

CPSC 430

Computers & Society

Class 3C: Privacy and the Government (Chapter 6)

Dr. Firas Moosvi | 2024_S1

Slides courtesy of Dr. Kevin Leyton-Brown

Class Outline

1. Announcements (10 mins)
2. Encryption (30 mins)
3. Activity (20 mins)
4. Break (10 mins)
5. Privacy and the Government (40 mins)
6. Activity (20 mins)
7. Reminders before next class (5 mins)

Announcements

Encryption

Encryption

- Method for concealing the content of a message
- Symmetric encryption:
 - Single key used to encrypt and decrypt a message
 - Problem: How does sender get key to receiver?
- Public-Key encryption (e.g., RSA):
 - Each person has two keys: public and private
 - To send ***R*** a message, encrypt it with ***R***'s public key
 - ***R*** decrypts message with ***R***'s private key
 - No need to communicate private keys
- SSL (https://...) is based on public-key encryption:
 - Upon connection, server reports its public key and a trusted certificate authority that can verify it. The client may verify the key.
 - The client encrypts a random number with the server's public key and sends the result to the server.
 - The server decrypts it with its private key.
 - From the random number, both parties generate key material for encryption and decryption.

Strong Encryption

- Strong encryption: encryption at a level that is believed not to be breakable by any other than sender/receiver
 - e.g., 256-bit AES
 - mathematical reasons to believe governments can't break it either
- Availability of strong encryption
 - Previously classified as a munition by US, regulated
 - 1991: US Senate passed a law requiring all encryption systems to include a “back door”
 - In response, Phil Zimmerman created PGP
 - Government tried to shut it down
 - 1999, 2000: courts ruled that these restrictions are illegal, encryption protects privacy and free speech
- *Questions*
 - *Should there be laws against use/distribution of strong encryption?*
 - *How should governments respond to its existence?*

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 105 voter(s) in 1170 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

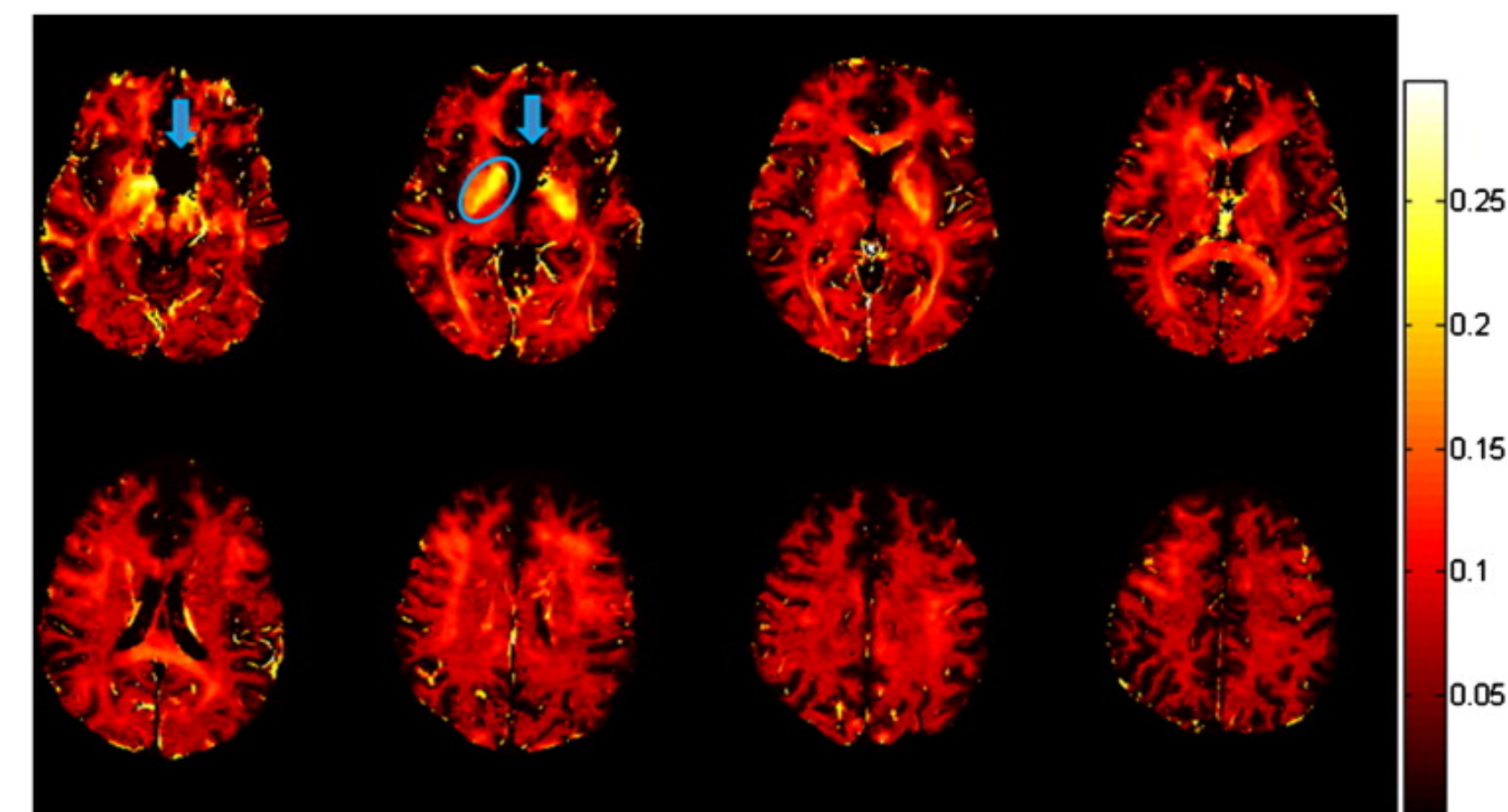
- Canada:

