Instructor
Dr. Rachel Greenstadt
Department of Computer Science
Drexel University
Office: University Crossings 140
Tel: 1 215 895 2920
Email: greenie AT cs drexel edu
Office Hours: Wed 3:00-4:00 or by appt

Course Overview
This seminar course will motivate the need for privacy protection and introduce basic privacy properties such as anonymity, unlinkability or unobservability. We will then discuss how these properties can be formalized, modeled and measured. The course will provide a broad overview of the state-of-the-art in privacy technologies, explain the main issues that these technologies address, what the current solutions are able to achieve, and the remaining open problems. An excerpt of topics covered:

- Measuring privacy using information theory
- Data privacy threats and protection measures.
- Privacy and web mining.
- Privacy at the communications layer.
- Privacy and usability.
- Social media and its implications for electronic privacy.

Prerequisites
This is a graduate course, so students should be prepared to read papers and conduct research.

Coursework and Grading
This will be a seminar style course. It will mainly involve engaging with papers in the scientific literature (reading list) and working on a research project on some topic related to privacy enhancing technologies. Good projects will form the foundation for a research paper. The topic of the project and its parameters are to be determined through agreement between instructor and student. Please email me if you would like to schedule an in-person or phone meeting to discuss your project idea. Projects may be done individually or in teams of up to 2 people. If project is done in a team, all members will get the same grade. Single projects are expected to be as good as group projects.

A project proposal, final written report, and final presentation to the class will form the basis of the project grade. The project proposal will be due April 26. The project proposal is a document with a maximum 2 pages of text (I advise using a tight two-column paper formatting). Your references may take up an additional page. The proposal should have the following sections:

- Problem Statement and Motivation: What is the problem that you are solving? What is the research question you want to answer? Why is it relevant and interesting? Why would the results you are proposing to achieve be significant?
- Approach: How do you plan to go about solving this problem and answering this research question? What techniques/algorithms are involved? This section will vary highly based on the type of project you are proposing, but should convince me that you know what you're doing and that you have a plan for attacking the problem.
- Related Work and Novelty: What other research papers are closest to yours? This section should demonstrate that (1) you have explored the space in some detail and you know what's out there and (2) your work is a novel contribution.
- Evaluation Approach: How will you (and I) determine if your approach solves the problem? Negative results (demonstrating that an approach does not work) are acceptable here, provided that
the approach was promising. In research, we shouldn't always know how things will turn out. This can be either theoretical analysis or experimental results.

- **Milestones:** How will you get the work done? Present a timeline of what and when various work will be accomplished. If you are working in a group, discuss how the work will be divided. What is the simplest version of your project that you can absolutely promise will be done by the end of term? How do you hope to extend it if you have time?

- **Bibliography:** containing the references cited in your proposal

You may be asked to revise your proposal if I believe it will lead to an unsatisfactory final project. In this case, your proposal grade will be based on both the original and revised proposals. The proposal is what I will use to evaluate your final project. Minor deviations from it are okay, but any major changes need to be approved by me. If you are unsure if a change is ok, just ask. Near the end of term, students will present their work to the class in a 30-minute (including five minutes for questions) conference-style presentation. At the end of the term, students will submit a workshop-quality paper, 10-15 pages in length, describing their project. Below is the grading breakdown:

- Facilitation: 20%
- Project: 50%
- Class participation: 20%
- Lab Assignments: 10%

Each paper will be presented to the class by one student. The reading list can be found here. In-person students will give a 25-minute conference-style presentation. The student presenting the paper will then lead the class in a discussion of the paper, taking 70 minutes for the presentation and discussion in total for each paper. Online students will be expected to either attend and participate virtually in the discussion via wimba classroom (linked from bbvista) or watch the discussion and write a blog post reflecting on points raised in the class discussion.

All students should also submit presentation feedback forms (one for each of the presentations per class period) by midnight (11:59 pm) of the day following the class period. These forms will be made available (anonymously) to the presenter.

Online students will present their papers in either a blog post (approximately two pages long) or in a posted video presentation of 25 min. Blog posts should summarize the main ideas and results of the paper, assess the paper's significance, bring up discussion points, and link to related work. The author will then moderate a comment thread in which all students are expected to participate. Blog posts will be due the Friday before class at 5 pm.

Students will be expected to post comments on the blog by the Monday before class at 11:59 pm. Feedback forms for blog posts will be due by class time. (If the post is a video presentation, please use the form for presentations) These forms will be made available (anonymously) to the presenter.

The class participation grade will be determined by (1) Active participation in class discussions (2) Online discussion on the course blog and (3) feedback on class presentations and blog posts.

### Reading List

*(This list may change from year to year)*

- **Privacy Foundations**
  - 'I've Got Nothing to Hide’ and Other Misunderstandings of Privacy (local cached copy)
  - A Classification for Privacy Techniques (local cached copy)
    Carlisle Adams, University of Ottawa Law & Technology Journal 3, 2006

- **Engineering Privacy**
  - Engineering Privacy (local cached copy)

- **PETs for the Internet**
  - Privacy-enhancing Technologies for the Internet (local cached copy)
    Ian Goldberg, David Wagner, Eric Brewer, IEEE COMPCON 1997
- Privacy-enhancing technologies for the Internet, II: Five years later (local cached copy)
  Ian Goldberg, PET 2002
- Privacy-enhancing technologies for the Internet III: Ten years later (local cached copy)

- Anonymous and Pseudonymous Communication
  - Untraceable electronic mail, return addresses, and digital pseudonyms (local cached copy)
  - Towards an Information Theoretic Metric for Anonymity (local cached copy)
  - Tor: The Second-Generation Onion Router (local cached copy)
    Roger Dingledine, Nick Mathewson, Paul Syverson, USENIX Security 2004

- Data Privacy
  - Robust De-anonymization of Large Sparse Datasets. (local cached copy)

- Differential Privacy
  - An Ad Omnia Approach to Defining and Achieving Private Data Analysis, (local cached copy)
  - Mechanism Design via Differential Privacy (local cached copy)

- Privacy Policies
  - Why we can't be bothered to read privacy policies: models of privacy economics as a lemons market (local cached copy)
  - A Comparative Study of Online Privacy Policies and Formats(local cached copy)
    Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley and Lorrie Faith Cranor. PETS 2009.

- Privacy Economics
  - Privacy in Electronic Commerce and the Economics of Immediate Gratification (local cached copy)

- Web Privacy
  - An Analysis of Private Browsing Modes in Modern Browsers (local cached copy)
  - How Unique Is Your Web Browser?(local cached copy)
    Peter Eckersley, PETS 2010.

- P2P Privacy
  - The Sybil Attack (local cached copy)
  - Vanish: Increasing Data Privacy with Self-Destructing Data(local cached copy)
  - Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs(local cached copy)

- Social Network Privacy
- Understanding Privacy Settings in Facebook with an Audience View (local cached copy)
- To Join or not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles (local cached copy)