University of Maine
School of Computing and Information Science

Course Name: Introduction to Privacy in ML **Number:** COS578/478 **Semester:** Fall 2025
Classroom: TBD **Class Hours:** TBD

Instructor: Sepideh Ghanavati **Office:** Boardman Hall234 **Email:** sepideh.ghanavati@maine.edu
Instructor Office Hours: By appointment.

Catalogue Listing: Overview of the role of AI and Machine Learning in improving understanding of privacy concepts as well as learning how to develop privacy-preserving and fair data-intensive applications.

Reading Materials: A reading list is provided in another document. The instructor will include the required reading material from the list at the end of each lecture slide. The reading materials will be divided into mandatory and optional readings.

Textbook: There is no official textbook for this course. The following are good resources.

- C. Dwork and A. Roth. The Algorithmic Foundations of Differential Privacy. 2014.
- S. Vadhan. The Complexity of Differential Privacy. 2017
- K. Ligett, K. Nissim, V. Shmatikov, A. Smith, J. Ullman. Differential Privacy: From Theory to Practice. 7th Bar Ilan University Winter School on Cryptography 2017

Course Prerequisites: By permission.

Expected prior knowledge and skills: The successful student should have an introductory knowledge of software engineering and Machine Learning and proficiency in programming languages such as Python.

Course objectives:
This course covers algorithms and techniques to help design and develop privacy-preserving applications.

Course Topics: Information privacy Fundamentals, differential privacy and its variants, algorithmic tools for differential privacy, applications of differential privacy, and differential privacy in industry.

Learning objectives:

- Learn the fundamental concepts related to privacy and legal frameworks.
- Understand the challenges in the analysis of legal or policy text.
- Learn about algorithmic tools for differential privacy and its variants.
- Develop privacy-preserving systems.

Learning Outcomes & Assessment Methods: Students who complete this course should have the ability to:

Outcomes	Assessment Methods
1. Ability to analyze and model privacy and legal requirements	A, D, TP
2. Ability to discuss and evaluate policy texts.	CP, A, D, TP
3. Understand and implement algorithmic models and tools of privacy.	A, TP
4. Ability to develop privacy-preserving applications.	A, D, TP
5. Professionalism and ethics.	CP, A, D, TP
6. Working in groups and support teamwork.	CP and TP

Activities and Evaluation:

Students' performance will be evaluated based on class participation, assignments, and a project.

- **Lectures** – There will be 150 minutes of lectures every week, on Tuesdays and Thursdays, in which students will learn about topics in privacy and AI.
- **Readings** – Students will be assigned weekly readings from the academic papers on different aspects of privacy.
- **(CP) – Class Participation and Discord Discussion (10%) –** Students reflect on reading materials and discussions in the class as well as on the COS598 Discord channel. We discuss different subjects related to the course in class, and participation is required, either in class, on Discord, or both. Discussions are **individual** assessments.
- **(A) – Assignments (30%) –** Students will submit 3 take-home assignments whereby students apply methods taught in class to sample problems. The assignments will be either **individual** or **group** efforts, depending on the nature of the assignment. The instructor will announce the type in class. **Graduate students must complete this activity individually.**
- **(D) – Discussion Reports (15%) –** Throughout the semester, students will submit 5 or 6 discussion reports. The instructor will provide the students with case study discussions, papers, or news-related topics, and students are expected to write a 1 – 2 page report on the discussion topic. This is an **individual** assessment. **Graduate students must complete all of the six reports. For undergraduate students, the best five out of six will be counted.**
- **(TP) – Term Project (50%) –** Students will work on a project on a topic from the list given by the instructor. The details of the topics must be approved by the instructor by the deadline specified below. The aim of these projects is to delve into one of the emerging topics related to privacy and AI. The details of the project are given on Brightspace. **Graduate students must submit their work to the UMaine Student Symposium in Spring. For undergraduate students, this is optional.**
- **Attendance Policy** – Attendance is not directly mandatory in this course. The students are expected to watch the Zoom sessions if they cannot attend the class, and they must participate in discussions in class or on the COS478/578 Discord channel regularly to receive the class participation grades.

Note that the total possible grade in this class is 105%, which includes a 5% bonus mark.

Grading Policy:

The grading scale for the final mark is as follows:

Letter Grades	Numerical Range	Letter Grades	Numerical Range
A	95 – 100	**C**	74 - 76.99
A-	90 - 94.99	**C-**	70 - 73.99
B+	87 - 89.99	**D+**	67 - 69.99
B	84 - 86.99	**D**	64 - 66.99
B-	80 - 83.99	**D-**	60 - 63.99
C+	77 - 79.99	**F**	0 - 59.99

This scale may be curved to raise student grades at the instructor's discretion.