- 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.

Activity

Privacy and the Government

Snowden and the NSA Scandal

- In Fall 2013, it emerged that the NSA was engaged in a very wide range of wiretapping

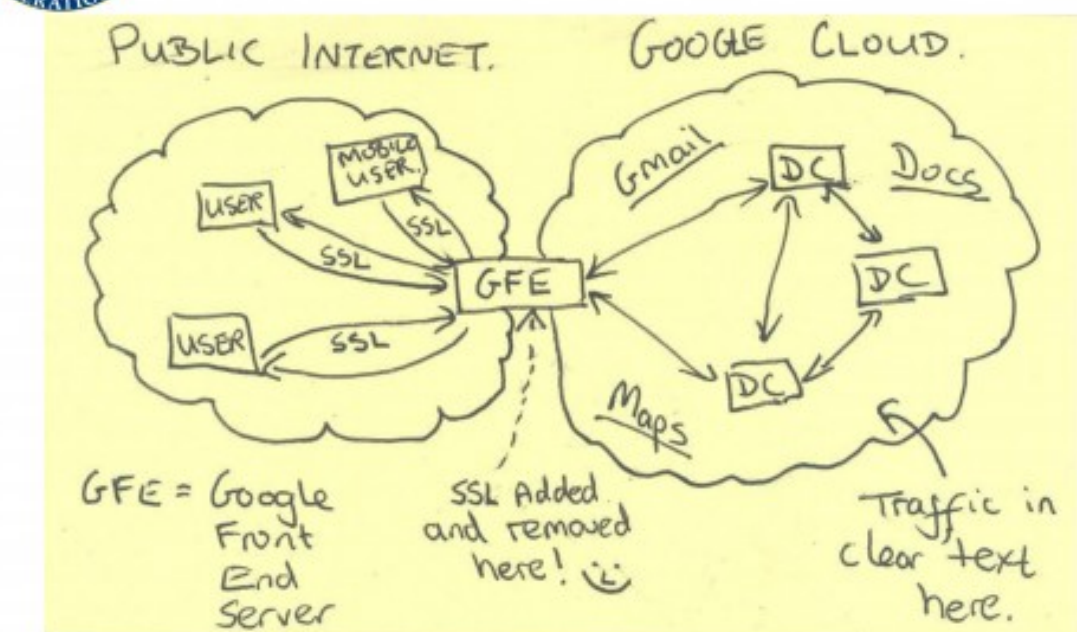
[https://en.wikipedia.org/wiki/Global_surveillance_disclosures_\(2013%E2%80%93present\)](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present))



- 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.



Current Efforts - Google



TOP SECRET//SI//NOFORN

Xkeyscore

<https://en.wikipedia.org/wiki/XKeyscore>

“What could you do if you would use XKeyscore?” Snowden:

- You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information. ... You can tag individuals ... Let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint, which is network activity unique to you, which means anywhere you go in the world, anywhere you try to sort of hide your online presence, your identity.*

Greenwald: low-level NSA analysts can, via systems like Xkeyscore:

- “listen to whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents. And it's all done with no need to go to a court, with no need to even get supervisor approval on the part of the analyst.”*
- analysis can listen "to the calls or read the emails of everything that the NSA has stored, or look at the browsing histories or Google search terms that you've entered, and it also alerts them to any further activity that people connected to that email address or that IP address do in the future".*

Discussion

Do you think Snowden behaved unethically?

What do you think about wiretapping more broadly?

Government-Issued ID

- Government-issued ID is needed for many activities
 - Getting into a bar
 - Flying on a plane
 - Renting a car
 - Opening a bank account
- Advantages:
 - reduce illegal activities
 - Hard for people to change identities
- Disadvantages:
 - Facilitates fraud (easier to assume my identity)
 - Facilitates data mining (provides a unique key)

Should everyone be required to have a government ID card? Should there be rules about what I'm allowed to do without showing government ID?

Public Records: Statutory Disclosures

- Census
 - Purpose: ensure that seats in Parliament are apportioned correctly
 - Worry: this data may also be used for other purposes
 - Much recent political discussion about the long-form census

...how worried should we be about the existence of such records?

Activity

Reminders before next class