DR. SARAH ABRAHAM

CS349

PRIVACY

RIGHT TO PRIVACY

- In 1890, Samuel Warren and Louis Brandeis published article “Right to Privacy” in the Harvard Law Review
- Declaration of a “right to be let alone”
- Response to use of journalist practices and technologies of the time:
  - Instant photography
  - Idle gossip as a trade

RIGHT TO PRIVACY (FIRST PARAGRAPH)

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible.

OLMSTEAD VS UNITED STATES

- Olmstead was a police officer who also ran the most successful bootlegging operation in the Pacific Northwest
- Federal agents used wiretapping to incriminate him
- Olmstead appealed the Supreme Court claiming wiretapping was unreasonable search and seizure
  - Violation of the 4th Amendment
- 5-4 verdict against Olmstead
  - Chief Justice William Howard Taft claimed a private telephone communication was no different than a public conversation
  - Justice Brandeis dissented, in part citing right to be let alone: To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

KATZ VS UNITED STATES

- 1967 case overturned Olmstead vs United States verdict
- Wiretapping by state or federal investigators requires a warrant
- Brandeis' previous dissent cited for overturn of Olmstead and ruling in favor of Katz
- Brandeis' idea of a constitutional "right to be let alone" not expressly included in the constitution but used in a number of notable court cases
  - Used in Roe vs Wade to allow access to abortions
  - Used in Griswold vs Connecticut to allow access to contraception
  - Used in Lawrence vs Texas to invalidate sodomy laws

BUT GOING BACK TO BRANDEIS' ORIGINAL CRITIQUE OF THE MEDIA. . .

- With such pervasive advertising, do we still have a right to be let alone?
- Is being let alone even possible?

CAMBRIDGE ANALYTICA

- UK-based data firm accused of trying to influence the US 2016 election
- Co-founder and whistle-blower, Christopher Wylie, accused firm of involvement in Brexit as well
  - Questions about involvement in elections in Nigeria and Kenya
- Gobal Science Research (GSR) created an app, thisisyourdigitallife, which collected data on 270k users who agreed to the study
- App also collected data on participants' friends to profile 50M users in total
- Intent was to create targeted political ads that swung voters to Trump

FACEBOOK'S INVOLVEMENT?

- No actual data breach
- Facebook's policy allows for collection of friends' data by app creators and academics
  - Selling data to third parties or using it for advertising is not prohibited
- Facebook claims GSR violated user policies by passing information to Cambridge Analytica
  - App was removed in 2015
  - Facebook requested data be deleted
  - Cambridge Analytica's account suspended

THE FALLOUT

- Facebook stock dropped by as much as $60B
- CEO Zuckerberg to testify before Congress
- Legal complaints filed against Cambridge Analytica and related parties by government watchdog group Common Cause
- Cook County, Illinois suing Facebook and Cambridge Analytica for violating state fraud laws
- Facebook being sued by shareholders and users
- Federal Trade Commission currently investigating Facebook

HOW TO MAINTAIN PRIVACY?

BUYING HABITS

- A man accused Target of encouraging his teen daughter to get pregnant by sending her coupons for baby clothes etc
  - Daughter was actually pregnant but had not revealed it to her father until he brought up the Target ads
- Target associates credit card, e-mail, and name to a guest id number
  - Guest id number tracks customer's purchasing history
  - Associated with demographic information of other customers and based on purchased third-party data
- Target statistician, Andrew Pole, admitted that Target mixes directed ads with general ads so that customers do not perceive themselves as being targeted

FACIAL FEATURES

- Stanford researchers data mined images from dating site to train AI “gaydar”
  - Claimed that, in a forced choice test between two photos, AI could guess who was more likely to be gay (81% of the time for men and 71% percent of the time for women)
- Not clear what features the neural net was using for classification
- Not clear how applicable this technology current is
- Researchers claim the point was to raise awareness about how AI can be misused

