DR. SARAH ABRAHAM

CS349

PRIVACY FROM GOVERNMENT

WHAT SHOULD THE GOVERNMENT KNOW ABOUT YOU?

- What should the government know?
- What is it allowed to collect from third parties?
- How does encryption fit into this?

CASE STUDY: SAN BERNARDINO ATTACK

- In December 2015, married couple, Syed Rizwan Farook and Tashfeen Malik, opened fire on a holiday party at the Inland Regional Center in San Bernardino
  - 14 people killed, 22 injured
- Both attackers killed by police
- Arsenal of ammunition and pipebombs in their home
- FBI received warrant to access to Farook's work iPhone (they destroyed their personal phones)

THE PROBLEM?

- Farook's iPhone ran iOS9 (recently released at the time)
- After 10 incorrect attempts at guessing the PIN, the AES (Advanced Encryption Standard) key would be erased
- All encrypted data would be rendered inaccessible

THE OTHER PROBLEM?

- Someone had reset the iPhone's password to Farook's iCloud account 24 hours after the shooting
  - iCloud password was now wrong on iPhone and it couldn't back up data until phone accessed directly
- Not possible to subpoena Apple for access to data

APPLE VS FBI

- In February 2016, the FBI requested Apple to create software that would bypass the auto-erase feature and allow unlimited attempts to try PIN
- Apple refused
- FBI received a court order mandating Apple create software for FBI
  - Order issued under All Writs Act of 1789

ALL WRITS ACT OF 1789

- Law signed by President George Washington
- All Writs Act gives federal judges the power to issue orders compelling people to do things within limits of the law
- Broad law that can still be invoked despite changes in technology
- Writs once common but now only used in extreme cases

OUTCOME

- In March 2016, FBI paid ~$900k to have a third-party company crack the iPhone
- Case is dropped
- Averted courtroom case that would have established precedent relating All Writs Act in relation to encryption
- Federal officials supposed to disclose security vulnerabilities they find in devices

INSTAPOLL QUESTION

- Do you agree with the FBI or Apple or neither party? Why?

ENCRYPTION LAWS ABROAD

- In 2016, UK established Investigatory Powers Act that allows government to compel communication providers to remove electronic protections, such as encryption, from communications and data
  - Generally avoided as it may ultimately lose
- Germany and Netherlands have disavowed backdoors

THE FOURTH AND FIFTH AMENDMENTS

- IV: 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.

- V: 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 offence 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.

ENCRYPTION AND THE FIFTH AMENDMENT

- In 2012, judge ordered a Colorado woman suspected of bank fraud ordered to decrypt her laptop
  - Laptop seized with a valid warrant
- Colorado District Judge concluded that requiring production of unencrypted contents did not violate the Fifth Amendment

ENCRYPTION AND THE FIFTH AMENDMENT

- In 2012, unidentified "Doe" defendant believed to be in possession of child pornography
  - Seized with valid warrant but found to be encrypted
- 11th US Circuit Court of Appeals said that an encrypted hard drive is the same as a combination to a safe
  - Compelling the unlocking of it is equivalent to forcing testimony
- Outcome came a day after bank fraud case

CARPENTER VS UNITED STATES

- In 2011, FBI suspected Timothy Carpenter was working as a getaway driver for a series of armed robberies
  - Used location data based on his phone as evidence
- Carpenter argued tracking his location using his cellphone without a warrant violated the Fourth Amendment
- Sixth Circuit Court of Appeals concluded warrant not required as Carpenter has no privacy or property rights in location data
  - Third-party doctrine states that information voluntarily given to a third-party cannot have any expectation of privacy
- Case reached Supreme Court in November 2017
  - The Court ruled, in a 5-4 decision, that the government was in violation of the 4th Amendment
  - Narrowly scoped to only include cellphone data and did not change third-party doctrine

PRIVACY VERSUS SECURITY

- What are the risks of allowing citizens to privacy?
- What are the risks of limiting citizens' privacies?

REFERENCES

- <http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html>
- <https://www.huffingtonpost.com/admiral-jim-stavridis-ret/apple-fbi-privacy-security_b_9404314.html>
- <http://mattwashchuk.com/articles/2016/2/24/how-and-when-apple-discloses-your-data-to-law-enforcement>
- <https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701>
- <http://www.latimes.com/business/la-fi-tn-apple-fbi-call-20160219-story.html>
- <https://www.smithsonianmag.com/smart-news/what-all-writs-act-1789-has-do-iphone-180958188/>

REFERENCES

- <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>
- <https://gizmodo.com/the-fbi-paid-900-000-to-unlock-the-san-bernardino-kill-1795010203>
- <https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act>
- <https://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/>
- <https://www.wired.com/2012/01/judge-orders-laptop-decryption/>
- <https://www.wired.com/2012/02/laptop-decryption-unconstitutional/>
- <http://nymag.com/daily/intelligencer/2017/11/the-supreme-courts-cell-phone-tracking-case-has-high-stakes.html>
- <https://www.oyez.org/cases/2017/16-402>