

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)

Office hours sign-up: <http://bit.ly/WolffOfficeHours> (Links to an external site.)

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

Susan Landau, [Listening In: Cybersecurity in an Insecure Age](#), New Haven: Yale University Press, 2017.

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.
- Louis D. Brandeis and Samuel D. Warren, “The Right to Privacy,” *Harvard Law Review*, 1890. Available

from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_war_r2.html (Links to an external site.).

- Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide,'" *The Chronicle of Higher Education*, May 15, 2011. Available from <http://www.uvm.edu/~dguber/POLS21/articles/solove.htm> (Links to an external site.).
- Eric Hughes, "A cypherpunk's manifesto," March 9, 1999. Available from <https://www.activism.net/cypherpunk/manifesto.html> (Links to an external site.).
- Helen Nissenbaum, "A contextual approach to privacy online," *Daedalus*, vol. 140, no. 4, pp. 32-48, 2011. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567042 (Links to an external site.).
- "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance," May 2014. Available from https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf (Links to an external site.).
- Julie McCarthy, "Indian Supreme Court Declares Privacy A Fundamental Right," NPR, Aug. 24, 2017. Available from <https://www.npr.org/sections/thetwo-way/2017/08/24/545963181/indian-supreme-court-declares-privacy-a-fundamental-right> (Links to an external site.).
- "The right to privacy in the digital age," Report of the United Nations High Commissioner for Human Rights, Aug. 3, 2019. Available from https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf (Links to an external site.).

Monday, Feb. 3: Intro to Encryption & Encryption Policy, Part I (1993-2015)

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.
- Steven Levy, "Battle of the Clipper Chip," *New York Times*, June 12, 1994. Available from <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html> (Links to an external site.).
- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," May 27, 1997. Available from <https://www.cs.columbia.edu/~smb/papers/paper-key-escrow.pdf> (Links to an external site.).
- Josh Halliday, "BlackBerry ban lifted in Saudi Arabia," *The Guardian*, Aug. 10, 2010. Available from <https://www.theguardian.com/technology/2010/aug/10/blackberry-saudi-arabia-ban-lifted> (Links to an external site.).
- Jane Wakefield, "Can the government ban encryption?" *The BBC*, Jan. 13, 2015. Available from <https://www.bbc.com/news/technology-30794953> (Links to an external site.).
- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L.

Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, and Daniel Weitzner, "Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data and Communications," MIT Computer Science and Artificial Intelligence Lab Technical Report, July 6, 2015. Available from <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf> (Links to an external site.).

- Cyrus Vance, François Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times*, Aug. 11, 2015. Available from <https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html> (Links to an external site.).

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:

- Alex Hern, "UK government can force encryption removal, but fears losing, experts say," *The Guardian*, March 29, 2017. Available from <https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act> (Links to an external site.).
- Lorand Laskai and Adam Segal, "The Encryption Debate in China," Carnegie Endowment for International Peace. May 30, 2019. Available from <https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216> (Links to an external site.).
- Bedavyasa Mohanty, "The Encryption Debate in India," Carnegie Endowment for International Peace. May 30, 2019. Available from <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213> (Links to an external site.).
- Gabriel Aleixo, Andréa Guimarães Gobbato, Isabela Garcia De Souza, Natalia Langenegger, Ronaldo Lemos, Fabro Steibel, "The Encryption Debate in Brazil," Carnegie Endowment for International Peace. May 30, 2019. Available from <https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219> (Links to an external site.).
- "Moving the Encryption Policy Conversation Forward," Carnegie Endowment Encryption Working Group, Sept. 10, 2019. Available from: <https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573> (Links to an external site.).
- "Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. To Assist Agents in Search, And Opposition to Government's Motion to Compel Assistance," United States District Court, Central District of California, Feb. 25, 2016. Available from <https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf> (Links to an external site.). Read pp. 1-19.
- Michael Keller and Gabriel Dance, "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *New York Times*, Sept. 28, 2019. Available from <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html> (Links to an external site.).
- Priti Patel, William Barr, Kevin McAleenan, and Peter Dutton, "Open Letter: Facebook's 'Privacy First' Proposals," Oct. 4, 2019. Available

from <https://www.justice.gov/opa/press-release/file/1207081/download> (Links to an external site.).

