**EEP 507 Introduction to Privacy Engineering**

***Summer 2025***

**Instructor:** Tamara Bonaci (t.bonaci@)

**Office hours:**

- After lectures and/or by appointment

**Course website:**

**Course assignment submission:**

**Course gradebook**:

**Course Piazza:**

## Course Overview:

You are an owner of a successful start-up, providing a service where your system continuously monitors various health and activity information about your customer, in order to better manage the customer's chronic health condition. Your business relies on cloud computing technologies, mobile devices, and recent developments in artificial intelligence.

As a part of your business, you collect throws of data about your customers. The data that you collect, mine and guard is valuable – without it, your business doesn't exist. However, the data is also highly sensitive (e.g., it consists of patients' biomedical, activity, location information, collected over an extended period of time)! So, even though you are only planning to use that data for legitimate purposes (and you are never planning to abuse it), you need to understand how such data may be misused, and by whom. More importantly, you need to understand what your responsibilities are, and what are technical approaches that you can implement in order to use the data only as intended.

This course surveys recent privacy approaches, applicable to various technical disciplines. In doing so, the course explores privacy threats arising from recent advancements in data mining and artificial intelligence. We will briefly discuss the history of privacy, and compare major privacy legal frameworks (such as GDPR and CCPA). We will then explore the phenomena of unravelling of privacy and inverse privacy. Next, we will survey several privacy design frameworks. We will then explore privacy-preserving techniques, such as anonymization, differential privacy, and polymorphic encryption.

## Course Goals:

By taking this course, the students will:

- Gain an appreciation for the importance of privacy in engineering.
- Learn about current research and tech policy efforts in the areas of privacy, privacy engineering and usable privacy.

- Learn how to collect, analyze and reconcile the diverse technological, business and tech policy aspects impacting how and why information is collected, managed, used and shared in some system.
- Evaluate system designs based on privacy principles, and privacy requirements.
- Learn how to integrate privacy into the engineering lifecycle phases.
- Work as a member of an interdisciplinary team, to address critical system requirements in a privacy-sensitive ecosystem.

## Course Outcomes:

Upon taking this course, students will:

- Be familiar with the different privacy aspects, applicable to diverse engineering systems.
- Develop critical thinking about the strengths and weaknesses of various privacy approaches and frameworks.
- Be able to implement different privacy paradigms, and embed them into various systems during both design and implementation phases.

## EEP 595, Summer 2025 – Course Logistics

**Lectures:** lecture slides, relevant reading and additional material will be made available in the following way:

  - Lecture notes and relevant reading material will be posted on Canvas, under the appropriate weekly module.
  - Pre-recorded video material (if available for the current module) will be posted on Canvas, under the appropriate weekly module.
- Every **xyz from 6:00-9:30pm PT,** we will meet ***on Zoom, using our recurring Zoom link, and in Electrical Engineering building, classroom xyz.*** Our lectures will focus on the outline weekly topics. Additionally, we will use lecture time to discuss weekly readings. We will do our best to record lectures, and make it available through Canvas + Panopto.

**Office hours:** After lectures, using the same UW Zoom link, or by appointment. **Office hours will not be recorded**, but may be attended by multiple students at the same time. If you would like to talk to me in private, please send me a note, and we can schedule a different time to meet.

**Classroom recordings:** This course, or parts of this course, may be recorded for educational purposes. These recordings will be made available only to students enrolled in the course, instructor of record, and any teaching assistants assigned to the course.

## Course Progression:

The following is a preliminary class progression covering 9 weeks of the course (June 26 – August 16). It is subject to changes.

**Week 1:**

**Lecture 1**: Course overview. Introduction to information security, privacy and usability.

**Week 2:**

**Lecture 2:** Foundations of privacy. Introduction to laws of computer technology.

**Week 3:**

**Lecture 3:** Introduction to privacy-preserving technologies. Introduction to anonymization.

**Week 4:**

**Lecture 4:** Static data anonymization – multidimensional data, time series data and graph data.

**Week 5:**

**Lecture 5:** Introduction to differential privacy.

**Week 6:**

**Lecture 6:** Differential privacy II.

**Week 7:**

**Lecture 7:** Privacy of health and biomedical data.

**Week 8:**

**Lecture 8:** Introduction to privacy preserving cryptographic methods and their applications. Gentle introduction to Zero Knowledge Proofs (ZKP), Secure Multiparty Computation (MPC), and Fully Homomorphic Encryption (FHE).

