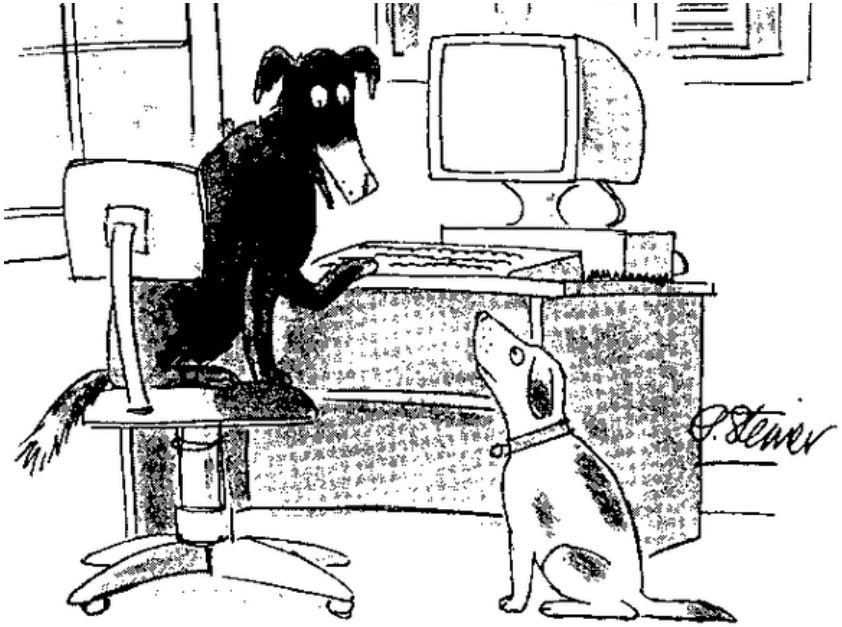
Lecture 5: Privacy

CS 138

Spring 2026



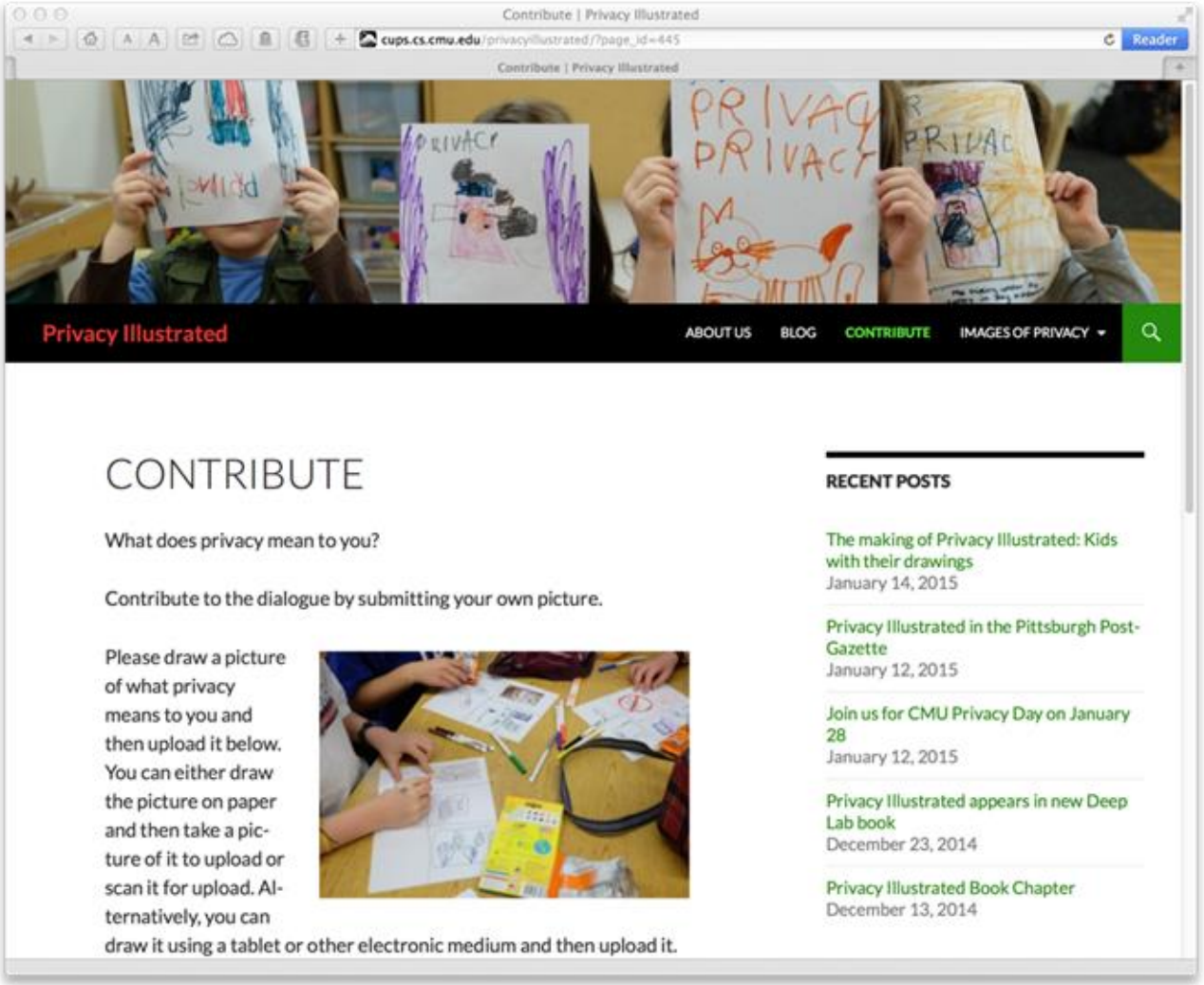
"On the Internet, nobody knows you're a dog."

Confidentiality
Integrity
Availability

What is Privacy?

Exercise: What does Privacy Mean to You?

- Draw a picture that represent privacy to you
- Or feel free to jot down some words, phrases



http://cups.cs.cmu.edu/privacyillustrated/

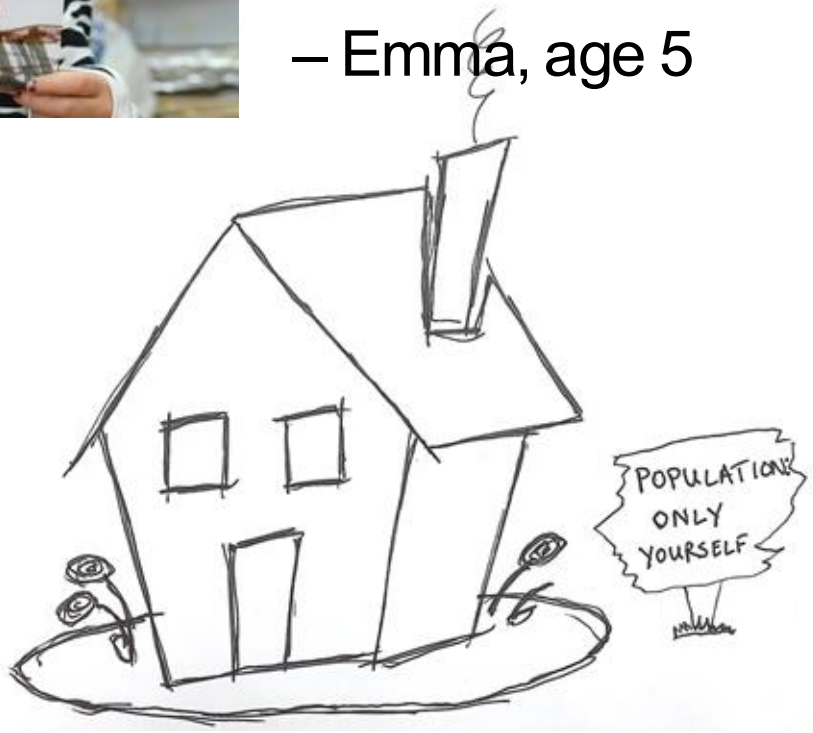
Being left alone

"Being alone."