CENSUS DATA

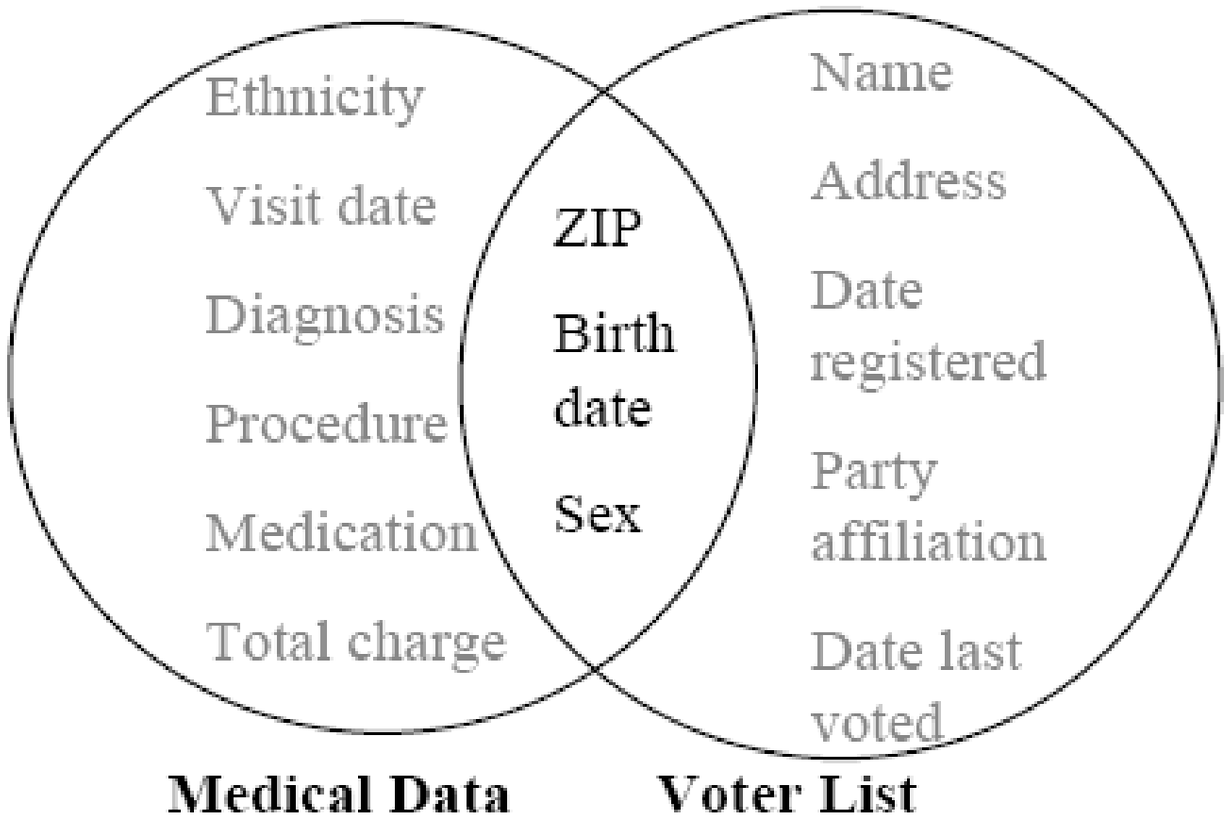
- Government records revealed US Census Bureau provided US Secret Service with names and addresses of Japanese-Americans during WWII
  - Census Bureau prohibited by law from revealing data that is linked to specific individuals
  - Second War Powers Act of 1942 temporarily repealed protections to allow Japanese-Americans to be rounded up
- Census Bureau has no records of this event but secret memos revealed communications between Bureau and Secret Service
- Census Bureau provided neighborhood data on Arab-Americans in 2002
  - But this information was also publicly available

UNINTENTIONAL DATA LEAKS

- A combination of characteristics can de-anonymize otherwise anonymous data sets
- Using 1990 census data set, 87% of US citizens (216M of 248M) were uniquely identifiable by 5 digit zip code, date of birth, and gender
- Also possible for anonymous data sets to be linked to de-anonymized

