What software engineers should know about

Privacy

17-313 Fall 2026

Foundations of Software Engineering

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

Administrivia

- **Great presentations yesterday, everyone, congratulations!** All teams did great.
- **P5B due Sunday, Dec 6** (finals week).
- **Exam 2:** sample midterms are posted on the course website. Some topics were covered on the old Exam 1.
- **Cheat sheet:** handwritten only, no AI (no template answers, etc.). Any indication of AI use on the cheat sheet will be considered an AIV.
- **Changing the exam date?** See next slide.

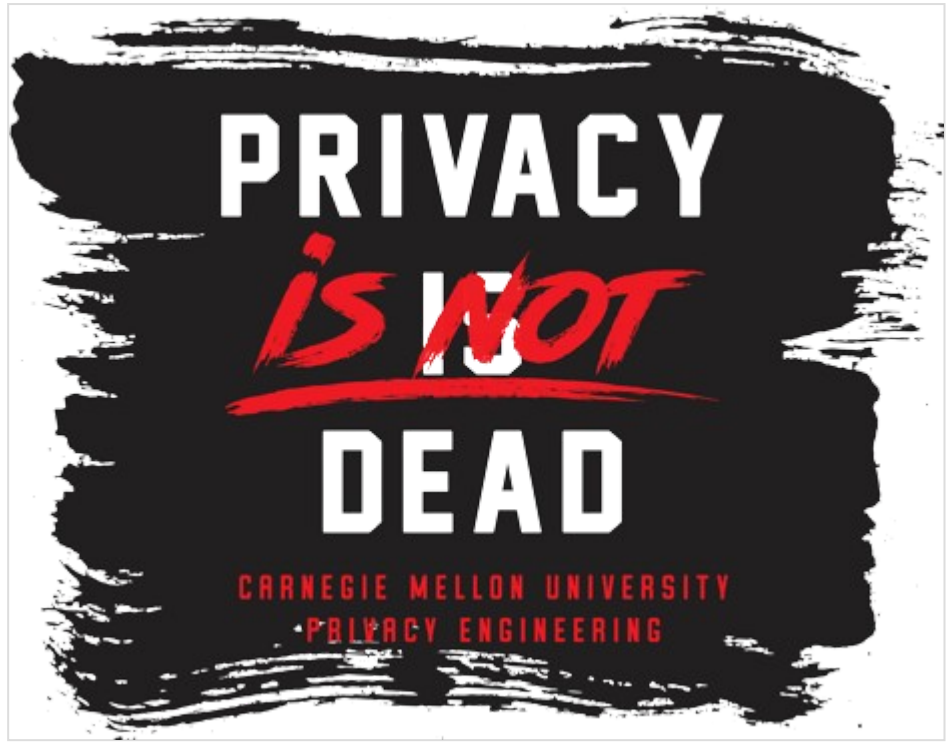
Learning Goals

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

Outline

- **Why Privacy Matters**
- Defining Privacy
- Is Privacy Dead?
- Privacy Principles
- Why Engineers Care
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- Wrap-Up

Privacy Is Not Dead



NOTES

This lecture is about the decisions software engineers make about personal data, not a legal survey. Despite frequent claims that "privacy is dead," specific concerns about personal data remain widespread.

Imagine…

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

NOTES

A running example used throughout this section: a car insurer wants more data about you to price a policy.

How Comfortable Are You Disclosing…?

- How many miles/year you drive.
- How fast you drive.
- Where you go and when (GPS / location).
- How many hours you sleep at night, based on your smartwatch.
- Your health history.

Which of these feel reasonable to share for an insurance quote, and which do not?

NOTES

This list moves deliberately from data that feels low-stakes (mileage) toward data that feels much more sensitive (health history). Most people don't draw an all-or-nothing line; they're comfortable sharing some of these and not others. That's the point: privacy judgments are about degree and context.

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 and IoT devices.

NOTES

The car-insurance exercise is evidence that privacy concerns are widespread even when people disagree on specifics, and that modern mobile and IoT devices make far more of this data collectible than most people realize. That combination, real concern plus real collectibility, is why privacy is an engineering problem.

Outline

- Why Privacy Matters
- **Defining Privacy**
- Is Privacy Dead?
- Privacy Principles
- Why Engineers Care
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- Wrap-Up

Concept of Privacy

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



HARVARD

LAW REVIEW.

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

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

WHAT the individual shall have, full protection in person and

"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

NOTES

Warren and Brandeis's 1890 Harvard Law Review article "The Right to Privacy" is considered one of the most influential law review articles ever written. They were responding to growing unease over new printing and photography technology making intrusions into private and family life possible for the first time.

Information Privacy

The claim that certain information should not be collected by government or businesses, or only under special circumstances and rules.