– Shane, age 4

Privacy is being by myself.

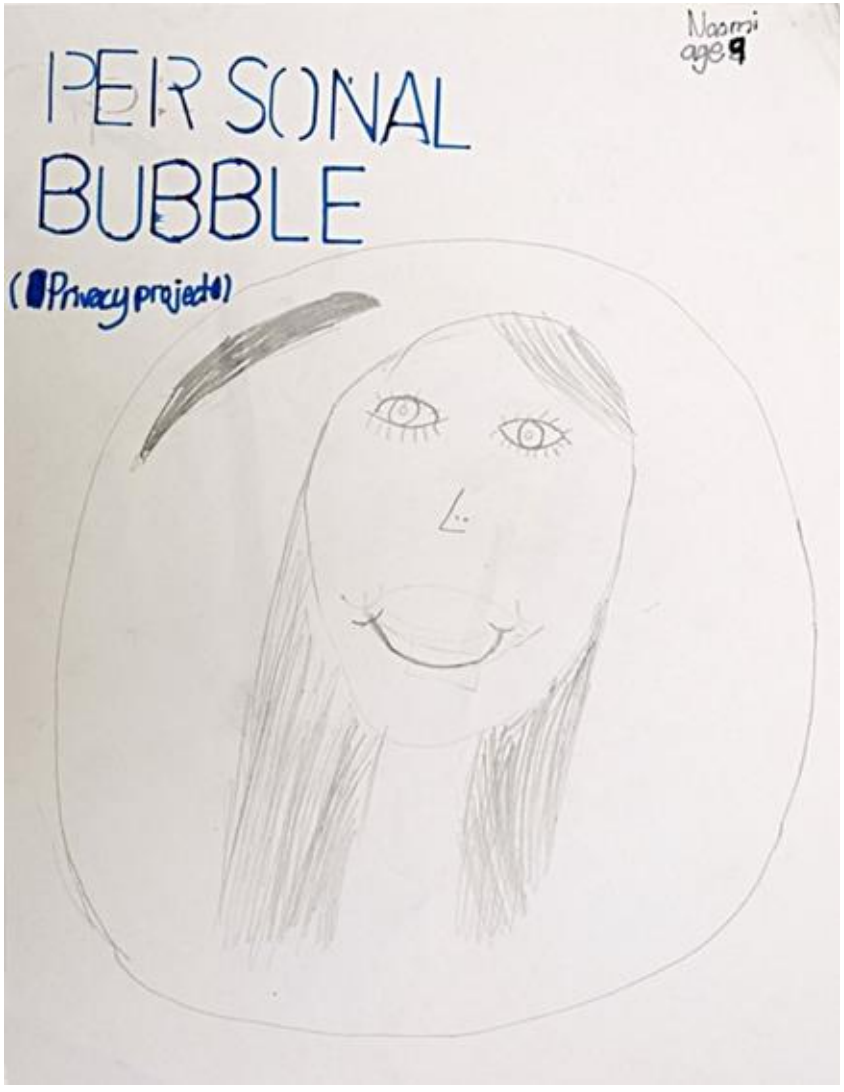
– Emma, age 5



Privacy is the right to be by yourself. Privacy is isolation.

– Kevin, age 28

Personal Bubble



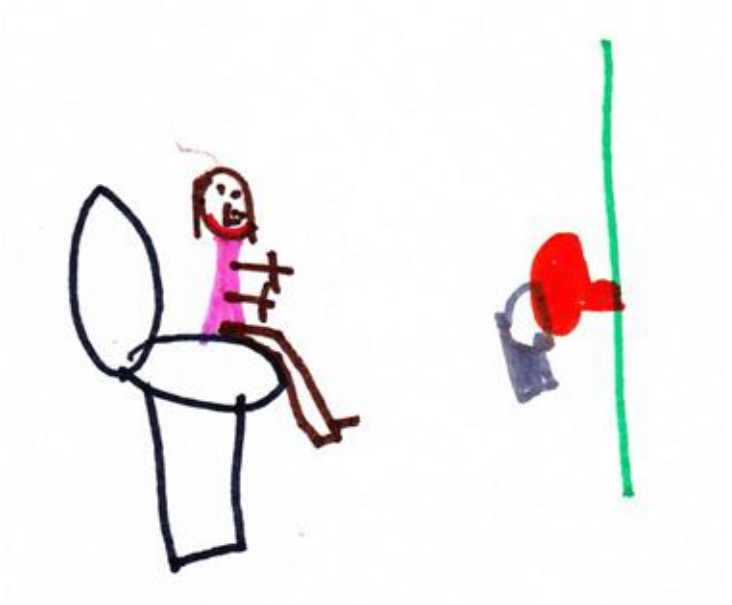
Privacy for me is like a place with a one-sided mirror. I can see outside but no one can see in unless I open the door. Also an extra wall on the outside just in case.

– Kim, age 21

Private Spaces

Your room is private.