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.
- *Olmstead v. United States* 277 US 438 (1928), opinion of the Court and Brandeis dissent. Available from <https://www.law.cornell.edu/supremecourt/text/277/438> (Links to an external site.).
- *Katz v. United States* 389 US 347 (1967), opinion of the court, Harlan concurrence. Available from <https://www.law.cornell.edu/supremecourt/text/389/347> (Links to an external site.).
- *Smith v. Maryland* 442 U.S. 735 (1979). Available from <https://www.law.cornell.edu/supremecourt/text/442/735> (Links to an external site.).
- “ECPA: Background,” Electronic Privacy Information Center. Available from <https://epic.org/privacy/ecpa/#background> (Links to an external site.).
- Jennifer Daskal and Peter Swire, “Why the CLOUD Act is Good for Privacy and Human Rights,” *Lawfare*, March 14, 2018. Available from <https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights> (Links to an external site.).
- Neema Singh Guliani and Naureen Shah, “The CLOUD Act Doesn’t Help Privacy and Human Rights: It Hurts Them,” *Lawfare*, March 16, 2018. Available from <https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them> (Links to an external site.).
- Paul Mozur and Aaron Krolik, “A Surveillance Net Blankets China’s Cities, Giving Police Vast Powers,” *New York Times*, Dec. 17, 2019. Available from <https://www.nytimes.com/2019/12/17/technology/china-surveillance.html> (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.
- “Electronic Surveillance,” Cornell Legal Information Institute. Available from https://www.law.cornell.edu/wex/electronic_surveillance (Links to an external site.).
- Glenn Greenwald, “NSA collecting phone records of millions of Verizon customers daily,” *The Guardian*, June 6, 2013. Available from <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (Links to an external site.).
- Glenn Greenwald and Ewen MacAskill, “NSA Prism program taps in to user data of Apple, Google and others,” *The Guardian*, June 7, 2013. Available from <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (Links to an external site.).
- Kim Willsher, “France approves ‘Big Brother’ surveillance powers despite UN concern,” *The Guardian*, July 24, 2015. Available from <https://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers> (Links to an external site.).
- Jacques Singer-Emery, “The Second Circuit Rules in United States v. Hasbajrami,” *Lawfare*, Jan. 7, 2020. Available from <https://www.lawfareblog.com/second-circuit-rules-united-states-v-hasbajrami> (Links to an external site.).
- Charlie Savage, “Disputed N.S.A. Phone Program Is Shut Down, Aide Says,” *New York Times*, March 4, 2019. Available from <https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html> (Links to an external site.).

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:

- Charles Duhigg, “How Companies Learn Your Secrets,” *New York Times*, Feb. 16, 2012. Available from <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (Links to an external site.).
- Julia Angwin, Surya Mattu, and Terry Parris Jr., “Facebook Doesn’t Tell Users Everything It Really Knows About Them,” *ProPublica*, Dec. 27, 2016. Available from <https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them> (Links to an external site.).

- Maggie Fick and Alexis Akwagyiram, “In Africa, scant data protection leaves internet users exposed,” *Reuters*, April 4, 2018. Available from <https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ> (Links to an external site.).
- Farhad Manjoo, “I Visited 47 Sites. Hundreds of Trackers Followed Me,” *New York Times*, Aug. 23, 2019. Available from <https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html> (Links to an external site.).
- Bennett Cyphers, “Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance,” Electronic Frontier Foundation, Dec. 2, 2019. Available from <https://www.eff.org/wp/behind-the-one-way-mirror> (Links to an external site.).
- 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.).
- Vindu Goel, “On Data Privacy, India Charts Its Own Path,” *New York Times*, Dec. 10, 2019. Available from <https://www.nytimes.com/2019/12/10/technology/on-data-privacy-india-charts-its-own-path.html> (Links to an external site.).
- Natasha Singer, “What Does California’s New Data Privacy Law Mean? Nobody Agrees,” *New York Times*, Dec. 29, 2019. Available from <https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html> (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:

- Yonah Jeremy Bob, "Knesset committee approves landmark biometric database law after 8-year experiment," *The Jerusalem Post*, Feb. 28, 2017. Available from <https://www.jpost.com/Israel-News/Politics-And-Diplomacy/Knesset-committee-approves-landmark-biometric-database-law-after-8-year-experiment-482783> (Links to an external site.).
- Nathan Heller, "Estonia, the Digital Republic," *New Yorker*, Dec. 11, 2017. Available from <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic> (Links to an external site.).
- Vindu Goel, "India's Top Court Limits Sweep of Biometric ID Program," *New York Times*, Sept. 26, 2018. Available from <https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html> (Links to an external site.).
- Lauren Frayer, "India's Biometric ID System Has Led To Starvation For Some Poor, Advocates Say," *NPR*, Oct. 1, 2018. Available from <https://www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say> (Links to an external site.).
- Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *New York Times*, Feb. 21, 2019. Available from <https://www.nytimes.com/2019/02/21/business/china-xinjiang-uyghur-dna-thermo-fisher.html> (Links to an external site.).
- Bruce Schneier, "Why 'Anonymous' Data Sometimes Isn't," *Wired*, Dec. 12, 2007. Available from <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/> (Links to an external site.).
- Arvind Narayanan and Vitaly Shmatikov, "Robust de-anonymization of large sparse datasets: a decade later," May 21, 2019. Available from <http://randomwalker.info/publications/de-anonymization-retrospective.pdf> (Links to an external site.).