Conflicting considerations

- Security and safety.
- Personalization.
- Productivity.

Ethical considerations

Under what situations should government and businesses be allowed to intrude in the lives of citizens and consumers?

NOTES

Information privacy narrows Warren and Brandeis's "being left alone" to the collection and use of personal information specifically. Organizations have legitimate reasons to want data, including security and safety (fraud detection), personalization (recommendations, pricing), and productivity (fewer logins, faster checkout), so the right frame is a design tension. Underneath that tradeoff is an ethical question that recurs through the rest of this lecture: under what situations should governments and businesses be allowed to intrude into the lives of citizens and consumers?

Outline

- Why Privacy Matters
- Defining Privacy
- **Is Privacy Dead?**
- Privacy Principles
- Why Engineers Care
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- Wrap-Up

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.

NOTES

Facebook founder Mark Zuckerberg told a live audience in 2010 that if he were to create Facebook again, user information would by default be public, not private as it was for years until the company changed dramatically in December 2009.

archive.nytimes.com, Jan 10, 2010

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?"

NOTES

A 2014 Forbes column argues privacy is "completely and utterly dead," pointing to how companies like Facebook, Google, and Apple have changed how they approach user data.

forbes.com, Aug 19, 2014

Is Privacy Dead?

"You have zero privacy anyway. Get over it."

Scott McNealy, former CEO of Sun Microsystems (1999)

wired.com, Jan 1999

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)

NOTES

These four quotations and screenshots are presented as recurring examples of a claim people keep making, not as current news.

pcworld.com, Dec 2009

Outline

- Why Privacy Matters
- Defining Privacy
- Is Privacy Dead?
- **Privacy Principles**
- Why Engineers Care
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- Wrap-Up

How Privacy Is Protected

Laws, self-regulation, and technology.

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

These ideas recur, in different words, in real frameworks. Next: two of them, compared.

US FTC's Fair Information Practice Principles

One widely used framework for the ideas on the last slide, from the US Federal Trade Commission.

- **Notice/awareness** (core principle): disclose practices.
- **Choice/consent** (core principle): opt-in, opt-out.
- **Access/participation:** users should be able to review and correct their information.
- **Integrity/security:** ensure data is secure, with limited access.
- **Enforcement:** mechanisms for handling violations.

OECD Fair Information Principles

OECD: Organisation for Economic Co-operation and Development, an intergovernmental group of mostly high-income democracies that issued these privacy guidelines in 1980. Most principles overlap with FTC, with two notable additions (bold).

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

NOTES

The OECD and EU have adopted more comprehensive approaches to fair information practices than the FTC's. Individual participation gives people specific rights to access and correct their own personal data; accountability holds the data controller responsible for complying with these principles.

Outline

- Why Privacy Matters
- Defining Privacy
- Is Privacy Dead?
- Privacy Principles
- **Why Engineers Care**
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- Wrap-Up

Why SWEs Should Care About Privacy

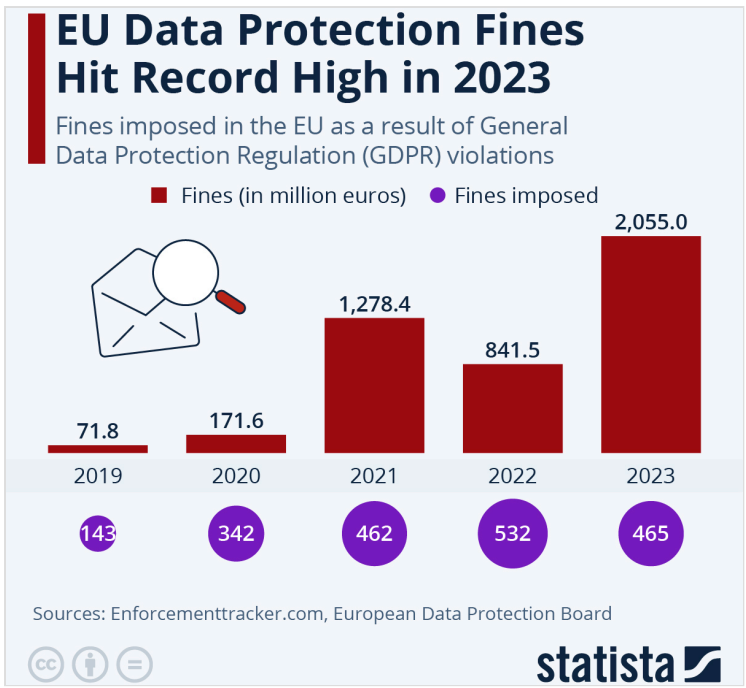
Ethical questions and legal rules across jurisdictions and sectors