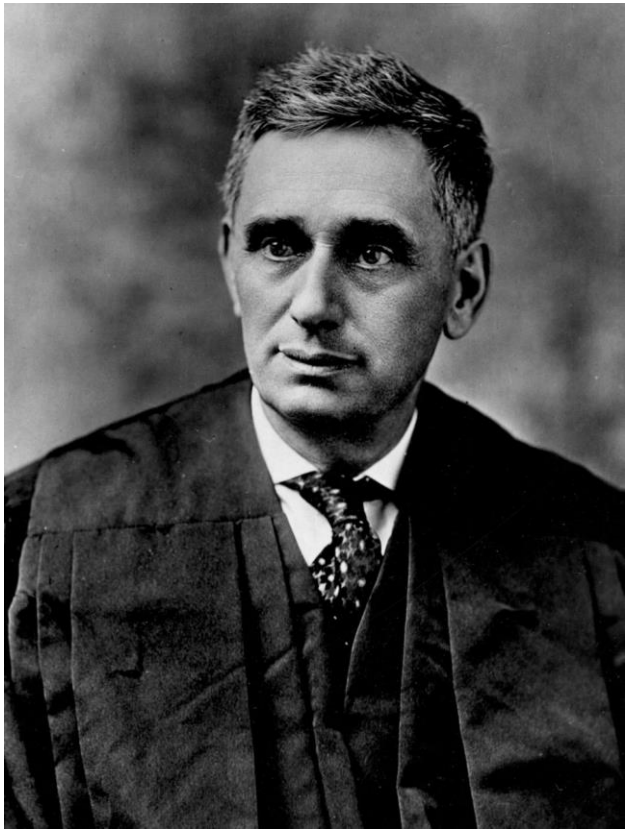
– Alexia, age 11

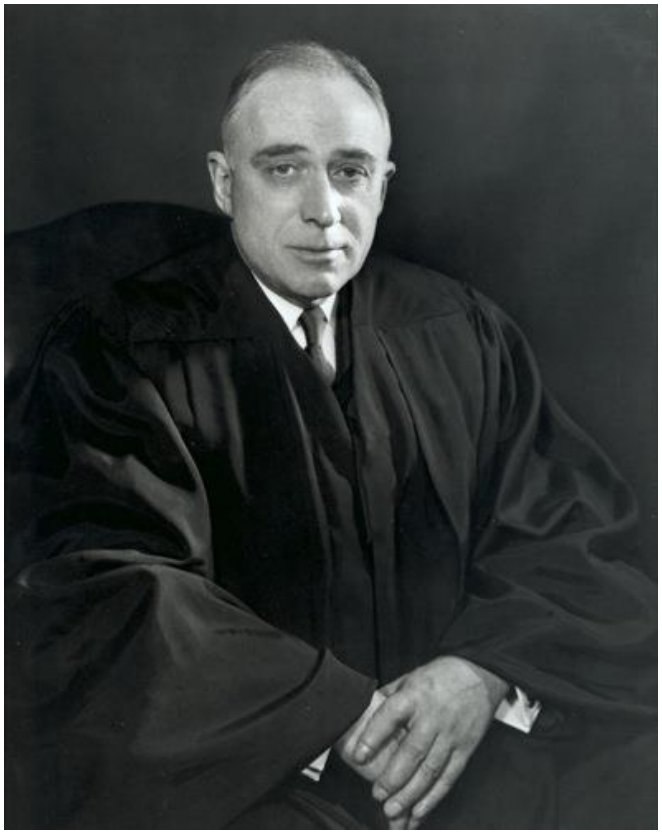


No one come in when I am in the bathroom!

– Sydney, age 7

"The Right to Privacy" (1890)





- Right to be left alone
- Some data is private

Sensitive Data Today

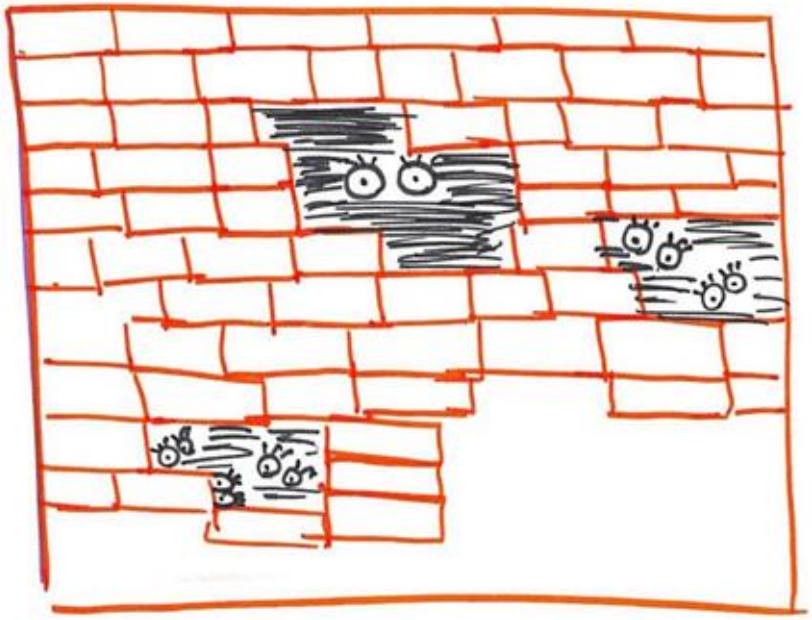
GDPR

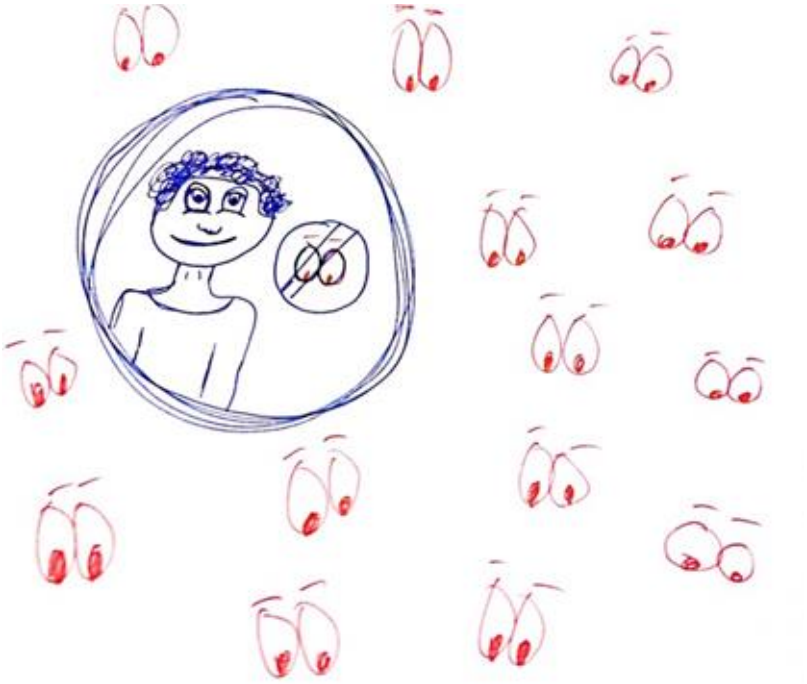
- “personally-identifiable data”
- sensitive data is a specific set of “special categories”:
  - Genetic data
  - Political opinions
  - Racial or ethnic origin
  - Data concerning health
  - Trade union membership
  - Religious or philosophical beliefs
  - Data concerning sex life or sexual orientation
  - Biometric data
- Extra restrictions on processing

CCPA

- “Personal information”
- “Sensitive personal information” means:
  - ID numbers (SSN, license number, etc)
  - financial info or credentials.
  - precise geolocation.
  - racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.
  - contents of mail, email, and text messages
  - genetic data.
  - neural data.
  - biometric information
  - health data
  - data about sex life or sexual orientation.

Freedom from Surveillance





"To me privacy means being able to get away from unwanted eyes."

