CS 5436 / INFO 5303: PRIVACY IN THE DIGITAL AGE

Instructors: Vitaly Shmatikov (CS), Helen Nissenbaum (IS)
TAs: Eugene Bagdasaryan (CS), Julia Len (CS)
Grader: Anam Tahir
Spring 2021: TTh 10:25-11:40 AM
Office hours: TBA

COURSE OVERVIEW

This course surveys the current state of digital privacy from multiple perspectives, including technology, philosophy, ethics, law, and policy. The course holds that privacy poses equally difficult challenges to technologists, policy makers, and ethicists. In order to make progress recognizing privacy threats, and protecting against them, representatives from all these domains must understand what privacy means in their respective domains as well as the mutual impacts of the domains on one another. The course will review key technologies , including web and mobile tracking, location tracking, privacy engineering, data analytics and differential privacy, facial recognition, and more. It will also introduce students to differing approaches to privacy, including technical, empirical, legal, and ethical. When addressing privacy threats in these areas, as well as potential solutions, the course sets out to pair a review of relevant technologies with a review of associated considerations in law and policy, ethics, and social sciences. Students will be expected to apply themselves to both the technical and nontechnical material with equal energy and enthusiasm.

LEARNING OUTCOMES

The class is oriented around the impact of digital technologies on privacy. Although the field is already much larger than any single semester-long class can cover, students enrolled in this class will gain insight into a range of the most significant contemporary digital systems that threaten privacy as well as those that have developed in response to such threats, aiming to protect and promote privacy. While instructors anticipate that the academic backgrounds and interests of enrolled students will differ, those who conscientiously perform technical readings, attend and participate in in-class lectures, and complete homework assignments will emerge with a solid working grasp of the respective technologies and a foundation, going forward, for developing deeper expertise in them.

Through assigned readings and in-class discussions students will gain insight into privacy as a philosophical and policy concept and an ethical value. They will appreciate why privacy is important to individuals, relationships, and societies and why it deserves protecting. The skills imparted in the philosophical and ethical dimensions of the course will enable students to identify practices and (socio-technical) systems that do and may compromise privacy, to identify circumstances where privacy conflicts with other rights and values, and how to reason about them. Assuming that students give full attention to the material in the philosophical and ethical aspects of the class, they will learn that reasoning well about these aspects demands both rigor

and precision. In moving back and forth between the technical and philosophical, they will develop a rare ability to map respective concepts onto one another and achieve a grasp of meaningful privacy.

PREREQUISITES

- Expert knowledge of Web and mobile technologies
- Knowledge of computer networking at the level of an undergraduate CS course
- Knowledge of algorithms at the level of an undergraduate CS course
- Familiarity with key machine learning techniques, especially deep learning
- Eagerness to devote energy and time to nontechnical material

COURSE MATERIALS

Course readings, required and recommended will be available in two ways: 1) as a download from the CANVAS website, or 2) through links given in the Course Schedule.

ASSIGNMENTS AND GRADING CRITERIA

We expect students to attend all classes and, beforehand, to have complete reading assignments thoroughly and with a critical eye. We encourage and will reward attendance and active participation during classes. Special note regarding Zoom: we expect students to attend classes with their video feed activated. If your circumstances do not allow for this on a given occasion, please reach out to instructors and we will evaluate case-by case. Over the course of the semester, we will assign five homework assignments, which include technical or nontechnical elements, or both.

Homework assignments (5): 60%
Attendance and participation: 20%
Take home exam: 20%

ACADEMIC INTEGRITY

We expect you to abide by Cornell’s Code of Academic Integrity at all times. Please note that the Code specifically states that a “Cornell student's submission of work for academic credit indicates that the work is the student's own. All outside assistance should be acknowledged, and the student's academic position truthfully reported at all times.” Please contact us if you have any questions or concerns about appropriately acknowledging others’ work in your submitted assignments. You should expect that we will rigorously enforce the Code.

WEEKLY SCHEDULE

Feb 9: Introduction

Readings:
"What They Know" series (WSJ).

