protect against vandalism and disputes about property
- ▶ Evanescent Evidence* – easily destroyed



— Fruit of the Poisonous Tree Doctrine

- ▶ If there was a “search” without a warrant and none of the exceptions applies then the evidence must be suppressed as “fruit of” an illegal search.



— Patch Work Court Decisions related to Cell Phone Searches

- ▶ Warrantless cellphone searches ARE constitutional
 - ▶ U.S. v. Diaz (SILA – of person & belongings, preservation of evidence)
 - ▶ U.S. v. Finley (Phone is part of person and container)
- ▶ Warrantless cellphone searches are NOT constitutional
 - ▶ Ohio v. Smith (Not container under Belton, holds large volume of data – NOT SILA because no safety or exigent circumstances)
 - ▶ California v. Park (NOT SILA -- Cell phone is not container and no safety or evidence concerns)

— Patch Work Court Decisions Related to Cell Phone GPS Logs and GPS tracking

- ▶ Warrantless Provider GPS log searches ARE constitutional
 - ▶ US v. Miller (Bank Transactional Records)*
 - ▶ Smith v. Maryland (Dialed cell phone numbers)*
- ▶ Warrantless Provider GPS log searches are NOT constitutional
 - ▶ Southern District of Texas
- ▶ Warrantless GPS tracking devices are NOT constitutional
 - ▶ US v. Jones

* Cases used to support warrantless access to cell phone tower logs

Cell Tower Logs (US v. Jones amended)

- ▶ Pinpoint location detail is not necessary to make inferences
 - ▶ What type of bars you visit
 - ▶ Which interns you are visiting and when
 - ▶ Which gentlemen's clubs you like to visit
- ▶ Equivalent to General Warrants that Founding Fathers were trying to prohibit
- ▶ Gov't supporting cases are OFF point
 - ▶ Not **voluntarily** transferring information to 3rd party (but Agent)
- ▶ Virtual Device Placement through Implied Agency
- ▶ Possible Solution: Hash historical data with secret key but keep current location unencrypted

5th Amendment

- ▶ No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; **nor shall be compelled in any criminal case to be a witness against himself**, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

5th Amendment Boiled Down

- ▶ **Compelled against the accused**
- ▶ Criminal Case
- ▶ To be **Witness** against Himself
- ▶ Personal
 - ▶ Cannot stop corporation or 3rd person from disclosing evidence related to an individual
- ▶ Limited to “Testimonial” evidence
 - ▶ Physical evidence is NOT protected under 5th (Schmerber)
- ▶ Incriminating (except when immunity).
 - ▶ Substantial and real threat

— Testimonial Evidence

- ▶ “Communications”
- ▶ But not compulsion which makes a suspect the source of real or physical evidence.
 - ▶ Blood samples
 - ▶ Line ups
 - ▶ Voice sample
 - ▶ Handwriting sample
- ▶ Revealing content of one’s mind
- ▶ Makes factual assertions or discloses information

Foregone Conclusion Doctrine

- ▶ When the fact of existence, authentication, or possession of produced evidence by the accused is a foregone conclusion (already known)
- ▶ Adds little or nothing to government's sum total of information
- ▶ Fisher case

Hubbell Case

- ▶ What if you are compelled to disclose the existence of incriminating documents that the government is not able to describe with reasonable particularity?
- ▶ Immunity?
- ▶ Make use of content of accused mind to identify, organize, and assemble compelled documents. (So Testimonial)
- ▶ But Gov. doesn't have to identify "every scrap of paper" it is requesting (Ponds)



5th Amendment Encryption Password Cases

- ▶ Is it Testimonial?
 - ▶ Key or Combination (Doe II)
- ▶ Who does the laptop belong to and where does the identified data reside?
 - ▶ Foregone Conclusion (In re Boucher and US v. Fricosu)
 - ▶ Communicates information which may lead to incriminating evidence (US v. THOMAS J. KIRSCHNER and US v. Doe III)
- ▶ Can the government identify the incriminating documents with reasonable particularity
 - ▶ Which documents do you want (Hubble)

Questions & Call for Action

