Day 4

Privacy: Key Aspects
Fair Information Principles
4th Amendment
Privacy Case Law

Re-identification
Secondary use
Informed consent
HIPAA
GLBA
FISMA
1. Freedom from intrusion (being left alone)
2. Control of information about oneself
3. Freedom from surveillance (from being tracked, followed, watched)
Privacy Threats

- Intentional, institutional uses of personal information
- Unauthorized use or release by “insiders”: AOL 2006
- Theft of information
- Inadvertent leakage of information
- Our own actions
  - Aware
  - Unaware

https://techcrunch.com/2006/08/07/aol-this-was-a-screw-up/
Privacy threat or cancer cure?

Microsoft Finds Cancer Clues in Search Queries

By JOHN MARKOFF  JUNE 7, 2016

The researchers focused on searches conducted on Bing, Microsoft’s search engine, that indicated someone had been diagnosed with pancreatic cancer. From there, they worked backward, looking for earlier queries that could have shown that the Bing user was experiencing symptoms before the diagnosis. Those early searches, they believe, can be warning flags.
Old issues, new risks:

- Government and private databases → Public record
- Sophisticated tools for surveillance and data analysis
- Vulnerability of data
Examples

Smartphones

- Data sometimes stored and sent without user’s knowledge
  - Roughly half the apps in one test sent the smartphone’s ID number or location to other companies (in addition to the one that provided the app).
  - Various apps copy the user’s contact list to remote servers.

http://www.wired.com/2015/03/apps-snoop-location-way-think/
This app won't work properly unless you allow Google Play services’ request to access the following:

- Calendar
- Camera
- Contacts
- Microphone
- Phone
- Body Sensors
- SMS
- Storage

To continue, open Settings, then Permissions, and allow all listed items.

Screen shot of friend’s phone, 1/2017, when trying to open Gmail
New Technology, New Risks – Summary of Risks:

- Anything we do in cyberspace is recorded.
- Some people are not aware of collection of data.
-Leaks happen.
- A collection of small items can provide a detailed picture → **metadata = content**

**RE-IDENTIFICATION** (Identifying individuals based on small pieces of info from multiple sources) has become much easier due to the quantity of information and power of data search and analysis tools.
We have been led to believe that metadata — or rather, activity logs — is nothing to worry about; it’s only the content that matters. This may have been true a couple of decades ago when the frequency of digital communications between people and systems was minimal and storage prohibitively expensive. Today, metadata collection and mining has become an industry of its own — accumulating and matching information across countless databases to produce detailed records of everyone’s activities and associations. The goals range from targeting users with relevant advertising to behavioral pattern recognition to aimless harvesting of records for yet unknown future use. 

-Nico Sell, Rita Zolotova

- Data collected for one purpose will find other uses → **SECONDARY USE**
- We depend on businesses and organizations to protect our info.
Terms to know

- **INVISIBLE INFORMATION GATHERING** - collection of personal information about a user without the user’s knowledge.

- **DATA MINING** – Searching and analyzing masses of data to find patterns & develop new information or knowledge.

- **COMPUTER PROFILING** – Analyzing data to see which people are likely to engage in a certain behavior.
**INFORMED CONSENT** — users are aware of/approve what information is collected and how it is used.

- **opt out** — Person must request (usually by checking a box) that an organization *not* use information.

- **opt in** — The collector of the information may use information only if person explicitly permits use (usually by checking a box).

![Email Subscriptions](image.png)
1. Inform people when you collect information.
2. Collect only the data needed.
3. Offer a way for people to opt out.
4. Keep data only as long as needed.
5. Maintain accuracy of data.
6. Protect security of data.
7. Develop policies for responding to law enforcement requests for data.
HIPAA 1996

0 Health Insurance Portability and Accountability Act

0 Protects the confidentiality and security of healthcare information, enforceable by law
Requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data, enforceable by law.
FISMA 2002

- Federal Information Security Management Act
- Assigns various responsibilities to various agencies to ensure the security of data in the federal government.
- Requires annual reviews of information security practices.
- Enforceable by law.
The right of the people to be secure in their person, 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.

—4th Amendment, U.S. Constitution
2 key problems arise from new technologies with the 4th amendment:

- Much of our personal info is no longer safe in our homes; it resides in huge databases outside our control.
- New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge.
  - particle sniffers, imaging systems, location trackers
Limits disclosure of records held by agencies of the federal government to other agencies, organizations, and individuals, although....

in an omission that disappointed privacy advocates and ignored the recommendations of the secretary's committee, it did not incorporate the private sector in its scope.

As of 2007, Dept. of Homeland Security and ADIS are exempt.

Some think it may have been a response to public outcry of “big government” and surveillance states as depicted in Orwell’s 1984 (1949).
Privacy Case Law

**Olmstead v. United States** (1928)

- Supreme Court **allowed** the use of **wiretaps** on telephone lines **without a court order**.

- Interpreted the Fourth Amendment to **apply only to physical intrusion** and only the search or seizure of **material things**, not conversations.
Supreme Court reversed its position and ruled that the Fourth Amendment does apply to conversations.

Court said that the Fourth Amendment protects people, not places. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order.
Court stated that where “the government uses a device that is not in GENERAL PUBLIC USE, ... the surveillance is a “search” and a warrant must be obtained.”
Search “Incident to Arrest”

Formerly permitted an officer to perform a warrantless search during or immediately after a lawful arrest, regardless of what the arrest was for.

The exception is now limited to the person arrested and the area immediately surrounding the person in which the person may gain possession of a weapon, in some way effect an escape, or destroy or hide evidence.

So can they search your phone?

Search/seizure of phones & computers

Update (6/14): cell phones may not be searched, even incident to arrest, without a warrant. BUT...

Court: Police can use your fingerprint to search your phone

By Cory Bennett - 10/31/14 09:21 AM EDT

The police can get your fingerprint, but not your password, to unlock your smartphone, a Virginia judge ruled this week.

A password is constitutionally protected individual knowledge, Virginia Beach Circuit Court Judge Steven Frucci ruled. But a fingerprint is similar to giving a DNA or handwriting sample, which the law allows, he said.

Feds Can't Force You To Unlock Your iPhone With Finger Or Face, Judge Rules

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/#15cc0c7842b7
Update 8/2017

iOS 11 has a ‘cop button’ to temporarily disable Touch ID

by Tom Warren | @tomwarren | Aug 17, 2017, 10:29am EDT

Update 6/2019

Give up your password or go to jail: Police push legal boundaries to get into cellphones

“The world should know that what they’re doing out here is crazy,” said a man who refused to share his passcode with police.

Update 6/2018

Supreme Court restricts police on cellphone location data

Lawrence Hurley

Carpenter v. US
Surveillance, facial recognition

- Security cameras
  - Increased security
  - Decreased privacy
- 2001 “SnooperBowl”

2013

Facebook, Walmart to Help Write Rules On Facial Recognition Technology

Facial Recognition Moves Into a New Front: Schools

A district in upstate New York has adopted the technology in the name of safety. Opponents cite privacy and bias concerns.

By Davey Alba
Feb. 6, 2020, 3:00 a.m. ET