- Submitted work is due when specified. **With the instructor's permission and only in special cases**, you may be able to submit **TWO** days late (with a penalty). For every 12 hours of late submission, 10% marks will be deducted. That is, if you are late by two full days, a 40% mark will be deducted. After 48 hours, your assignment, project, and reports will be marked as 0, **with no exception.**
- Every submission must be done through Brightspace in a digital format. Submissions via email or in person will be marked as 0. If you encounter any problems with Brightspace, it is your own duty to inform the instructor **in a timely manner, before the due date**.

Course Schedule: The table (below) provides the initial distribution of topics discussed over the weeks in the semester. **This schedule is tentative and subject to change during the semester at the instruction discretion**. All changes will be announced in class or on the course website (Brightspace). Students are responsible for making sure they are informed about announcements.

Week	Class (TT)	Activity	Material
1	08/31	L0	Syllabus, Introduction and Academic Paper Writing
	09/02	L1	Introduction to Information Privacy
2	09/07	L2	Analysis of Privacy Regulations – **Project Topic Selection (Due Date)**
	09/09	L3	AI and Law – **Assignment 1 (Posted)**
3	09/14	L4	Database Privacy: Anonymization and De-Identification Paradigm
	09/16	L5	Reconstruction Attack I
	09/17	-	**Project Deliverable 0 (Due Date)**
4	09/21	L6	Reconstruction Attack II
	09/23	L7	Differential Privacy Fundamentals I
	09/24	-	**Assignment 1 (Due Date)**
5	09/28	L8	Differential Privacy Fundamentals II – **Assignment 2 (Posted)**
	09/30	L9	Differential Privacy Fundamentals III
	10/01	-	**Project Deliverable 1 (Due Date)**
6	10/05	L10	Advanced Composition
	10/07	L11	Exponential Mechanism and Report Noisy Max I
7	10/12	-	Fall Break
	10/14	L12	Exponential Mechanism and Report Noisy Max II
8	10/19	L13	Approximate Differential Privacy I
	10/21	L14	Approximate Differential Privacy II
	10/22	-	**Project Deliverable 2 (Due Date)**
9	10/26	L15	Differentially Private Empirical Risk Minimization I
	10/28	L16	Differentially Private Empirical Risk Minimization II
10	11/02	L17	Private Mean Estimation
	11/04	L18	Local Differential Privacy
	11/05	-	**Assignment 2 (Due Date)**
11	11/09	L19	Learning with Privacy – Privacy Gradient Descent I
	11/11	-	Veteran Day – **Assignment 3 (Posted)**
12	11/16	L20	Learning with Privacy – Privacy Gradient Descent II
	11/18	L21	Differential Privacy in Industry I
	11/21	-	**Discussion Report 3& 4**
13	11/23	L22	Differential Privacy in Industry II
	11/25	-	Thanksgiving Break
	11/28		**Project Deliverable 3 (Due Date)**
14	11/30	L23	Advanced Research in DP I
	12/02	L24	Advanced Research in DP II
	12/05	-	**Assignment 3 (Due Date)**
15	12/07	P1	Differential Privacy in Industry III
	12/08	-	**Project Presentations Slides and Videos**
	12/09	P2	Project Presentations
	12/11	-	**Discussion Report 5**
	12/12	-	**Project Deliverable 4 (Due Date)**

Academic Honesty Statement:

Academic honesty is very important. It is dishonest to cheat on exams, to copy term papers, to submit papers written by another person, to fake experimental results, or to copy or reword parts of books or articles into your own papers without appropriately citing the source. Students committing or aiding in any of these violations may be given failing grades for an assignment or for an entire course, at the discretion of the instructor. In addition to any academic action taken by an instructor, these violations are also subject to action under the University of Maine Student Conduct Code. The maximum possible sanction under the student conduct code is dismissal from the University. Please see the University of Maine System's Academic Integrity Policy listed in the Board Policy Manual as Policy 314 (***Date Issued:** September 1, 2020): https://www.maine.edu/board-of-trustees/policy-manual/section-314/

COVID-19 Return:

To keep our campus safe, students are expected to comply with all University policies related to the COVID-19 pandemic. For the latest guidance, please visit https://umaine.edu/return

The website address could be, alternatively, the system one: https://www.maine.edu/together/community-guidance/students/

Students Accessibility Services Statement:

If you have a disability for which you may be requesting an accommodation, please contact Student Accessibility Services, 121 East Annex, 581.2319, as early as possible in the term. Students who have already been approved for accommodations by SAS and have a current accommodation letter should meet with me, Dr. Sepideh Ghanavati, privately as soon as possible.