**Week 9:**

Project presentations.

## About the Course:

The course will consist of ***readings and discussion, labs and a project.***

***Readings and Discussion:***

Readings and discussions of assigned papers are an important part of this course. The goal of this exercise is to work together on understanding broader implications of the foundational privacy research. Additionally, we will also try to keep up with the state-of-the-art privacy research, with the focus on the recent privacy engineering work.

Every week, a single research paper will be assigned, and you will be expected to post to the class discussion board about it. Your post should contain something original beyond what others have already posted. You may consider posting:

- A summary of the paper,
- Evaluation of the paper's strengths and weaknesses,
- Open research question related to the topic of the paper, or
- Question you would like to discuss in class.

All posts are due by **11:59pm PT on a xyz,** and they will be graded on the scale of 0-2, where:

- 0 means missed or irrelevant post,
- 1 means a relevant post submitted, and
- 2 means a good and interesting post.

Post submitted after the deadline will receive no credit. There will be a total of 7 reading assignments, and we will take 5 best scores when determining your grade.

***Labs:***
We will have six Python-based lab assignments, intended to give you experience with some simple data mining and privacy engineering techniques. The labs will utilize publicly available data sets.

***Project:***
The final component of this course is a project, and its goal is to give you a deeper understanding of how to think about, and how to solve a real-life problem from a privacy-engineering perspective.

For the project, you will choose a topic related to any area of privacy and security (including those not directly covered in this course). You can work on the project either individually, or in groups of up to three persons. When working in a group, your end result should reflect the fact that it is a multi-person effort.

Your work on the project will consists of several milestones:
- Project pitch – due in Week 2,
- Project proposal – due in Week 3,
- Project update – due in Week 7
- Project presentation – due in week 9
- Final report – due in week 9

## Grading:
Your grade in this course will be based on readings and discussion, homework assignments, and project. The expected grade breakdown is:
- Readings and discussion – 20%
- Labs: 25%
- Project – 55%

## Course Material:
There is no required textbook for this course, but some recommended books that you might want to consider include:
- MITRE Privacy Engineering Framework, online: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive-enterprises/privacy-systems-engineering
- NIST, Privacy Engineering Program, online: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering
- NIST, An Introduction to Privacy Engineering and Risk Management in Federal Systems, online: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf
- Ian Oliver, Privacy Engineering: A Data Flow and Ontological Approach, 2014
- Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran: The Privacy Engineer's Manifesto, 2014
- Courtney Bowman, Ari Gesher, John K. Grant, Daniel Slate, and Elissa Lerner:

The Architecture of Privacy, O'Riley, 2015
- Woodraw Hartzog, Privacy Blueprint: The Battle To Control and Design New Technologies, Harvard University Press, 2018
- Helen Nissenbaum, Privacy in Context: Technology, Policy and Integrity of Social Life, Standford University Press, 2010
- Ari Ezra Weldman, Privacy as Trust, Information Privacy for an Information Age, Cambridge University Press, 2018

## Assignment Turn-In and Late Submission Policy:

**Collaboration:** In this course, we want you to learn from each other. Therefore, you are allowed (and encouraged!) to talk to your classmates and other students about all course assignments. You may also consult outside reference materials, and the instructor. ***However, all material that you decide to turn in should reflect your own understanding of the subject matter at the time of writing.*** This means that you should write your own posts about the assigned papers, and code up your own lab assignments, and prepare your own course project. If you work with someone else on any assignment, please include their names on the material that you turn in.

**Assignment Turn-in:** Posts about the assigned papers should be submitted using the Canvas discussion board. All other material (lab and project assignments) should be submitted using course website on Canvas. Please, ***do not use*** email for assignment submissions.

**Late Assignment Turn-in:** All assignments are due **by 11:59pm PT on the assigned date,** but we understand that you may have to sometimes turn them in late. The grading penalty is 5% of the grade that you would otherwise receive for each day, or part of the day, that you are late. No submissions will be accepted after two weeks.

**Checking grades:** Grades will be posted to the course gradebook.