CS 5436 / INFO 5303: PRIVACY IN THE DIGITAL AGE

Instructors: Vitaly Shmatikov (CS), Helen Nissenbaum (IS)
TAs: Madiha Choksi, Eugene Bagdasaryan (½)
Spring 2022: TTh 11:25a-12:40p

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 FOR THE CS SECTION

- 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 time and energy to non-technical material

PREREQUISITES FOR THE INFO SECTION

- Undergraduate-level coursework in one or more of the following: social science, philosophy, ethics
- Ability to program
- Familiarity with Web and mobile technologies
- Introductory-level understanding of computer networking and machine learning

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 (4): 72%
Take-home exam: 18%
Attendance and participation: 10%

SPECIAL NOTE ABOUT HOMEWORK AND FINAL:
Because the study of privacy benefits from different disciplinary perspectives, we are trying something new this semester to accommodate a broader range of backgrounds of Cornell Tech students.

- All students are expected to attend all lectures and complete all reading assignments, except where indicated
- All homework assignments will include questions for all students, plus a few different questions designed for those enrolled in IS 5303 and CS 5436, respectively

- Final exam will include questions for all students, plus different questions designed for those enrolled in IS 5303 and CS 5436, respectively

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.

SPRING 2022 SCHEDULE

Jan 25: Course Overview

Readings:
Cyphers and Gebhart. "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance".
Optional:
Christl. “Corporate Surveillance in Everyday Life”.

Jan 27: Web Tracking and Online Advertising

Readings:
Mayer and Mitchell. "Third-Party Web Tracking: Policy and Technology".
Narayanan and Reisman. “The Princeton Web Transparency and Accountability Project”.
Optional:
Acar et al. “No Boundaries: Data Exfiltration by Third Parties Embedded on Web Pages”.
Bashir and Wilson. "Diffusion of User Tracking Data in the Online Advertising Ecosystem".
Additional:
Acar et al. “The Web Never Forgets: Persistent Tracking Mechanisms in the Wild”.
Faizullabhoy and Korolova. “Facebook’s Advertising Platform: New Attack Vectors and the Need for Interventions”.

Feb 1: Cross-Device Tracking

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

Feb 3: 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”.

Feb 8: Ethical and Philosophical Approaches to Privacy

Readings:
PIC Chapters 4 and 5.
Optional:
Gavison. "Privacy and the Limits of Law". *The Yale Law Journal* 89.3 (1980): 421.

Solove. "The meaning and value of privacy". *Social dimensions of privacy: Interdisciplinary perspectives* 71 (2015): 71.
Citron and Solove. “Privacy Harms”. 102 B.U L. Rev. (forthcoming 2022).
Additional:
Cohen. "Examined lives: Informational privacy and the subject as object". *Stan. L. Rev.* 52 (1999): 1373.

Feb 10: Puzzles and Paradoxes of “Standard” Definitions of Privacy

Readings:
PIC Chapter 6.

Feb 15: Contextual Integrity (Part 1)

Readings:
PIC Chapter 7.

Release homework #1 (due Feb 22)

Feb 17: Location Privacy

Optional for CS:
Martin and Nissenbaum. "What Is It About Location?" Berkeley Technology Law Journal (2020): 103.

Feb 22: 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).
Reidenberg et. al. “Ambiguity in Privacy Policies and the Impact of Regulation”.
Optional:
Shvartzshnaider et. al. “Going against the appropriate flow: A Contextual Integrity approach to analyzing privacy policies”.

Feb 24: Contextual Integrity (Part 2)

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

Mar 3: Behavioral (Surveillance) Advertising – Lee McGuigan

Readings:
Christl. “Corporate Surveillance in Everyday Life”.
McStay. “Micro-Moments, Liquidity, Intimacy and Automation: Developments in Programmatic Ad-tech: Information or Disinformation?”.
Van der Vlist and Helmond. “How partners mediate platform power: Mapping business and data partnerships in the social media ecosystem”.
Optional:
Strandburg. “Free Fall: The Online Market’s Consumer Preference Disconnect”.
Additional:
Hoofnagle et al. "Behavioral advertising: The offer you can't refuse". Harv. L. & Pol'y Rev. 6 (2012): 273.

March 8: End-2-end Secure Communication and “Going Dark”

Readings:
Abelson et al. “Bugs in our Pockets: The Risks of Client-Side Scanning”.
Additional:
Abelson et al. “Keys under doormats: Mandating insecurity by requiring government access to all data and communications”.
Levy. “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 10: Anonymity Networks and Censorship Resistance

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

Release homework #2 (due March 23)

Mar 15: U.S. Legal Landscape

Readings:
Solove and Schwartz (2015). Privacy Law Fundamentals.
Warren and Brandeis (1894). The Right to Privacy.
Additional:
Prosser. "Privacy: A Legal Analysis’(1960)". *California Law Review* 48: 383.