Katz v. United States (1967)

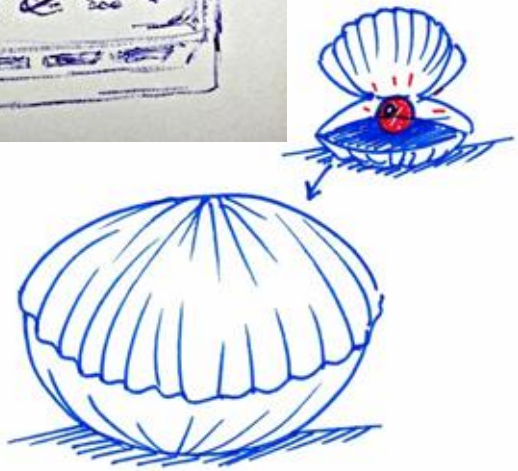
- “Because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure”

- “reasonable expectation of privacy”

Exercise: Reasonable expectation of privacy

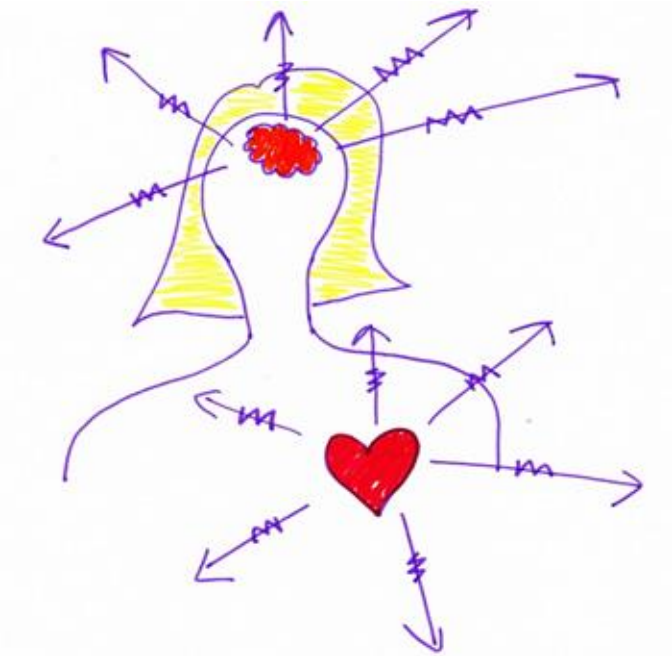
- In-person conversations
- Phone records (who you talk to, for how long, etc)
- Phone conversations (actual content)
- Emails/DMs
- Bank Records
- Things you put out in the trash/recycling
- Your DNA
- Your GPS location

Locks and Barriers



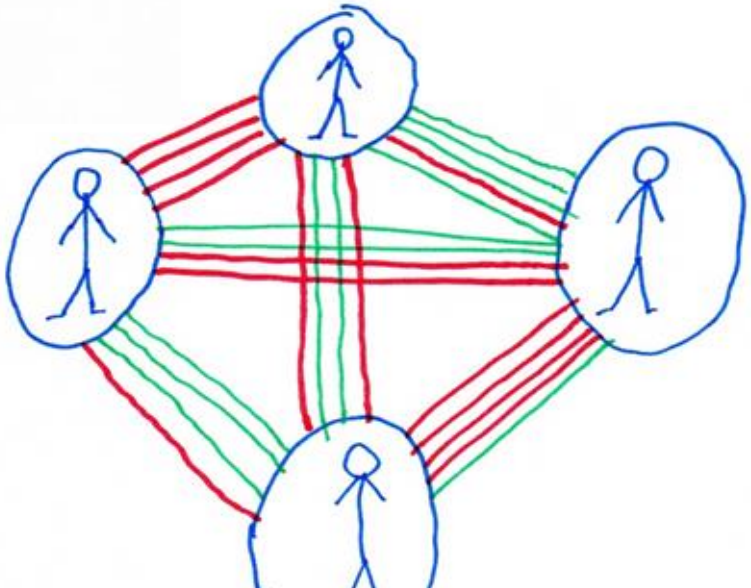
PEARL OYSTERS HAVE SOMETHING VALUABLE TO PROTECT - THE PEARL.
THEY CAN DO SO BY SIMPLY 'CLOSING THE LID'
IF ONLY SAFEGUARDING THE DATA IN MY LAPTOP WERE THAT SIMPLE!

Privacy as Control



Privacy is about control – controlling what is shared about your thoughts and preferences, the things that make you you.

– KRB, age 39



Privacy is a network: I share what I want with whom I want and trust and what matches with those in the network….

Green = share.
Red = don't.

Privacy and Freedom (1967)

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

– Alan Westin

Rights to Control Today

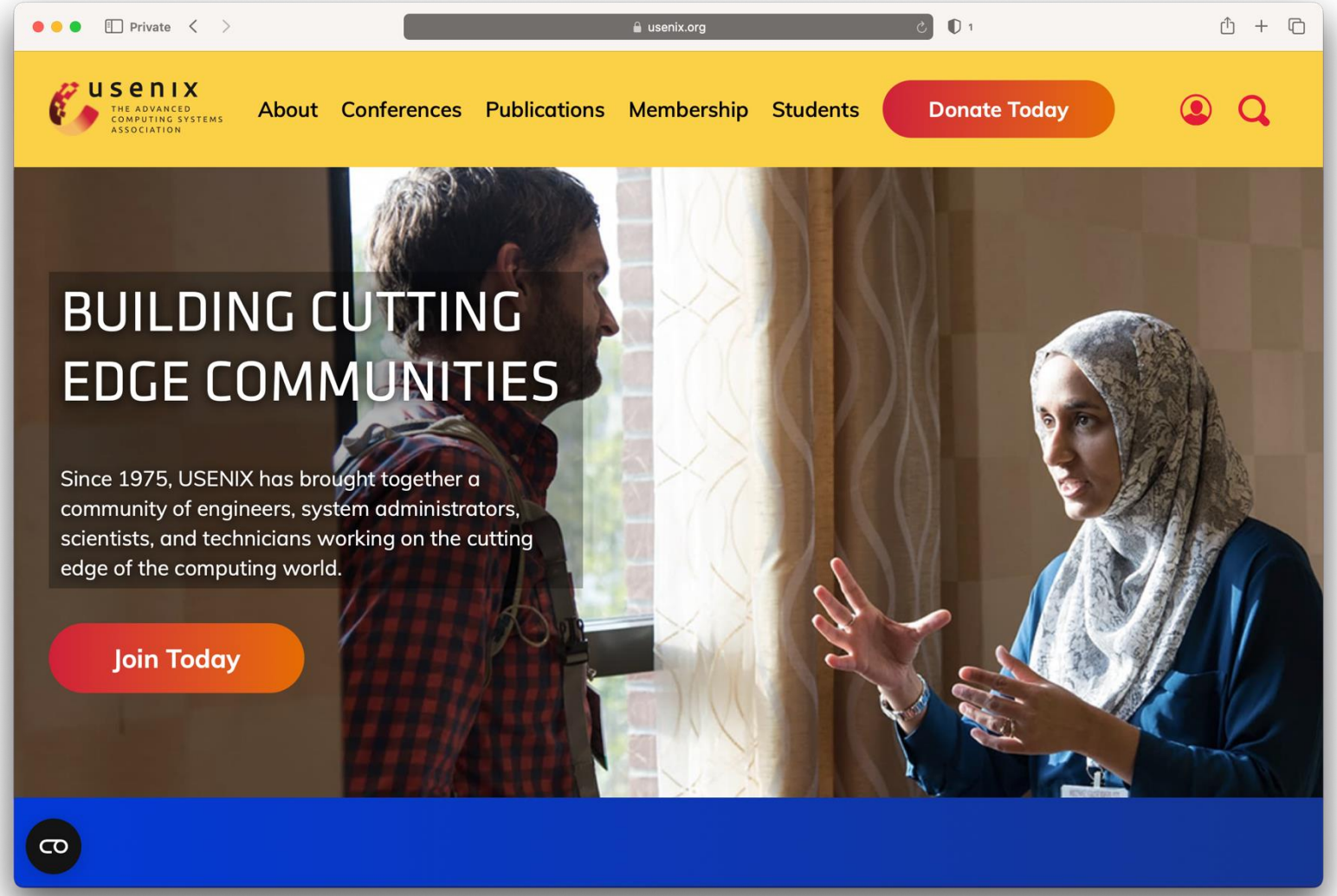
GDPR

- Right to Access
- Right to Rectification
- Right to Erasure
- Right to Data Portability
- Right to Object to Automated Decision Making
- Consent as basis for processing