LINKING DATA

- 37 states have legislative mandates for hospitals to collect patient data
  - Made available to researchers and individuals as set is consider anonymous
- Voter registration lists available for purchase
- In 1998, Researcher Latanya Sweeney linked the then-governor of Massachusetts to his medical records
  - 6 voters had his birthdate, 3 were male, only 1 in his zipcode



K-ANONYMITY

- Information property of released data such that the information of one individual cannot be distinguished from at least k-1 other individuals
- Data can be hidden or generalized to help achieve better k-anonymity
- The higher the data dimensionality, the more difficult it is to maintain higher k-anonymity

GATHERING DATA…

- Ask person for permission!
  - Promotions, quizzes and games, etc
- Use extra bits of information
  - Cookies, device fingerprinting, device identifiers
- Passive attacks
  - Eavesdropping, network analysis, monitoring

VIRTUAL PRIVATE NETWORKS (VPNS)

- Secure tunnel between devices on a public network that allows for communication as if on a private network
- Used in businesses for securely connecting remotely and/or connecting multiple offices
- External traffic routed through VPN allowing for greater anonymity
- Also offers data encryption within network and tamper detection to check for packet modification

VPN USES

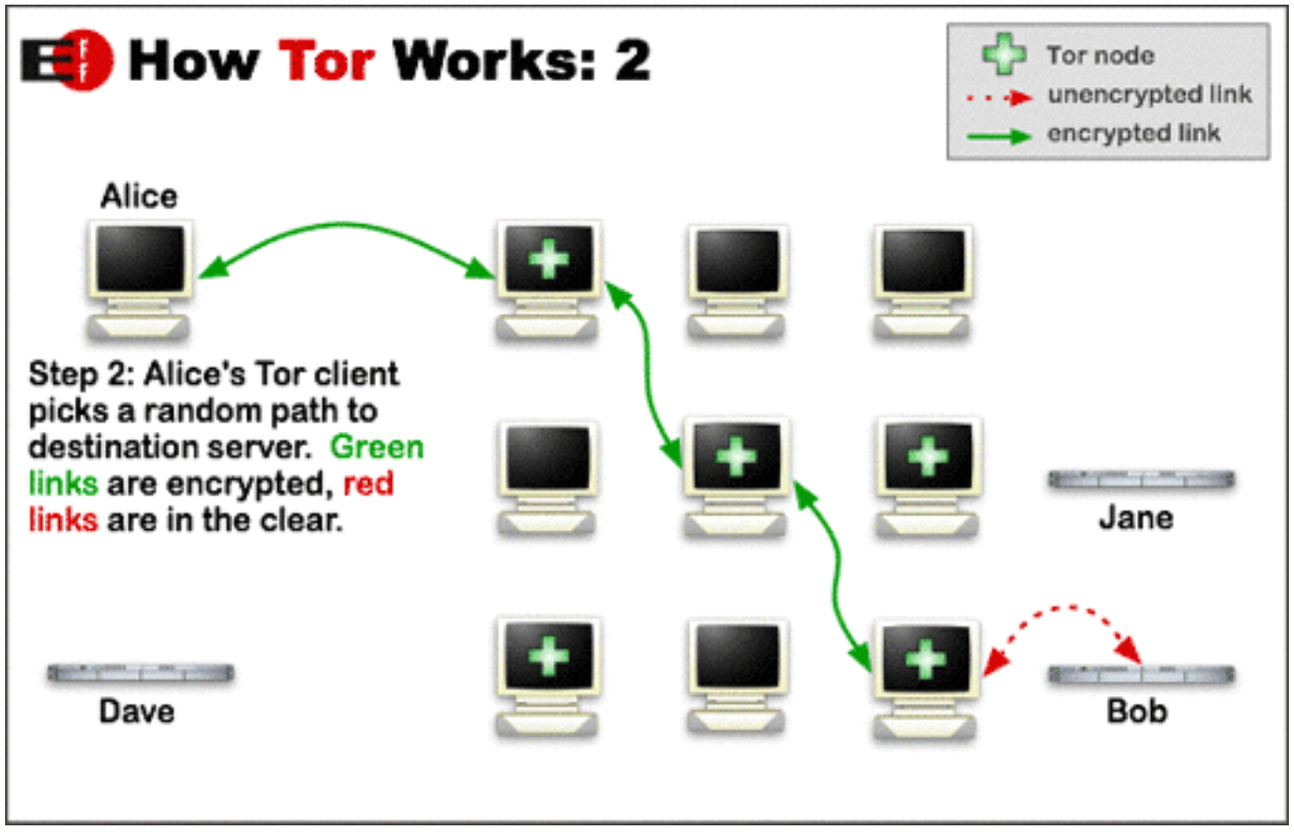
- Allows secure access of sensitive material from a remote location
- Hides IP address and physical location to avoid censorship and geo-restrictions
- Protects from dangers of insecure or unknown access points (e.g. public wifi)

