**DHP-P237/COMP-0150: Privacy in the Digital Age**

**Spring 2020: M 3:20pm-5:20pm**

Prof. Josephine Wolff (josephine.wolff@tufts.edu)
Office hours: M 12:30-2pm & W 11am-12:30pm (Mugar 252-E)

**Course Description**

This course will study the threats to and protections for privacy in the digital age, examining public and private sector threats from an international perspective. We will examine several broad themes relating to privacy, including: Who cares about privacy in which contexts and why? How are ideas about privacy different in different cultures, and do those ideas change over time? How do anonymity and security relate to privacy? How do we weigh positive and negative consequences of privacy-protecting technologies? How should we understand the choices people make about their privacy online? Topics to be covered include encryption policy, privacy threat models, location tracking and first- and third-party collection by private parties, government threats to privacy, and privacy preserving technologies. The course will include a mixture of technical and policy material, but students are not required to have any computer science background to take the course, just a willingness to engage with some technical material related to encryption and Internet architecture.

**Required Text**


**Course Schedule**

**Tuesday, Jan. 21 (Monday schedule): Introduction**

• What do we mean by “privacy“?
• Where and how can privacy protections be implemented at different places in the Internet’s architecture?
• How does privacy relate to issues of security and anonymity?
• How do the Internet and ubiquitous personal computing change ideas about privacy?

Readings: None

**Monday, Jan. 27: Privacy as a Right**

• What legal protections exist around the world for privacy as a human right?
• Where do ideas about the legal status of privacy come from and how are they interpreted in different countries and contexts?
• Does privacy matter even if we have “nothing to hide“?

Readings:

• Landau, *Listening In*, Preface and Chapter 1.

In-Class Debate #1: Should Apple keep a copy of the decryption key for every iPhone stored on its servers?

- What is public key encryption?
- How did governments around the world react to encryption technologies in the 1990s and early 2000s?

Readings:

- Landau, Listening In, chapters 2 and 3.
- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L.


Monday, Feb. 10: Encryption Policy, Part II (2016-2020) & Compelled Decryption

- What is end-to-end encryption?
- How have countries shifted their stance on encryption in the past five years?
- Which specific issues and incidents have changed the tenor of debates on encryption and how?
- What capabilities and legal authorities does law enforcement have to compel individuals to decrypt their own devices?

Readings:

Assignment #1: Encryption Memo (Due by 3:20pm on Monday, Feb. 17)

Governments around the world have been grappling with the question of how—and if—encryption should be regulated for more than two decades. Pick a country that has enacted, or considered enacting, some type of policy with regard to encryption and write a 3-4 page (double-spaced) memo summarizing (1) how the encryption debate has evolved in that country since the mid-1990 and whether the motivations and arguments on each side have changed, (2) where encryption policy currently stands in the country of your choice, and (3) what important future policy decisions the country will have to make with regard to encryption.

Monday, Feb. 17: Communications Interception for Law Enforcement

In-Class Debate #2: Should the United States government be able to use warrants to seize data stored in other countries by U.S. persons through data centers owned by companies headquartered in the United States?

- How do law enforcement entities access and intercept digital communications?
- What do the Fourth Amendment and the Electronic Communications Privacy Act (ECPA) protect, and what is “third-party doctrine” in the United States?
- How do mutual legal assistance treaties (MLATs) and the Clarifying Lawful Overseas Use of Data (CLOUD) Act enable law enforcement to access data stored in other countries?

Readings:

- Listening In, chapter 5.
- “ECPA: Background,” Electronic Privacy Information Center. Available from https://epic.org/privacy/ecpa/#background (Links to an external site.).
Monday, Feb. 24: Communications Interception for Intelligence

- How do intelligence agencies access and intercept digital communications?
- What legal authorities for collecting digital communications are granted to intelligence agencies through FISA, the PATRIOT Act, and Executive Order 12333?
- What can we learn from the Snowden leaks about classified surveillance programs?

Readings:

- Listening In, chapter 6.

Monday, March 2: Corporate Surveillance & Online Advertising

In-Class Debate #3: Has the GDPR significantly improved the state of Internet users’ privacy?

- What restrictions are placed on private companies collecting, processing and selling personal information?
- What protections does the European General Data Protection Regulation provide to individuals?
- How is personal data collected by companies used and what can be learned from it?

Readings:


• Ben Wolford, “What is GDPR, the EU’s new data protection law?” GDPR.EU. Available from https://gdpr.eu/what-is-gdpr/ (Links to an external site.).


Assignment #2: Surveillance Memo (Due by 3:20pm on Monday, March 9)

Option #1: Select one of the documents leaked by Edward Snowden regarding a digital surveillance program and do a close analysis of it in a 3-4 page (double-spaced) memo. For a searchable archive of many of the leaked documents, see: https://www.cjfe.org/snowden (Links to an external site.). To the extent possible, describe (1) what the program does, what kind of data it collected, from whom, and for how long, (2) what legal authority or policy was used to authorize the program, (3) what technical capabilities enabled the program, (4) any privacy concerns or issues raised by the program. If you select a document that does not include all of these details, that is OK—do as much as you can with the material.