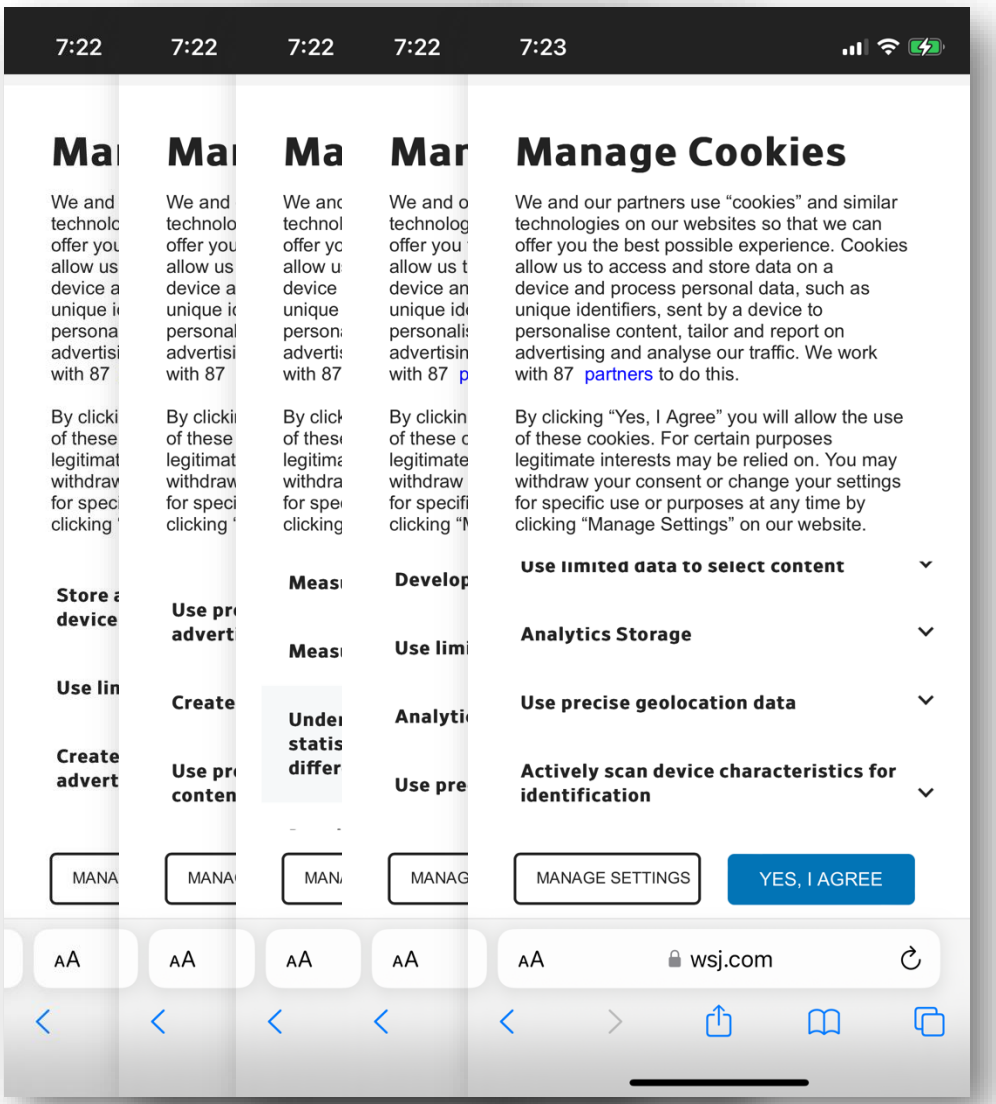
CCPA

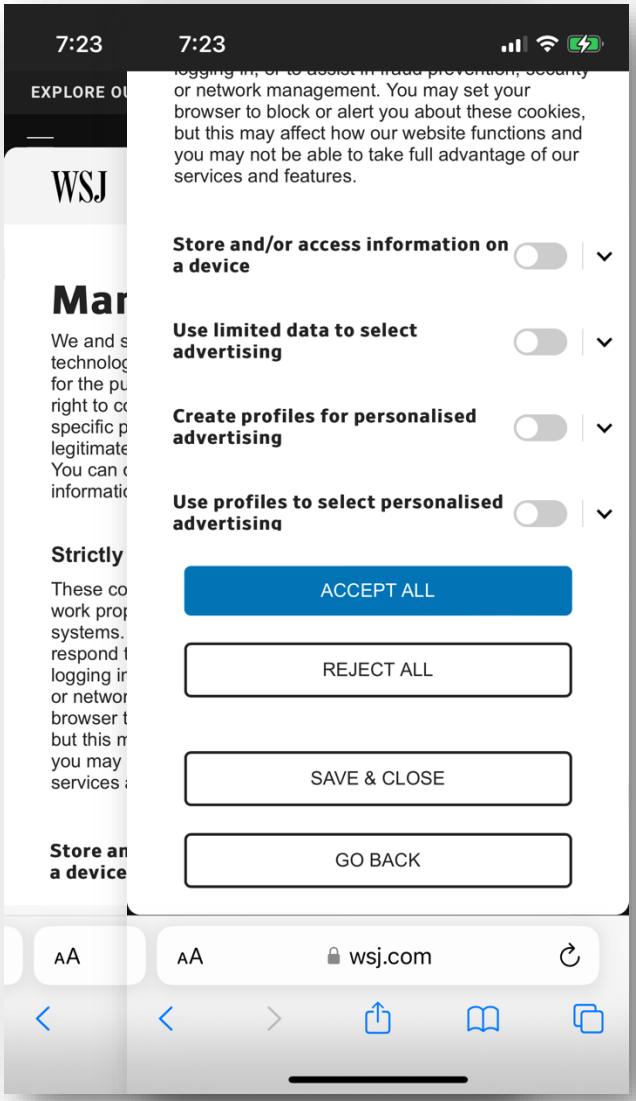
- Right to Know
- Right to Correct
- Right to Delete
- Right to Opt-out of Sale or Sharing
- Right to Limit Use of Sensitive Personal Info
- Right to non-discrimination for exercising CCPA Rights