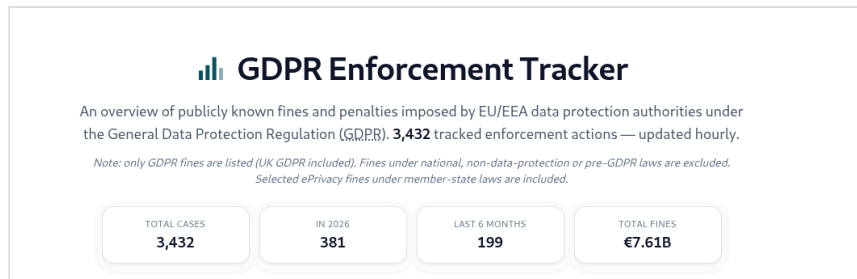
- **Laws restricting data collection by government agencies:** Privacy Act (1974), Electronic Communications Privacy Act (ECPA, 1986).
- **Laws restricting data collection in specific economic sectors:** COPPA, HIPAA, FERPA.
- **State and local laws:** e.g., CCPA (California).
- **EU:** General Data Protection Regulation (GDPR).

NOTES

These examples show that legal obligations around personal data span jurisdictions and sectors.

Why SWEs Should Care About Privacy





NOTES

On the left, a 2023 historical example of GDPR enforcement; on the right, the live enforcementtracker.com dashboard.

Source: Statista, Enforcementtracker.com, European Data Protection Board

Goals of Privacy Engineering

An established, emerging discipline within systems and software engineering: building privacy protections directly into systems, products, and data workflows

- **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:** privacy as a core value, a differentiator.
- **Promoting privacy as a societal value:** safeguarding privacy rights and advocating for ethical data practices.

Outline

- Why Privacy Matters
- Defining Privacy
- Is Privacy Dead?
- Privacy Principles
- Why Engineers Care
- **Mechanisms & Threat Modeling**
- Activity: Threat Identification
- Wrap-Up

Mechanisms in Privacy Engineering

- **Collect less:** purpose-driven, selective data collection; minimize what you gather in the first place.
- **De-identify what you do collect:** pseudonymization, anonymization. Pseudonymization alone does not guarantee anonymity: re-identification is often still possible.
- **Retention and deletion:** a separate design choice from collection and de-identification: how long is data kept, and when is it deleted?
- **Protect it:** cryptographic tools, access controls, secure data storage.
- **Check your decisions:** socio-technical audits, privacy-by-design (PbD).
- **Threat modeling:** systematically find what could still go wrong.

Threat Modeling

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

LINDDUN Taxonomy of Privacy Threats



NOTES

LINDDUN stands for Linking, Identifying, Non-repudiation, Detecting, Data disclosure, Unawareness and unintervenability, and Non-compliance. Example: an admissions API that lets outsiders test whether a named applicant has an account is a Detecting threat.

Source: linddun.org

Outline

- Why Privacy Matters
- Defining Privacy
- Is Privacy Dead?
- Privacy Principles
- Why Engineers Care
- Mechanisms & Threat Modeling
- **Activity: Threat Identification**
- Wrap-Up

Group Activity: Privacy Threat Identification

Consider a university admissions system that manages the application process for prospective students: collecting application materials, evaluating candidates, and making admissions decisions.

- In groups of 2-3, identify **two specific privacy threats**.
- Label each with a LINDDUN category where possible.
- Propose **one mitigation per threat**.



For reference

4 minutes

LINDDUN categories: linddun.org

Debrief: Possible Answers

Examples only. Other defensible threat/mitigation pairs are fine.

- **Document metadata reveals an applicant's identity** (Identifying / Data Disclosure). Mitigation: strip unnecessary metadata.
- **A registration response reveals that a named person already applied** (Detecting). Mitigation: avoid account-existence disclosures.
- **Logged access without a stated purpose, or access control that doesn't limit which employees can see personal data** (Non-compliance). Mitigation: enforce access control and data minimization.

Outline

- Why Privacy Matters
- Defining Privacy
- Is Privacy Dead?
- Privacy Principles
- Why Engineers Care
- Mechanisms & Threat Modeling
- Activity: Threat Identification
- **Wrap-Up**

Wrap-Up: What You Need to Know

- **Privacy is contextual:** willingness to share one kind of data for one purpose doesn’t imply willingness to share everything.
- **Principles guide concrete decisions:** the FTC’s and OECD’s frameworks turn "be careful with data" into specific commitments like notice, access, and accountability.
- **Mechanisms are distinct choices:** collecting less, de-identifying, retention/deletion, and security are separate levers
- **Threat modeling finds specific failures:** LINDDUN gives a vocabulary (linking, identifying, detecting, and more) for concrete mitigations.