Option #2: Download all of your data from one of the following companies: Apple, Amazon, Facebook, Google, or Snapchat (if you don’t have an account with any of these companies, pick a different prompt… this one won’t be very interesting). Write a 3-4 page (double-spaced) reflection on (1) what, if anything, surprised you in the information you receive; what did you learn about yourself? (2) how you think the information you receive could be, or is being, used by that company or its partners, and (3) what value, if any, you think there is in being able to download all of your own data from this company.

Option #3: Pick a company with a data privacy policy and write a 3-4 page (double-spaced) memo analyzing that policy. Include some discussion of (1) what types of data the company may collect based on its function, (2) what types of analysis it may be able to do with that data, (3) any self-imposed restrictions on what it does with collected data or whom it shares that data with, and (4) any capabilities granted to individual users to provide them with more autonomy or control over their data.
Monday, March 9: Identity, Biometrics & Anonymity

In-Class Debate #4: Should India abandon its Aadhaar biometric system and delete all collected biometrics because it causes more harm than good?

- How do governments around the world use digital technologies and biometrics for identifying online users?
- How effective are anonymization measures intended to protect individuals’ privacy?

Readings:


Monday, March 16 — NO CLASS (Spring Break)

Assignment #3: Final Paper Proposal (Due by 3:20pm on Monday, March 23)

Write a 3-4 page (double-spaced) proposal for your final research paper looking at a specific topic related to digital privacy in depth, using primary sources or data sets of your choosing. Your proposal should include (1) the central research question your paper will address, (2) the motivation and brief context for answering this question, (3) a detailed description of the primary sources and/or data you will use to answer this question (these could be anything from legal rulings or regulatory orders to technical data sets, government memos or reports, transcripts of legislative hearings or court arguments, original interviews you plan to conduct, etc., anything that is not just second-hand reporting on an issue from journalists or other researchers), and (4) a description of how you will use/analyze these sources to answer the research question you have proposed.
Monday, March 23: Tools for Privacy

- How do tools like Tor, DuckDuckGo, and VPNs help protect internet users’ privacy and what are their limitations?
- What is differential privacy and how can it be applied to different online and digital contexts?

Readings:

- [Listening In, chapter 4.](http://example.com/)

Monday, March 30: Guest Lecture by Susan Landau on Searching Metadata & Electronic Devices

- What is the law, practice, and value of electronic device and metadata searches?
- How is the special case of location information handled in law and policy?
- How is the evidentiary value of mobile devices and other searches changing?

Readings:

- Moy, I used to track cell phone location information for prosecutors. My experience illustrates the overwhelming need for better technical resources for defense attorneys, *Hackernoon*, November 28, 2017. Available from [https://medium.com/hackernoon/i-used-to-track-cell-phone-location-information-for-prosecutors-b0dbd4325997](https://medium.com/hackernoon/i-used-to-track-cell-phone-location-information-for-prosecutors-b0dbd4325997).
- Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council, Bulk Collection of Signals Intelligence:
Technical Options, 2015, Chapters 1-4. Available from https://www.nap.edu/read/19414/chapter/1 (Links to an external site.)


- Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, Evaluating the Privacy Properties of Telephone Metadata, Proceedings of the National Academy of Sciences May 17, 2016. Available from https://pdfs.semanticscholar.org/dbe1/07ce415a8252009f764afa0a058693596c64.pdf (Links to an external site.)


Monday, April 6: Usable Privacy & Behavioral Economics

**In-Class Debate #5: Should Facebook users be able to pay $100 per year to Facebook in exchange for none of their data being analyzed by the company and not being shown any ads?**

- What challenges do users encounter when trying to use privacy-protecting tools and software?
- What design decisions can help (or hinder) the use of privacy-protecting technologies?
- How do users make decisions about privacy and to what extent do those decisions reflect their self-reported opinions about digital privacy?

**Readings:**


Monday, April 13: Privacy as Privilege & Protecting Vulnerable Populations

- Who is afforded the most online privacy and why?
- Which groups face particular privacy challenges in digital contexts and how can technology designers and policy-makers do a better job protecting these vulnerable populations?

Readings:


Monday, April 20 – NO CLASS (Patriot’s Day)

Monday, April 27: Wrap-up and Looking Ahead

- To what extent have predictions made decades ago about the impact of technology and the Internet on privacy proved true?
- In what ways have digital technologies enhanced and eroded personal privacy?
• What future technological developments will have a significant impact on privacy and how should we be preparing for them?
• How are companies and governments changing their positions on privacy and what factors are driving them?

Readings:


Final Paper Assignment (Due by 11:59pm on Friday, May 1)
The final paper for this class is a 10-12 page research paper examining a specific topic of your choice related to digital privacy using primary sources. The paper should pose a clear research question and build a strong argument based on evidence drawn from primary sources, as well as appropriate secondary sources. If you would like to do a more technical analysis of data that is fine, but it must include a final written product, as well as some discussion of the policy implications and relevance of the work.

Grading
Assignment #1 (due Feb. 17): 15%
Assignment #2 (due March 9): 15%
Assignment #3 (due March 23): 15%
Final paper (due May 1): 30%
Class participation and in-class debate: 25%