Right to Consent

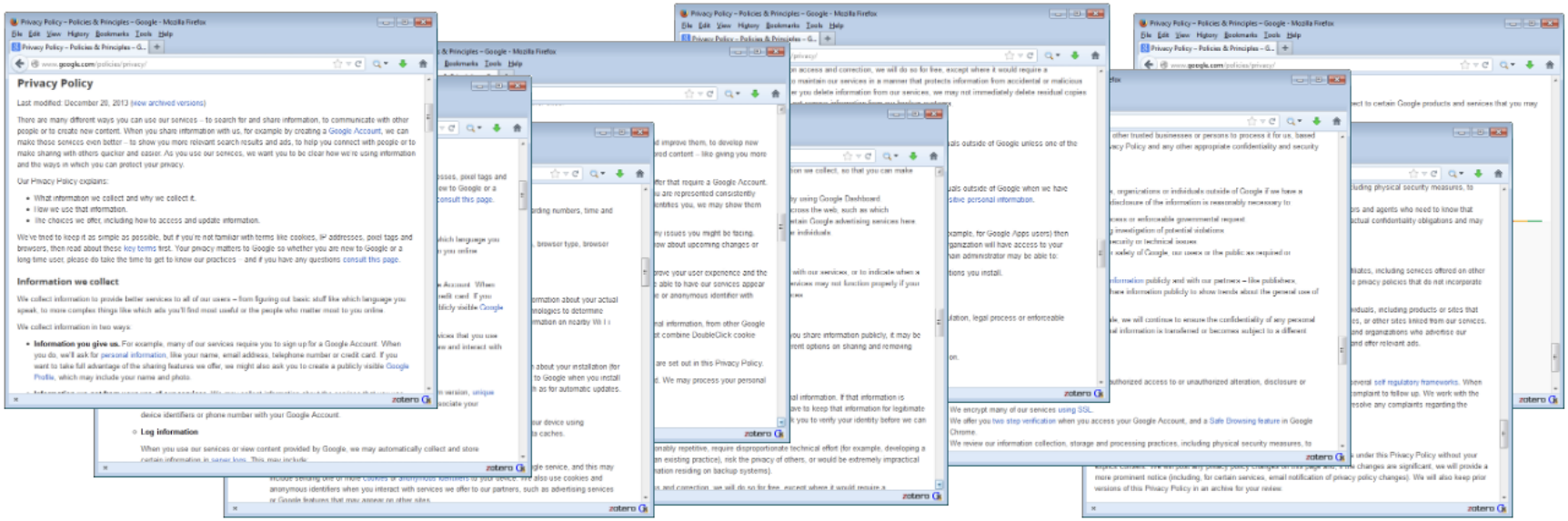


Right to Consent

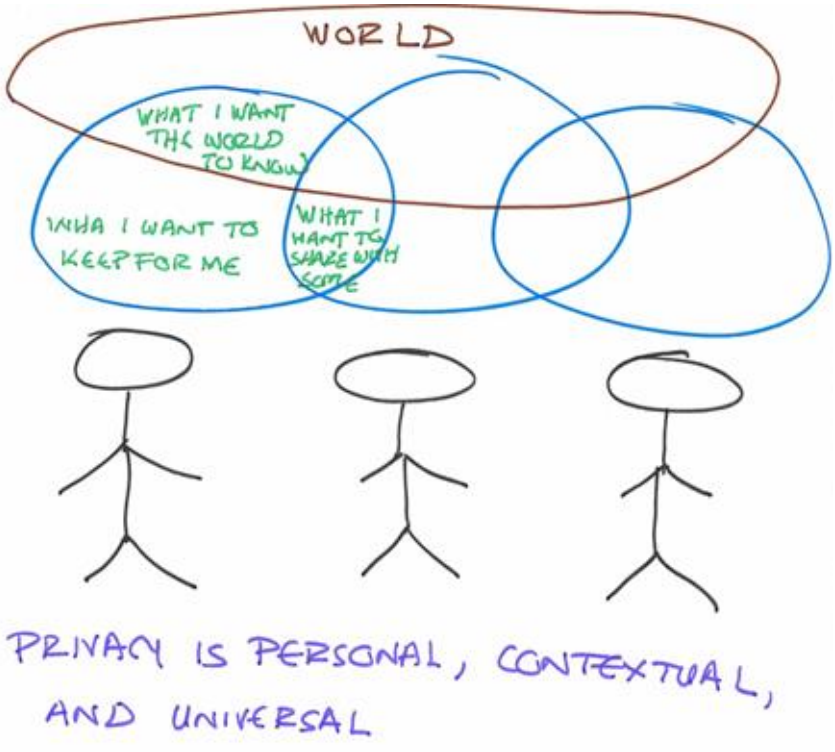




What about Transparency…



Societal Values



Privacy is a value that is very important to have in a society to work and progress

– Pedro, age 35

Contextual Integrity

- defines privacy relative to appropriate context
- considers information type, time, location, purpose, principals involved (subject, sender, receiver)
- dependent on social norms
- norms can change over time

Contextual Integrity

CI says a context can be defined by:

1. **Data Type:** what sort of information is being shared?
2. **Subject:** who is the information about?
3. **Sender:** who is sharing the information?
4. **Recipient:** who is receiving the information?
5. **Transmission Principle:** constraints on data flow
   - with subject's consent
   - with notice (some sort of advance announcement or disclosure)
   - reciprocity ("I'll show you mine if you show me yours")
   - subject to legal requirements
   - the Chatham House Rule (information can be reshared only without attribution)

Norms are identified and flows are evaluated within this context

Contextual Integrity Example

- Anyone can track a Venmo user's purchase history and glean a detailed profile – including their drug deals, eating habits and arguments – because the payment app lacks default privacy protections.

- **Relevant Norm:** My transaction only visible to me and the receiver by default.

- **Example flow violating norm:**

  data type = transaction information

  sender=me, receiver=friend, subject=me

  transmission principle = public/no constraints

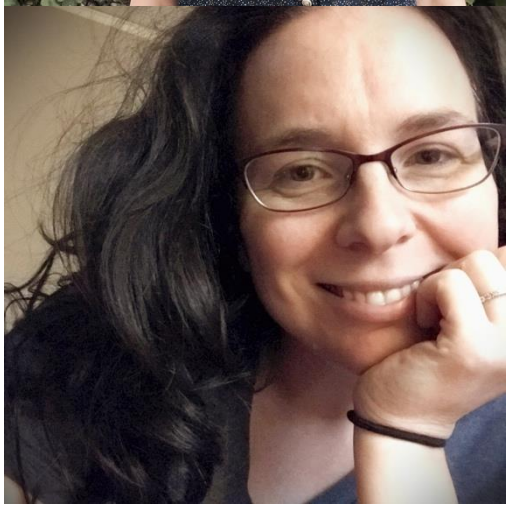
- **Privacy-preserving solution:** make app setting private by default

Exercise: Contextual Integrity

1. An Uber driver has put a video of hundreds of his passengers online without letting them know.
2. Pomona puts Amazon Echo devices in all dorm rooms.
3. Google tracks your movements even if you set the settings to prevent it.
4. Meta asked large U.S. banks to share financial information on their customers.
5. California decides to post all public records in an online, searchable database, which can also be downloaded.

https://docs.google.com/spreadsheets/d/11IbG2kCw4eKsauIZ_10woVPN0G5A6_SO9AnZQ0xzkdY/edit?usp=sharing

Privacy as Vulnerabilities



- limitations of norms for protecting privacy
- vulnerable populations
  - more likely to be susceptible to violations
  - harms are higher impact
- draws on feminist and queer theory

How privacy is protected

- Self regulation
- Laws
- Technology

FIPPs

The FTC's Fair Information Practice Principals (FIPPs) are the most broadly recognized guidelines for handling private data in information systems

