

Privacy and the Government

Lecture 8-2

Computers & Society (CPSC 430)

Hedayat Zarkoob

<https://www.students.cs.ubc.ca/~cs-430/>

Original slides by Kevin Leyton-Brown.

Review

- Strong Encryption
 - e.g., 256-bit AES
 - mathematical reasons to believe governments can't break it either
- In Fall 2013, it emerged that the NSA was engaged in a very wide range of wiretapping

[https://en.wikipedia.org/wiki/Global_surveillance_disclosures_\(2013%E2%80%93present\)](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present))

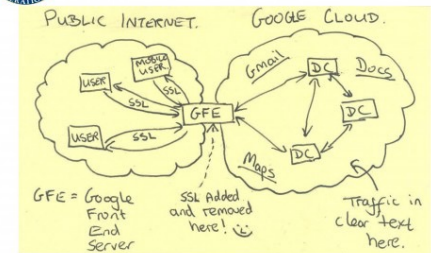


- Washington Post summary of the leaks:
 - Taken together, the revelations have brought to light a global surveillance system that cast off many of its historical restraints after the attacks of Sept. 11, 2001. Secret legal authorities empowered the NSA to sweep in the telephone, Internet and location records of whole populations.



TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

Discussion

Do you think Snowden behaved unethically?

What do you think about wiretapping more broadly?

FBI–Apple encryption dispute (2015-2016)

Follows https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute

- In 2015 and 2016, Apple Inc. received and objected to or challenged at least 11 orders issued by United States district courts seeking to compel it “to use its existing capabilities to extract data like contacts, photos and calls from locked iPhones running on operating systems iOS 7 and older” in order to assist in criminal investigations and prosecutions
 - Newer phones use strong encryption, which Apple can’t break
 - The government has sought to compel Apple to write new software that would let the government bypass these devices’ security and unlock the phones
- **Best known case:**
 - Feb 2016: FBI wanted Apple to create and electronically sign new software that would enable the FBI to unlock a work-issued iPhone 5C it recovered from one of Dec 2015 San Bernardino terrorists (killed 14 people, injured 22)
 - The phone was locked with a four-digit password; set to erase all data after ten failed password attempts
 - Apple declined to create the software
 - A day before the hearing, the government obtained a zero-day exploit and unlocked the phone itself
 - The Los Angeles Times later reported that “the FBI eventually found that Farook's phone had information only about work and revealed nothing about the plot”

Privacy and the Government

“It should be illegal to sell a mobile phone that cannot be decrypted by the police if so ordered by a court.”

A total of 59 voter(s) in 1439 hours



“Lie Detectors”

- Present Day: Polygraphs

- Scientific status: ambiguous

- NAS: better than chance, far from perfect (in lab conditions)

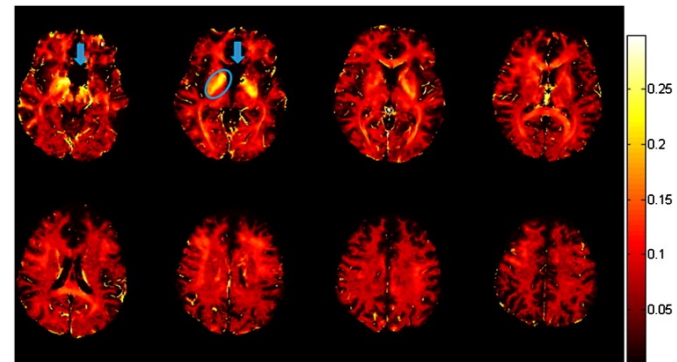
- Legal status:

- USA:
 - Maybe admissible as evidence
 - Subject must volunteer
 - Canada:
 - Not admissible as evidence
 - Legal for investigating

- Near Future: Neuroimaging

- Legal status:

- India: 1 murder conviction



A Working Lie Detector

- *Suppose a 98%-accurate lie detector were invented. What should its legal status be?*
 - A. Admissible in court, and can be court ordered.
 - B. Admissible in court, if the subject volunteers. (USA)
 - C. Usable during investigation, not admissible in court. (Canada)
 - D. Never to be used.