Feb 11: Web Tracking and Online Advertising

Readings:
Mayer and Mitchell. "Third-Party Web Tracking: Policy and Technology".
Bashir and Wilson. "Diffusion of User Tracking Data in the Online Advertising Ecosystem".
Additional:
Englehardt and Narayanan. "Online Tracking: A 1-million-site Measurement and Analysis".
Acar et al. "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild".
Hoofnagle, Chris Jay, et al. "Behavioral advertising: The offer you can't refuse." *Harv. L. & Pol'y Rev.* 6 (2012): 273.
Faizullabhoy and Korolova. "Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions".

Feb 16: Cross-Device Tracking

Readings:
Brookman et al. "Cross-Device Tracking: Measurement and Disclosures".

Feb 18: Behavioral (Surveillance) Advertising

Readings:
Turow
Nadler and McGuigan
Optional:
Strandburg

Feb 23: Ethical and Philosophical Approaches to Privacy

Readings:
PIC Chapters 4 and 5
Optional:
Gavison, Ruth. "Privacy and the Limits of Law." *The Yale Law Journal* 89.3 (1980): 421.
Solove, Daniel J. "The meaning and value of privacy." *Social dimensions of privacy: Interdisciplinary perspectives* 71 (2015): 71.
Additional:
Cohen, Julie E. "Examined lives: Informational privacy and the subject as object." *Stan. L. Rev.* 52 (1999): 1373.

Feb 25: Mobile Tracking + Fingerprinting

Readings:
Forbrukerrådet. "Out of Control: How Consumers Are Exploited by the Online Advertising Industry".
Additional:
Reardon et al. "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System".

Mar 2: Location Privacy

Readings:
Martin, Kirsten E., and Helen Nissenbaum. "What Is It About Location?" Berkeley Technology Law Journal (2020): 103.

Mar 4: Puzzles and Paradoxes of "Standard" Definitions of Privacy

Readings:
PIC Chapter 6

Mar 9: No class / Wellness Day

Mar 11: Contextual Integrity (Part 1)

Readings:
PIC Chapter 7

Mar 16: End-2-end Secure Communication and "Going Dark"

Readings:
Abelson et al. "Keys under doormats: Mandating insecurity by requiring government access to all data and communications".
Additional:
Levy S. "Battle of the Clipper Chip," *The New York Times*, June 12, 1994
https://www.forbes.com/sites/zakdoffman/2020/03/14/new-warning-issued-for-all-whatsapp-and-imessage-users-major-threat-to-encryption/?sh=278febe153f5

Mar 18: Anonymity Networks and Censorship Resistance

Readings:
Dingledine et al. "Tor: The Second-Generation Onion Router".

Mar 23: Contextual Integrity (Part 2)

Readings:
PIC Chapter 8
Regan. "Privacy as a Common Good in the Digital World".

Mar 25: Anonymization

Readings:
Narayanan and Shmatikov. “Myths and Fallacies of ‘Personally Identifiable Information’.”
Ohm, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization." *UCLA l. Rev.* 57 (2009): 1701.

Mar 30: U.S. Legal Landscape

Readings:
Solove and Schwartz (2015), Privacy Law Fundamentals.
Warren and Brandeis.
Additional:
Prosser, W. "Privacy: A Legal Analysis’(1960)." *California Law Review* 48: 383.

Release homework #3 (due Apr 6)

Apr 1: Fourth Amendment
Guest: Salome Viljoen, DLI Postdoc Fellow

Readings:
Carpenter v. United States (EPIC amicus brief)
Farivar, C. *Habeas data: privacy vs. the rise of surveillance tech,* Melville House, (2018): 18-44.
Howe, A. "Opinion analysis: Court holds that police will generally need a warrant for sustained cellphone location information." *SCOTUS blog* (2018).
Additional:
Supreme Court of the United States . *Carpenter v. United States*. No. 16–402, 22 June 2018.
Justia. “Fourth Amendment of the US Constitution -- Search and Seizure.” *Justia*,https://law.justia.com/constitution/us/amendment-04/, Accessed 29 March 2021.

Apr 6: The Threat of “Big Data”

Readings:
Duhigg’s NYT article (incl. the Target story)
Barocas, Solon, and Helen Nissenbaum. "Big data’s end-run around anonymity and consent." In *Privacy, big data, and the public good: Frameworks for engagement,* Eds. J. Lane, V. Stodden, S. Bender, H. Nissenbaum, Cambridge: Cambridge University Press.(2014): 44-75.
Optional:

J. Shattuck. “Computer Matching is a Serious Threat to Individual Rights.” Communications of the ACM 27(6), June 1984, pp. 538-541.
R. Kuserow. “The Government Needs Computer Matching to Root Out Waste and Fraud.” Communications of the ACM 27(6), June 1984, pp. 542-545.
Additional:
Cohen, Julie E. "Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace, A." Conn. L. Rev. 28 (1995): 981.

