# EE P __: INTRODUCTION TO PRIVACY ENGINEERING

Number of credits: 4 credits

Quarter and year: Summer 2023

Instructor's name: Tamara Bonaci

Email Address: tbonaci@uw.edu

## CATALOG COURSE DESCRIPTION

Explores privacy threats arising from advancements in data mining and artificial intelligence, the history of privacy, and major privacy legal frameworks (such as GDPR and CCPA). Covers topics such as unraveling of privacy and inverse privacy, privacy design frameworks, privacy-preserving techniques, such as anonymization, differential privacy, and polymorphic encryption.

## SUMMARY

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 unraveling 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 OBJECTIVES

By the end of this course, students will demonstrate the ability to:

- Understand the importance of privacy in engineering and the current research and tech policy efforts in the areas of privacy, privacy engineering and usable privacy.

- 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 and 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.
- Critically evaluate the strengths and weaknesses of various privacy approaches and frameworks.
- Implement different privacy paradigms, and embed them into various systems during both design and implementation phases

**COURSE SCHEDULE**

The following is a preliminary class progression covering 9 weeks of the course (June 21 – 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.

## 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/enterpriseengineering/engineering-informationintensive-enterprises/privacy-systemsengineering
- NIST, Privacy Engineering Program, online: https://www.nist.gov/itl/appliedcybersecurity/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, Stanford University Press, 2010
- Ari Ezra Weldman, Privacy as Trust, Information Privacy for an Information Age, Cambridge University Press, 2018

## COURSE ELEMENTS AND GRADING CRITERIA

**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 Wednesday, 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 8 reading assignments, and we will take 6 best scores when determining your grade.

**Labs:**

We will have five 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.

- Readings and discussion: 20%
- Labs: 25%
- Project: 55%

**COURSE FORMAT**

**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 Wednesday from 6:00-9:30 pm PT, we will meet in the Electrical Engineering building, classroom 269.
- 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.

## RELIGIOUS ACCOMMODATIONS

Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/).

## ACCOMMODATIONS AND ACCESS

If you have already established accommodations with Disability Resources for Students (DRS), please communicate your approved accommodations to me at your earliest convenience so we can discuss your needs in this course. If you have not yet established services through DRS, but have a temporary health condition or permanent disability that requires accommodations (conditions include but not limited to; mental health, attention-related, learning, vision, hearing, physical or health impacts), you are welcome to contact DRS at 206-543-8924 or uwdrs@uw.edu or disability.uw.edu. DRS offers resources and coordinates reasonable accommodations for students with disabilities and/or temporary health conditions. Reasonable accommodations are established through an interactive process between the student, instructor, and DRS. It is the policy and practice of the University of Washington to create inclusive and accessible learning environments consistent with federal and state law.

## ACADEMIC INTEGRITY

Engineering is a profession demanding a high level of personal honesty, integrity and responsibility. Therefore, it is essential that engineering students, in fulfillment of their academic requirements and in preparation to enter the engineering profession, adhere to the College of

Engineering Statement of Principles. Any student in this course suspected of academic misconduct (e.g., cheating, plagiarism, or falsification) will be reported to the College of Engineering Dean's Office and the University's Office of Community Standards and Student Conduct to initiate the student conduct process. Any student found to have committed academic misconduct may receive a zero for their grade on the impacted academic work (e.g., assignments, project, or exams), and academic consequences, with the possibility of expulsion

**TITLE IX**

"UW, through numerous policies, prohibits sex- and gender-based violence and harassment, and we expect students, faculty, and staff to act professionally and respectfully in all work, learning, and research environments. For support, resources, and reporting options related to sex- and gender-based violence or harassment, visit UW Title IX's webpage (https://www.washington.edu/titleix/), specifically the Know Your Rights & Resources guide (https://www.washington.edu/titleix/files/2020/08/KYRR-guide-8-10-2020-LINKED.pdf).

If you choose to disclose information to me about sex- or gender-based violence or harassment, I will connect you (or the person who experienced the conduct) with resources and individuals who can best provide support and options. You can also access those resources directly:

- Confidential: Confidential advocates (https://www.washington.edu/sexualassault/support/advocacy/) will not share information with others unless given express permission by the person who has experienced the harm or when required by law.
- Private and/or anonymous: SafeCampus (https://www.washington.edu/safecampus/) provides consultation and support and can connect you with additional resources if you want them. You can contact SafeCampus anonymously or share limited information when you call

Please note that some senior leaders and other specified employees have been identified as "Officials Required to Report." (https://www.washington.edu/titleix/title-ix-officials-required-to-report/) If an Official Required to Report learns of possible sex- or gender-based violence or harassment, they are required to call SafeCampus and report all the details they have in order to ensure that the person who experienced harm is offered support and reporting options (https://www.washington.edu/titleix/resources/)."