- Seek consent
- Minimize data use
- Limit storage
- Avoid linking

OECD fair information principles

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

Privacy laws around the world

- Europe has comprehensive privacy laws (GDPR) and data protection commissioners in every country
- 162 countries have privacy or data protection laws
- US has mostly sector-specific laws, minimal protections, often referred to as “patchwork quilt”
  - No explicit constitutional right to privacy or general privacy law
  - Narrow regulations for health, financial, education, children, etc.
  - Federal Trade Commission jurisdiction over fraud + deceptive practices
  - 19 states have comprehensive privacy laws
    - California laws: CCPA and CPRA

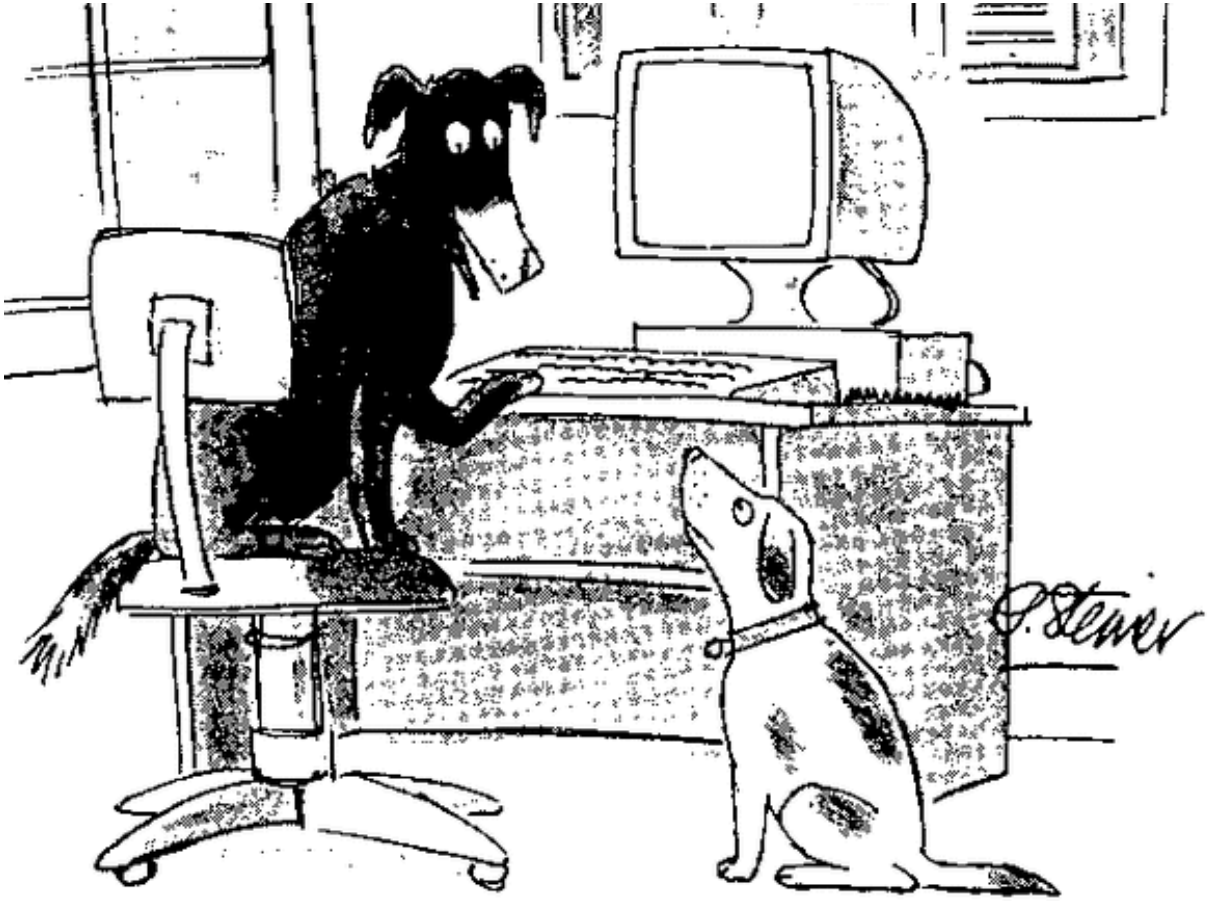
Privacy-Enhancing Tools

- Cryptography
  - encryption
  - homomorphic encryption
  - blinded signatures
  - zero-knowledge proofs
  - anonymous credentials
- Differential Privacy
- Onion Routing, VPNs
- Privacy-preserving advertising
- Privacy-preserving machine learning

Privacy mechanisms require usability

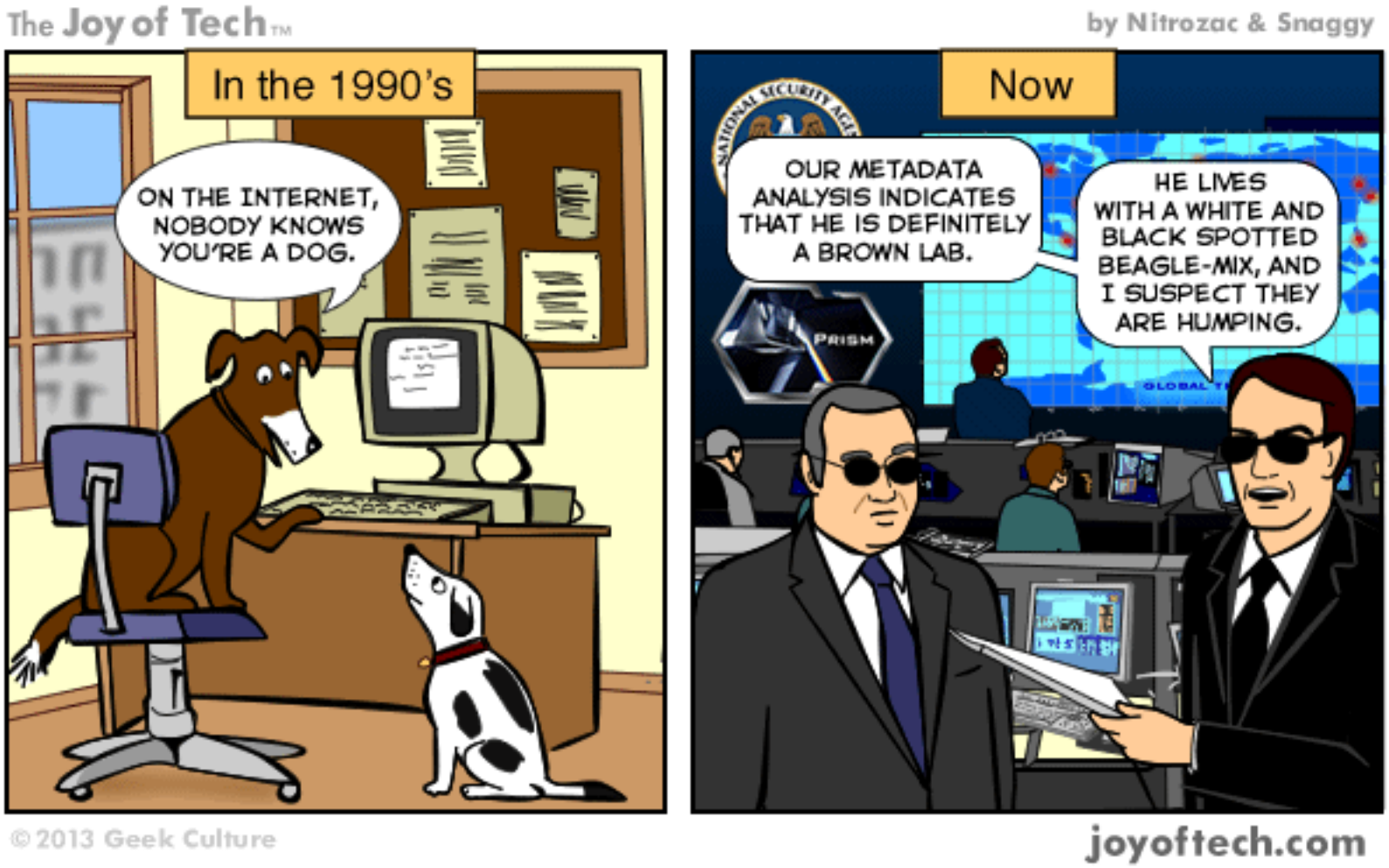
- Clear and plain language
- Concise, transparent, intelligible and easily accessible
- Clear and conspicuous
- Easy to find, read, and use
  - Use of data
  - Access data that organization has collected
  - Request data deletion
  - privacy-enhancing technologies

