**New York University Tandon School of Engineering**
Computer Science and Engineering
Course Outline CS 9223 Privacy in the Electronic Society
**Spring 2020**
**Professor Greenstadt**

To contact professor:

Course Pre-requisites :
CS 6813 or Instructor approval

## Course Description

This seminar course will motivate the need for privacy protection and introduce privacy properties such as anonymity, differential privacy, and 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 and threats, explain the main issues that these technologies address, what current solutions are able to achieve, and the remaining open problems. An excerpt of topics covered: Data privacy threats and protection measures. Privacy and web mining. Privacy at the communications layer. Interpersonal privacy and social trust. Privacy and usability. Social media, mobile devices, and their implications for electronic privacy. Privacy and government surveillance. This will be a seminar style course. It will mainly involve engaging with papers in the scientific literature and working on a research project on some topic related to privacy enhancing technologies.

## Course Objectives

- Understand privacy properties and definitions
- Learn the state of the art in privacy enhancing technologies
- Learn to read and discuss privacy research papers
- Learn to conduct research in privacy

## Course Structure

This will be a seminar style course. It will mainly involve engaging with papers in the scientific literature and working on a research project on some topic related to privacy enhancing technologies. Each paper will be presented to the class by one student, who will give a 20-minute conference-style presentation. The student presenting the paper will then lead the class in a discussion of the paper. 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.

## Readings

The text will involve readings from the privacy literature. Links to the papers will be available on the course website.

Course requirements

25% of the grade will come from class participation, which is required when students do not have an excused absence. This grade will be split between (1) Attendance in class, (2) Participating in class discussions, and (3) Quizzes on the weekly readings.

Class facilitation [Due date varies] [25% of final grade]
[Students will be expected to lead assigned in class discussions (likely 2) and give a 20 minute presentation to kick off discussion ]

Project Proposal [Due Mar 11] [10% of final grade]

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 work has been done on this topic and how is it related to what you are trying to do? 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. Your proposal should have at least five references, cited properly (author, title, publication venue (conference or journal (if journal, give issue/number)), year).

Project Final Presentation [Due May 6] [10% of final grade]

Each group will present their work on the final day of class. Groups should choose one member of the group to give the presentation, though all members can contribute to answering questions from the class and myself. This is your opportunity to show off the work that you did. The presentation should be clear, engaging, and demonstrate your contributions. Think of it as an advertisement for your paper (But don't leave us in suspense—in general, suspense is a bad thing in research papers. Tell us what you did up front. I promise I'll read the whole thing). If appropriate, demo your project. I will inform you of the length of the presentations when I know how many projects there are.

Project Final Paper [Due May 6] [30% of final grade]
Papers must be a maximum of 6 pages and formatted in double-column 10 pt font. I suggest using laTeX, many conferences (AAAI, usenix, ACM, IEEE) provide appropriate templates. You should also provide a one-page or less document explaining how what you have done reflects or differs from your proposal.

The paper should contain:

. An abstract, summarizing your problem and results.

. An introduction, describing and motivating your problem. Spell out the research contributions here (remember, no suspense).

. A Background section. This should provide enough background on your topic for a fellow grad student who has taken cs680 (and did a project on an unrelated topic) to understand your paper. If your work is directly based on another piece of research, your should discuss that work here.

. Approach. Discuss your approach here in more detail than you did in the proposal. If I wanted to redo your project, I should be able to figure out how by reading this.

. Evaluation section. This is where you show me how you came to your conclusions. Detail your methodology, then give me the results. Explain the strengths and weaknesses of the approach.

. Related work. Basically the same as in the proposal, but add anything you've discovered since.

. Conclusions. What have you (and the reader) learned because of your project? Which part is most significant? Where could you (or someone else) take this work from here?

. A Bibliography, containing the referenced cited in your paper.

All projects are different. You may need additional sections or to present your work a little differently. We will be reading many papers this year in class (and you will be reading more on your project topic). These papers will give you an idea of the proper tone and organization of the paper.

**Schedule (Readings may be subject to change)**

**[2/3] Introduction and Syllabus**

**[2/10] Privacy Foundations**

- Daniel J. Solove 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy San Diego Law Review, Vol. 44, 2007
- Gordon Hull "Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2533057
- Helen Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review, Vol. 79, Number 1, 2005, https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr

**[2/17] Government Surveillance**

- *William Marczak and Vern Paxson (UC Berkeley)* Social Engineering Attacks on Government Opponents: Target Perspectives and Defenses, Proceedings on Privacy Enhancing Technologies, Volume 2017, Issue 2.

- Making Sense from Snowden, Susan Landau, IEEE Security and Privacy, Volume 11, Issue 4, July 2013. (also Part II, Susan Landau, IEEE Security and Privacy, Volume 12, Issue 1, January 2014.
- A Systematic Analysis of the Juniper Dual EC Incident, Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Makiewicz, Eric Rescorla, Hovav Schachm, and Ralf-Philipp Weinmann, ACM CCS 2016.