Course Schedule Disclaimer (Disruption Clause):

In the event of an extended disruption of normal classroom activities (due to COVID-19 or other long-term disruptions), the format for this course may be modified to enable its completion within its programmed time frame. In that event, you will be provided an addendum to the syllabus that will supersede this version.

UMaine Student Code of Conduct:

All students are expected to conform to the UMaine Student Code of Conduct.

Classroom Civility:

Civility should be conveyed to all others through courteous expression, politeness, esteem and regard for others, and a general respect for others, regardless of differences from self.

Inclusive and Non-Sexist Language:

The University of Maine, as an equal opportunity educational institution, is committed to both academic freedom and the fair treatment of all individuals. It therefore discourages the use of sexist language. Language that reinforces sexism can arise from imprecise word choices that may be interpreted as biased, discriminatory, or demeaning even if they are not intended to be. Accordingly, all University communications, whether delivered orally or in writing, shall be free of sexist language.

This policy shall apply to all future University publications, whether produced through Public Affairs or elsewhere, that are intended for distribution to students, parents, faculty, staff, or other people interested in the University of Maine. University publications shall include, but not necessarily be limited to: University printing office publications; promotional materials distributed by all units of the University both academic and nonacademic; and policy booklets prepared for students and faculty. Inventory on hand of existing publications may be used until exhausted or a publication is revised.

Each member of the University community is urged to be sensitive to the impact of language and to make a personal commitment to eliminate sexist language. Supervisory personnel have a particular responsibility to discuss this policy with faculty and staff and to make available to them guidelines on nonsexist language. Guidelines of the American Psychological Association on the use of nonsexist language provide direction and are recommended because they are brief and list examples, but others may be used. Consult the Communications and Marketing Department or Women's Gender and Sexuality Studies Program for alternatives (https://umaine.edu/womensgenderandsexualitystudies/) .

Observance of Religious Holidays/Events:
The University of Maine recognizes that when students are observing significant religious holidays, some may be unable to attend classes or labs, study, take tests, or work on other assignments. If they provide adequate notice (at least one week and longer if at all possible), these students are allowed to make up course requirements as long as this effort does not create an unreasonable burden upon the instructor, department or University. At the discretion of the instructor, such coursework could be due before or after the examination or assignment. No adverse or prejudicial effects shall result to a student's grade for the examination, study, or course requirement on the day of religious observance. The student shall not be marked absent from the class due to observing a significant religious holiday. In the case of an internship or clinical, students should refer to the applicable policy in place by the employer or site.

Sexual Discrimination Reporting:
The University of Maine is committed to making campus a safe place for students. Because of this commitment, if you tell a teacher about an experience of **sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct or any form of gender discrimination** involving members of the campus, **your teacher is required to report** this information to Title IX Student Services or the Office of Equal Opportunity.

If you want to talk in confidence to someone about an experience of sexual discrimination, please contact these resources:

For *confidential resources on campus*: **Counseling Center: 207-581-1392** or **Cutler Health Center: at 207-581-4000**.

For *confidential resources off campus*: **Rape Response Services:** 1-800-871-7741 or **Partners for Peace**: 1-800-863-9909.

Other resources: The resources listed below can offer support but may have to report the incident to others who can help:

For *support services on campus*: **Title IX Student Services: 207-581-1406**, **Office of Community Standards: 207-581-1409**, **University of Maine Police: 207-581-4040 or 911**. Or see the OSAVP website for a complete list of services.

Copyright Notice for Materials Accessible through this Website
Most materials accessible through this site, such as linked articles, should be assumed to be copyright protected.

1. Unless the "fair use" provisions of copyright law apply or language is contained in a work permitting its use, permission should be obtained from the copyright holder for copying the work.

2. Use of the instructor prepared web pages and the slides affiliated with each lecture on the syllabus may be assumed to be controlled by the University of Maine System Broad Application Copyleft License (proposed, current, or future) or through a similar license that may be posted at the bottom of each web page.
3. All class videos (lectures) should be assumed to be copyright protected in accordance with the University of Maine System Statement of Policy Governing Patents and Copyrights.

Contingency Plans in the Event of an Epidemic:

In the event of an influenza or similar epidemic that precludes the ability to meet in face-to-face sessions, assume that the instructor will either (1) host the course on our usual zoom url for the class at the normal time and everyone will participate at a distance or (2) record a video of the lecture I would have otherwise presented in person and post it for viewing by downloading from the syllabus and/or from a web streaming video site (example: recorded on zoom or recorded and then posted on the Spatial Information Science and Engineering YouTube Channel). All other reading and module assignments should proceed as usual. If you yourself become sick, simply inform the instructor and the instructor will arrange appropriate extensions based on your particular circumstances.