Mar 17: GDPR – Elettra Bietti

Readings:

Hoofnagle et al. "The European Union General Data Protection Regulation: What It is and What It Means". 28 Information & Communications Technology Law 65 (2019).

Optional:

Purtova. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law". 10(1) Law, Innovation and Technology (2018)

Mar 22: The Fourth Amendment – Sunoo Park

Readings:

U.S. Constitution Amendment IV.

"The Fourth Amendment in the Digital Age". Brennan Center Report (March 2021) -- pages 1-11.

Goitein. "How the FBI Violated the Privacy Rights of Tens of Thousands of Americans". Brennan Center Analysis (October 2019).

Additional:

Justia. "Fourth Amendment of the US Constitution -- Search and Seizure".

Supreme Court of the United States . *Carpenter v. United States*. No. 16–402, 22 June 2018.

Carpenter v. United States (EPIC amicus brief).

Farivar. "Habeas data: privacy vs. the rise of surveillance tech". Melville House, (2018): 18-44.

Howe. "Opinion analysis: Court holds that police will generally need a warrant for sustained cellphone location information". *SCOTUS blog* (2018).

Mar 24: The Threat of "Big Data"

Readings:

Barocas and 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.

Duhigg. "How Companies Learn Your Secrets" (NYT).

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.

Mar 29: Anonymization

Readings:

Narayanan and Shmatikov. "Myths and Fallacies of 'Personally Identifiable Information'".

Ohm. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". *UCLA l. Rev.* 57 (2009): 1701.
Optional:
Narayanan and Shmatikov. “Robust De-anonymization of the Netflix Prize Dataset”.

Mar 31: Data Analytics and Differential Privacy

Readings:
Nissim et al. Differential Privacy: A Primer for a Non-technical Audience.
Lee. Why the 2020 census has 9 fake people in a single house.
Optional for INFO:
Erlingsson et al. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response.
Optional:
Garfinkel. Differential Privacy and the 2020 US Census.
Additional:
McSherry. “Privacy Integrated Queries” (CACM).
McSherry. “Privacy Integrated Queries” (SIGMOD).
Dwork et al. “Calibrating Noise to Sensitivity in Private Data Analysis”.

Apr 12: HCI/design – Nathan Malkin

Release homework #3 (due April 26)

April 14: Standards – Nick Doty

April 19: Secure Multi-Party Computation and Privacy-Preserving Ad Attribution

Readings:
Corrigan-Gibbs and Boneh. “Prio: Private, Robust, and Scalable Computation of Aggregate Statistics”.
Taubeneck et al. “Interoperable Private Attribution”.

April 21: Biometrics and Face Recognition

Additional:
Hartzog and Selinger. “Facial Recognition Is the Perfect Tool for Oppression”.
Harwell and Timberg. “How America’s Surveillance Networks Helped the FBI Catch the Capitol Mob”.

April 26: Genomic Privacy

Readings:
Gymrek et al. “Identifying Personal Genomes by Surname Inference”.
Alondra Nelson. “The Social Life of DNA and the Need for a New Bioethics” (start at minute 13).

Optional:
Erlich and Narayanan. "Routes For Breaching and Protecting Genetic Privacy".
Additional:
Barocas and Levy. "Privacy Dependencies." *Washington Law Review.*

April 28: Privacy in Machine Learning

Readings:
Shokri et al. "Membership Inference Attacks Against Machine Learning Models".
Carlini et al. "Extracting Training Data from Large Language Models".

Release homework #4 (due May 10)

May 3: Federated Learning at Google – Peter Kairouz, Zheng Su, Hugo Song

McMahan et al. "Communication-Efficient Learning of Deep Networks from Decentralized Data".
Bonawitz et al. "Federated Learning and Privacy".
McMahan and Thakurta. "Federated Learning with Formal Differential Privacy Guarantees".

May 6 (Helen out): 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

May 10 (Vitaly out?): ???

No deliverables: Apr 15, 22-23, May 5-6, 11-13

Release take-home final (due May 14?)

Leftover topics

Privacy Engineering (2021: 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.

Behavioral Economics / Empirical Methods (2021: Laura Brandimarte)

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.

Usable Privacy (2021: Xinru Page)

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)

Privacy engineering in industry (Brave? Apple? DuckDuckGo?)

Differential privacy in industry (Miguel Guevara @ Google)

Google/Apple Covid exposure APIs (privacy by design) + Covid-related surveillance

Other Spring 2021 external speakers

Paula Kift: GDPR

Salome Viljoen: 4th Amendment

<u>Leftover readings</u>

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.