what software engineers should know about

# Privacy

17-313 Fall 2025

Foundations of Software Engineering

https://cmu-17313q.github.io

Eduardo Feo Flushing

Sources:

- Some slides adapted from CMU 17-437/637 Web Application Development
- *"What software engineers should know about privacy"*. MSE Seminar. Hana Habib. CMU
- *"Ethics, Fairness, Responsibility, and Privacy in Data Science"*. CMSC 25900. U. Chicago

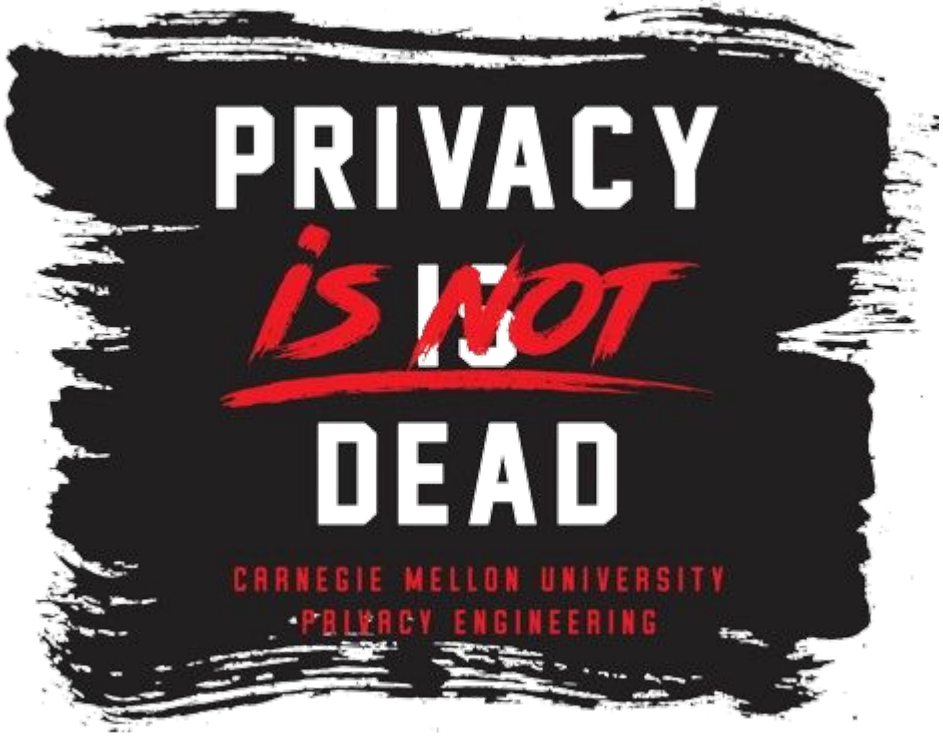
# Learning goals

- Explain why privacy is not dead
- Describe common privacy principles and techniques
- Differentiate privacy threats

# Smoking Section

- Last **two** full rows

# Privacy


PRIVACY
is NOT
DEAD
CARNEGIE MELLON UNIVERSITY
PRIVACY ENGINEERING

# Imagine …

- You are about to purchase a car insurance policy
- The insurance companies you request quotes from want to know more about you …

# How comfortable you are disclosing

- How many miles/year you drive
- How fast you drive
- Where you go and when
  - GPS
- How many hours you sleep at night
  - Based on information collected by your smartwatch
- Health history

# Observations

- Not everyone feels the same way about these issues
- Most people have concerns about at least a subset of these scenarios
  - We all care about privacy
- Today all this information is readily available and can be collected by mobile & IoT devices

# Concept of Privacy

- Moral right of individuals to **be left alone**, free from surveillance or interference from other individuals or organizations, including state

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

*"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, ... Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."*

**Warren and Brandeis, 1890**

# Information Privacy

- The claim that certain information should not be collected by government or businesses – or possibly under special circumstances (and special rules)
- There are **conflicting considerations**
  - Security and safety
  - Personalization
  - Productivity
- There are **ethical considerations**
  - Under what situations should **government and businesses** be allowed to intrude in the lives of **citizens/consumers**, after all?

# Is Privacy Dead?

## Facebook's Zuckerberg Says The Age of Privacy Is Over

By MARSHALL KIRKPATRICK of ReadWriteWeb
Published: January 10, 2010

PRINT

Facebook founder Mark Zuckerberg told a live audience yesterday that if he were to create Facebook again today, user information would by default be public, not private as it was for years until the company changed dramatically in December.

https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html

# Is Privacy Dead?

Forbes

LEADERSHIP

## Privacy Is Completely And Utterly Dead, And We Killed It

**Jacob Morgan** Contributor ⓘ
*I write about and explore the future of work!*

Follow

Aug 19, 2014, 12:04am EDT

Privacy...everyone keeps talking about it and apparently everyone is concerned with it, but going forward does it even matter? I recently watched the documentary, "Terms and Conditions may Apply," which provides a fascinating look at how organizations such as Facebook, Google , Apple , and others have changed the way they look at and approach privacy. After watching the movie it had me wondering, "does privacy even matter anymore?"