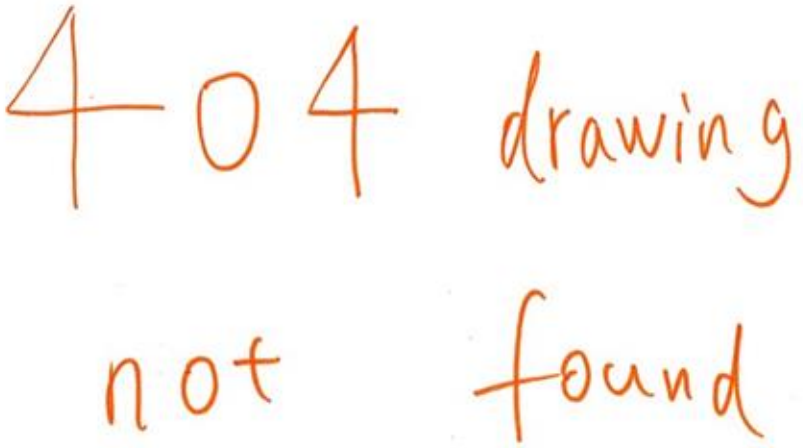
Internet Privacy



"On the Internet, nobody knows you're a dog."

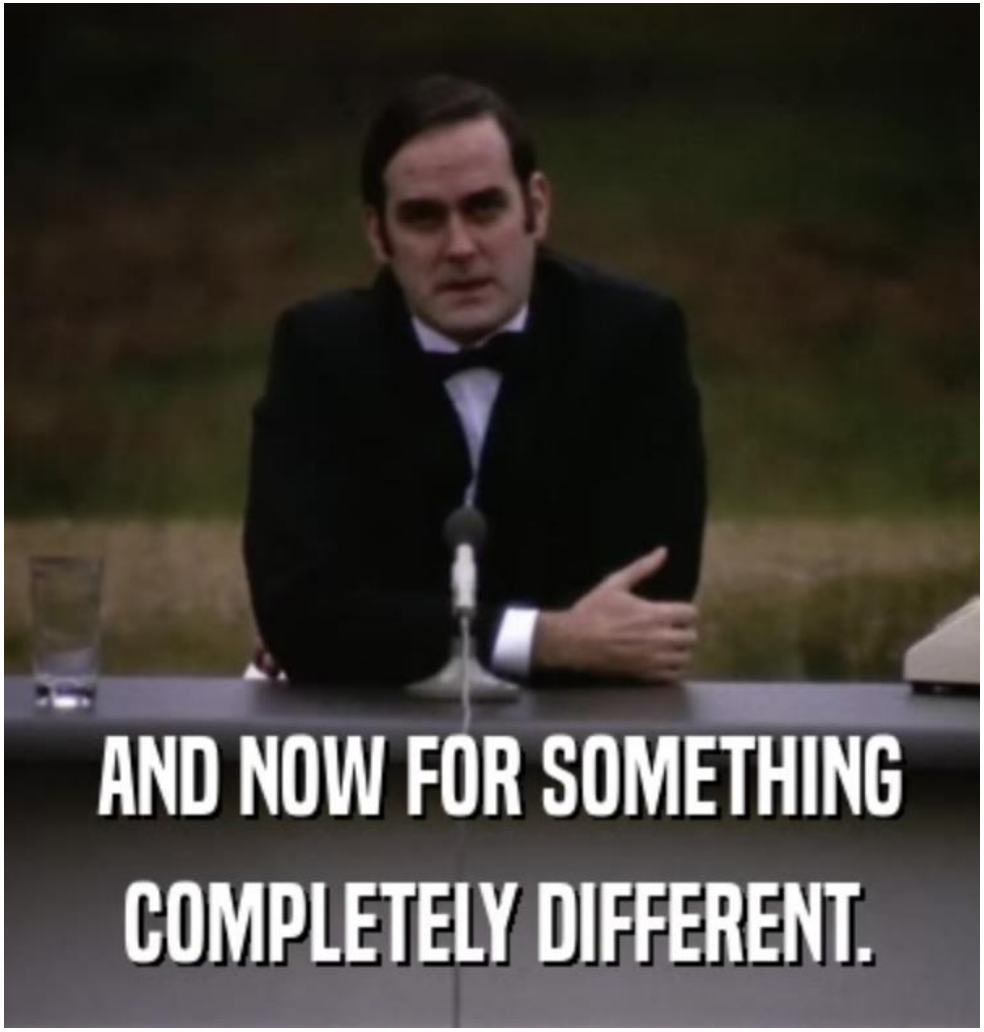
Internet Privacy





That's a private drawing and my idea is my privacy. :)

– XCY age 23


AND NOW FOR SOMETHING
COMPLETELY DIFFERENT.

Course Projects

Project Description

CS 138 students are expected to participate in a group project to build a software system that has non-trivial security functionality. A high-level introduction to the project is given in the project overview.

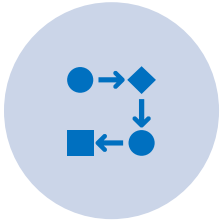
Project Milestones

Milestone	Description	Due Date
M0	Charter	**Tues February 10 at 11:59pm**
M1	Requirements	**Tues February 17 at 11:59pm**
M2	Prototype	**Tues March 10 at 11:59pm**
M3	Alpha Release	**Tues April 8 at 11:59pm**
M4	Beta Release	**Tues April 20 at 11:59pm**
M5	Gamma Release	**Tues April 28 at 11:59pm**
M6	Final Project Deadline	**Wednesday May 6 at 11:59pm**
	Final Presentations	**May 4 and May 6, in class**

Forming a group…

What system(s) are you exciting about building?

What skills/ experience do you bring to a group?



How challenging do you want your project to be?

How often/when are you available to meet?

What programming language do you want to use?