ISSUES?

- VPN services subject to laws of company's country
  - May hand over information based on warrants
- Terms of use and privacy policies vary by company
  - May not allow torrenting
- Does not always work with streaming services
  - Issues with encryption and country copyright
- Increases latency of network connection
  - Many VPN services won't work with gaming
- Cannot protect user from malware attacks or after packets exit VPN

THE TOR PROJECT

- Network of volunteer servers that uses series of virtual tunnels to obfuscate source and destination of data requests
- Designed to protect data transport



WHO USES TOR?

- Journalists, whistleblowers, and dissidents
- NGO workers who do not want to communicate their location
- Web and chat services for people with socially sensitive information (rape survivors, people with illnesses etc)
- Corporations doing competitive analysis or conducting sensitive work/negotiations
- The US Navy for open source intelligence gathering

TOR DEANONYMIZATION

- Operational Security (OPSEC) failures
  - Attackers monitor patterns of behavior of Tor users to accumulate sufficient data to deanonymize
- Targeting Tor-affiliated systems
  - Attackers perform standard cyberattacks to breach system running a node in the Tor network
- Attacks on hidden services
  - Using services such as SSH or Apache through a public IP address as well as through an onion address can make hidden services visible to public
- Traffic and timing correlation attacks
  - Statistical analysis of traffic can reveal connections between entry nodes and exit nodes/hidden services

ISSUES?

- The dark net is full of unsavory (if not outright illegal) things...
  - Child pornography
  - Snuff and torture videos
  - Drug markets
  - Pirated content
- How can we protect privacy while enforcing laws?

REFERENCES

- <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>
- <https://constitutioncenter.org/blog/olmstead-case-was-a-watershed-for-supreme-court>
- <http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=5312&context=mulr>
- <https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html>
- <http://abcnews.go.com/Politics/exclusive-cambridge-analytica-accused-violating-us-election-laws/story?id=54010145>
- <https://gizmodo.com/illinois-cook-county-sues-facebook-and-cambridge-analyt-1824084835>
- <https://www.thestreet.com/story/14536213/1/everyone-who-is-suing-facebook-for-cambridge-analytica.html>
- <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

REFERENCES

- <https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy>
- <https://www.scientificamerican.com/article/confirmed-the-us-census-b/>
- <https://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf>
- <https://www.consumer.ftc.gov/articles/0042-online-tracking>
- <https://ac.els-cdn.com/S1877050915006353/1-s2.0-S1877050915006353-main.pdf?_tid=0bbc314a-52ad-4d4d-8ae6-52dcb98996c9&acdnat=1522365735_1f7663d8d36912ab547fb0b4d56968bc>
- <https://www.pcmag.com/article/352757/you-need-a-vpn-and-heres-why>
- <https://www.torproject.org/about/overview.html.en>
- <https://www.deepdotweb.com/2017/09/12/overview-modern-tor-deanonymization-attacks/>