Apr 8: Data Analytics and Differential Privacy

Readings:
Nissim et al. Differential Privacy: A Primer for a Non-technical Audience
Erlingsson et al. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response
Optional:
McSherry. “Privacy Integrated Queries” (CACM).
Additional:
Dwork et al. “Calibrating Noise to Sensitivity in Private Data Analysis”
McSherry. “Privacy Integrated Queries” (SIGMOD).

Apr 13: Privacy in Industry Settings
Guest: Paula Kift, Palantir EU Data Protection Lead

Apr 15: Empirical methods for studying privacy: Behavioral Economics
Guest: Laura Brandimarte, University of Arizona

Readings:
Hofstetter, Reto, Roland Rüppell, and Leslie K. John. "Temporary sharing prompts unrestrained disclosures that leave lasting negative impressions." *Proceedings of the National Academy of Sciences* 114.45 (2017): 11902-11907.
Optional:
John, Leslie K., Kate Barasz, and Michael I. Norton. "Hiding personal information reveals the worst." *Proceedings of the National Academy of Sciences* 113.4 (2016): 954-959.
Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and human behavior in the age of information." *Science* 347.6221 (2015): 509.

April 20: Privacy Policies

Readings:
United States Department of Health, Education & Welfare. 1973. *Records, Computers, and the Rights of Citizens*. Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, (Summary and Recommendations: pages 1-3).
J. Reidenberg, et. al. “Ambiguity in Privacy Policies and the Impact of Regulation

Release homework #4 (due Apr 29) -- 2 extra days due to “wellness break”

April 22: Privacy by Design (Ero Balsa)

Readings:
Seda Gürses, Carmela Troncoso, and Claudia Diaz. "Engineering privacy by design." Computers, Privacy & Data Protection 14.3 (2011): 25.
Optional:
Jaap-Henk Hoepman. "Privacy design strategies". In Proceedings of ICT systems security and privacy protection (IFIP SEC), pp. 446–459. Springer, 2014.

April 27: Privacy in Machine Learning + Federated Learning

Readings:
Shokri et al. "Membership Inference Attacks Against Machine Learning Models".
Carlini et al. Extracting training data from models.
McMahan et al. "Communication-Efficient Learning of Deep Networks from Decentralized Data".

April 29: Face Recognition and Biometrics Privacy

May 4: Xinru Page. Usable Privacy.

Readings:
Page, X. et. al., "Pragmatic Tool vs. Relational Hindrance: Exploring why Some Social Media Users Avoid Privacy Features" *PACM on Human-Computer Interaction*, Vol.3 No CSCW, Article 110, Publication date: November 2-19
Page, X. et. al., "Social Media and Privacy," In *Modern Socio-Technical Perspectives on Privacy*, Eds. Knijnenburg, B. et. al. (Forthcoming)

May 6: Vinay Goel and Michael Kleber

Release homework #5 (due May 13)

May 11: Genomic Privacy

Readings:
Gymrek et al. "Identifying Personal Genomes by Surname Inference".
Alondra Nelson: Watch this lecture (start at minute 13)
https://www.youtube.com/watch?v=giiXWtBdVFc&feature=youtu.be&t=780
Optional:
Barocas, Solon, and Karen Levy. "Privacy Dependencies." *Washington Law Review*

May 13: Smart Home: Voice Assistants (Alexa), Security Cameras (Ring), Smart TVs

Exercise on ambient recording
Reading: https://people.eecs.berkeley.edu/~daw/papers/listen-nspw19.pdf

Apthorpe's paper on privacy and IoT

Release take-home final (due May 18)

Leftover topics

Privacy Engineering in Industry
Differential Privacy in Industry (Miguel Guevara @ Google)
Google/Apple Covid exposure APIs (privacy by design) + Covid-related surveillance

Leftover readings

- Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30.1 (2015): 75.
- Regan, Priscilla M. Legislating privacy: Technology, social values, and public policy. Univ of North Carolina Press, 2000.