https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/

# Is Privacy Dead?

*“You have zero privacy anyway. Get over it.”*

Scott McNealy, Former CEO of Sun Microsystems (1999)

https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

# Is Privacy Dead?

*"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time... that information could be made available to the authorities."*

Eric Schmidt, Former CEO of Google (2009)

https://www.pcworld.com/article/515472/googles_schmidt_roasted_for_privacy_comments.html

# How Privacy is Protected

Laws, self-regulation, technology

- Notice and access
- Control over collection, use, deletion, sharing
- Collection limitation
- Use limitation
- Security and accountability

# US FTC's Fair Information Practice Principles

1. Notice/awareness (core principle)
    a. Disclose practices
2. Choice/consent (core principle)
    a. Opt-in, opt-out
3. Access/participation
    a. Users should be able to review & correct their information
4. Integrity/Security
    a. Ensure is secure, limited access
5. Enforcement
    a. Mechanisms for handling violations

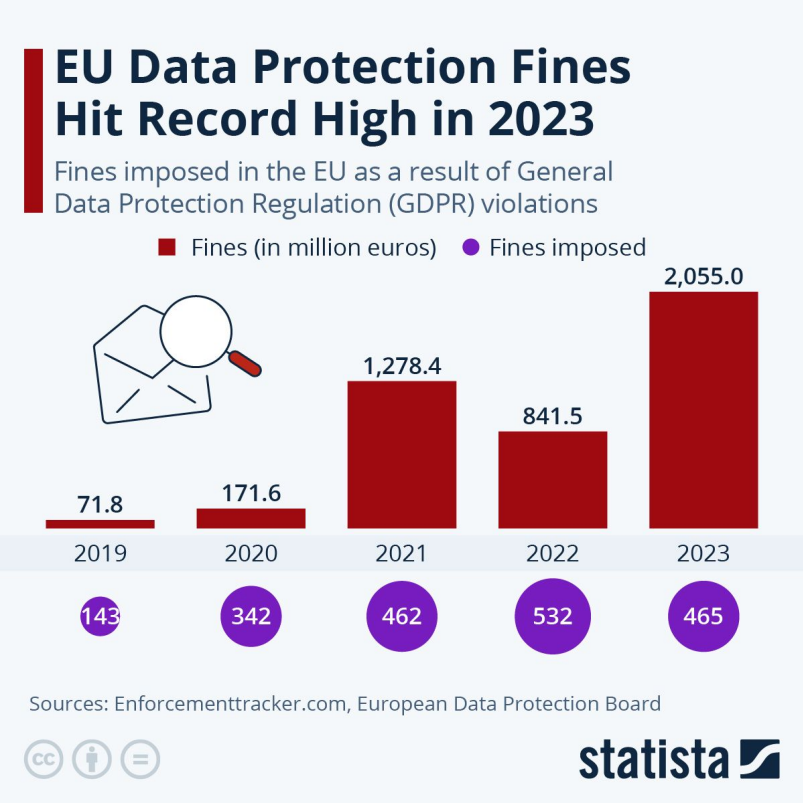
# OECD Fair Information Principles

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

# Why SWEs should care about privacy

- Ethical questions (next: **Ethics** lecture)
- Laws restricting data collection by government and agencies
  - Freedom of Information Act  (1966), Privacy Act (1974), Electronics and Communications Act (1986), ...
- Laws restricting data collection in different economic sectors
  - COPPA, HIPAA, FERPA, etc
- State Laws (e.g., CCPA) and local laws
- EU - General Data Protection Regulation

# Why SWEs should care about privacy



# Goals of Privacy Engineering

- Ensuring legal compliance
  - GDPR, CCPA, etc.
- Aligning with consumer expectations
  - Transparency about data practices
  - Accurate statements about privacy policies
- Building trust and goodwill
  - Commitment to protecting user data
- Competing on privacy protection
  - Privacy as core value
- Promoting privacy as a societal value
  - Safeguarding privacy rights and advocating for ethical data practices

# Mechanisms in Privacy Engineering

- Selective data collection
  - Purpose-driven, minimize amount of personal information
- Data minimization
  - De-identification, pseudonymization, anonymization
  - Remove sensitive data
- Data retention policies
- Cryptographic tools
  - Confidentiality
- Access controls and secure data storage
- Socio-technical processes and audits
- Privacy-by-design (PbD)
- **Threat modeling**

# Threat Modeling

- Applicable to both security and privacy
- A wide variety of possible security and privacy threats.
  - How can we organize our analysis?
- Basic idea: systematic methodology to identify possible threats and methods to mitigate these threats
- Approach: use a taxonomy  of possible threats

# LINDDUN Taxonomy of Privacy Threats


Source: linddun.org

# Group activity: Privacy Threat Identification

- Consider a university admissions system that manages the application process for prospective students, including collecting application materials, evaluating candidates, and making admissions decisions.
- In groups of 2-3, identify **two** privacy threats and propose ways to mitigate them

Faculty Course Evaluation (FCE)

TA Evaluation