**[2/24] Tracking**

- Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, and Bart Preneel. "FPDetective: Dusting the Web for Fingerprinters". 2013 ACM Conference on Computer and Communications Security, November 2013. [PDF]
- Giridhari Venkatadri, Athanasios Andreou, Yabing Liu, Alan Mislove, Krishna P. Gummadi, Patrick Loiseau, and Oana Goga. "Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface". IEEE Symposium on Security and Privacy 2018. [PDF]
- Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, NarseoVallina-Rodriguez, and Serge Egelman. "“Won’t Somebody Think of the Children?” Examining COPPA Compliance at Scale". Proceedings on Privacy Enhancing Technologies 2018.3 [PDF]

**[3/3] Covid Privacy and Contact Tracing**

- Hargittai, E., Redmiles, E. M., Vitak, J., & Zimmer, M. (2020). Americans’ willingness to adopt a COVID-19 tracking app. *First Monday*, *25*(11). https://firstmonday.org/ojs/index.php/fm/article/view/11095/9985

- Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland. Marcel Salathé, Christian L. Althaus, Nanina Anderegg, Daniele Antonioli, Tala Ballouz, Edouard Bugnion, Srdjan Capkun, Dennis Jackson, Sang-Il Kim, James R. Larus, Nicola Low, Wouter Lueks, Dominik Menges, Cédric Moullet, Mathias Payer, Julien Riou, Theresa Stadler, Carmela Troncoso, Effy Vayena, Viktor von Wyl
- Decentralized Privacy-Preserving Proximity Tracing.Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Capkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, José Pereira. 2020.

## [3/10] Anonymity

- Roger Dingledine, Nick Mathewson, Paul Syverson , Tor: The Second-Generation Onion Router (local cached copy) , USENIX Security 2004.
- Characterizing the Nature and Dynamics of Tor Exit Blocking. Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, Vern Paxson. **USENIX Security 2017**
- Akshaya Mani, T Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. 2018. Understanding Tor Usage with Privacy-Preserving Measurement. In Proceedings of the Internet Measurement Conference. ACM. https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/tor-usage-imc18.18-1231-2064.pdf

## [3/17] Privacy Policies

- **Project Proposal DUE**
- The Privacy Policy Landscape After the GDPR: Thomas Linden, Rishabh Khandelwal, Hamza Harkous and Kassem Fawaz, Proceedings on Privacy Enhancing Technologies, Volume 2020, Issue 1
- Aleecia M. McDonald and Lorrie Faith Cranor ,The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf
- Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning". USENIX Security Symposium 2018 [PDF]

## [3/24] Differential Privacy

- Cynthia Dwork. An Ad Omnia Approach to Defining and Achieving Private Data Analysis. ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD (PinKDD 2007). [PDF]
- Using Apache Spark and Differential Privacy for Protecting the Privacy of the 2020 Census Respondents, at the Spark+AI virtual conference. [Video]

## [3/31] Internet Censorship and Collective Privacy Behavior

- Mending Wall: On the Implementation of Censorship in India (local cached copy) Devashish Gosain, Anshika Agarwal, Sahil Shekhawat, H. B. Acharya, Sambuddho Chakravarty, SecureComm 2017
- Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China (local cached copy) Jeffrey Knockel, Masashi Crete-Nishihata, Jason Q. Ng, Adam Senft, Jedidiah R. Crandall, FOCI 2015
- Aylin Caliskan, Jonathan Walsh, and Rachel Greenstadt, Privacy Detective: Detecting Private Information and Collective Privacy Behavior in a Large Social Network, Workshop on Privacy and the Electronic Society, 2014. https://www.cs.drexel.edu/~greenie/papers/wpes2014_privacy_detective.pdf

**[4/7] Privacy Mental Models and Censorship Circumvention**

- David Fifield, Threat modeling and circumvention of Internet censorship, PhD Thesis, UC Berkeley, 2017. https://www.bamsoftware.com/papers/thesis/info.html (presentation by two students)
- .Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration (local cached copy) Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, Lorrie Cranor, Proceedings on Privacy Enhancing Technologies 2018.4

**[4/14] Hot Topics in Privacy**

- .**The Many Kinds of Creepware Used for Interpersonal Attacks**, Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy, IEEE Symposium on Security & Privacy (Oakland), San Francisco, CA, May 2020
- Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. "Membership Inference Attacks against Machine Learning Models". IEEE Symposium on Security and Privacy 2017. [PDF]
- Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq., NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking, Proceedings on Privacy Enhancing Technologies ; 2018 (4):125–140 https://petsymposium.org/2018/files/papers/issue4/popets-2018-0035.pdf

**[4/21] Guest Lecture or TBA**

**[4/28] Guest Lecture or TBA**

**[5/5] Final Project Presentations**

- Final Project paper due

### Moses Center Statement of Disability

If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 3rd floor.

### NYU School of Engineering Policies and Procedures on Academic Misconduct – complete Student Code of Conduct is found here.

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

1. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.

2. Fabrication: including but not limited to, falsifying experimental data and/or citations.
3. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.
4. Unauthorized collaboration: working together on work meant to be done individually.
5. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.
6. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.

**NYU School of Engineering Policies and Procedures on Excused Absences – complete policy is found here with associated form:**

A. Introduction: An absence can be excused if you have missed no more than **10 days of school**. If an illness or special circumstance has caused you to miss more than two weeks of school, please refer to the section labeled Medical Leave of Absence.
B. Students may request special accommodations for an absence to be excused in the following cases:
    1. Medical reasons
    2. Death in immediate family
    3. Personal qualified emergencies (documentation must be provided)
    4. Religious Expression or Practice

Deanna Rayment, deanna.rayment@nyu.edu, is the Coordinator of Student Advocacy, Compliance and Student Affairs and handles excused absences. She is located in 5 MTC, LC240C and can assist you should it become necessary.

**NYU School of Engineering Academic Calendar – complete list is here:**

The last day of the final exam period is _____. Final exam dates for undergraduate courses will not be determined until later in the semester. Final exams for graduate courses will be held on the last day of class during the week of _____. If you have two final exams at the same time, report the conflict to your professors as soon as possible. Do not make any travel plans until the exam schedule is finalized.
Also, please pay attention to notable dates such as Add/Drop, Withdrawal, etc. For confirmation of dates or further information, please contact Susana M. Garcia-Henriquez at sgarcia@nyu.edu.