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.
- Dune Lawrence, "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built," *Bloomberg Businessweek*, Jan. 23, 2014. Available from <https://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency> (Links to an external site.).
- Matt Burgess and Victoria Woollaston, "DuckDuckGo: What is it and how does it work?" *Wired*, Feb. 1, 2017. Available from <https://www.wired.co.uk/article/duckduckgo-anonymous-privacy> (Links to an external site.).
- Josephine Wolff, "The Internet Censor's Dilemma: The more countries try to restrict virtual private networks, the more people use them," *Slate*, March 5, 2018. Available from <https://slate.com/technology/2018/03/virtual-private-networks-become-more-popular-as-countries-restrict-their-use.html> (Links to an external site.).
- Tianqing Zhou, "Explainer: what is differential privacy and how can it protect your data?" *The Conversation*, March 18, 2018. Available from <https://theconversation.com/explainer-what-is-differential-privacy-and-how-can-it-protect-your-data-90686> (Links to an external site.).

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:

- Citizen Lab, *The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security*, May 21, 2015. Available from <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/> (Links to an external site.).
- *Riley v. California*, 134 US 2473 (2014), Opinion of the Court. Available from <https://www.law.cornell.edu/supct/pdf/13-132.pdf> (Links to an external site.).
- 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> (Links to an external site.).
- *Carpenter v. United States*, 819 F. 3d 880 (2018), Opinion of the Court. Available from https://www.law.cornell.edu/supremecourt/text/16-402#writing-16-402_OPINION_3 (Links to an external site.).
- 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.).

- *US v. Jones* 132 US 945 (2012), Syllabus and Sotomayor concurrence. Available from <https://www.law.cornell.edu/supremecourt/text/10-1259> (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.).
- *Kyllo v. United States*, 533 U.S. 27 (2001). Available from <https://www.law.cornell.edu/supct/html/99-8508.ZO.html> (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 to those decisions reflect their self-reported opinions about digital privacy?

Readings:

- Alma Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," In Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 169-183. Available from https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/USENIX.pdf (Links to an external site.).
- Alessandro Acquisti and Jens Grossklags, "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," 2007 Workshop on Economics of Information Security. Available from <http://weis07.infosecnet.org/papers/66.pdf> (Links to an external site.).
- Alessandro Acquisti and Jens Grossklags, "What Can Behavioral Economics Teach Us About Privacy?" *Digital Privacy: Theory, Technologies, and Practices* (Taylor and Francis Group, 2007). Available from <https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf> (Links to an external site.).
- Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang, "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2012. Available from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.703.1972&rep=rep1&type=pdf> (Links to an external site.).
- Maritza Johnson, Serge Egelman, and Steven M. Bellovin, "Facebook and Privacy: It's Complicated," Proceedings of the Eighth Symposium on Usable Privacy and Security, 2012. Available from https://www.cs.columbia.edu/~smb/papers/a9_Johnson.pdf (Links to an external site.).

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:

- Amanda Hess, “How Privacy Became a Commodity for the Rich and Powerful,” *New York Times*, May 9, 2017. Available from <https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html> (Links to an external site.).
- Nithya Sambasivan, Nova Ahmed, Amna Batool, Elie Bursztein, Elizabeth Churchill, Laura Sanely Gaytán-Lugo, Tara Matthews, David Nemer, Kurt Thomas, and Sunny Consolvo, “Toward Gender-Equitable Privacy and Security in South Asia,” *IEEE Security & Privacy*, July 2019. Available from https://nithyasambasivancom.files.wordpress.com/2019/09/ieee_genderequity.pdf (Links to an external site.).
- Tara Matthews, Kathleen O’Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo, “Stories from survivors: Privacy & security practices when coping with intimate partner abuse,” CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, ACM, New York, NY, USA (2017), pp. 2189-2201. Available from <https://dl.acm.org/doi/pdf/10.1145/3025453.3025875> (Links to an external site.).
- Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell, “ ‘A Stalker’s Paradise’: How Intimate Partner Abusers Exploit Technology,” CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, April 2018. Available from <http://nixdell.com/papers/stalkers-paradise-intimate.pdf> (Links to an external site.).
- Manya Sleeper, Tara Matthews, Kathleen O’Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo, “Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy,” CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 2019. Available from https://dl.acm.org/ft_gateway.cfm?id=3300319&type=pdf (Links to an external site.).
- Amy Harmon, “As Cameras Track Detroit’s Residents, a Debate Ensues Over Racial Bias,” *New York Times*, July 8, 2019. Available from <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html?smid=nytcore-ios-share> (Links to an external site.).
- “Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law,” Federal Trade Commission press release, Sept. 4, 2019. Available from <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (Links to an external site.).

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:

- Charles Arthur, “Explaining the ‘right to be forgotten’ – the newest cultural shibboleth,” *The Guardian*, May 14, 2014. Available from <https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth> (Links to an external site.).
- Princeton University CITP, “Implications of Quantum Computing for Encryption Policy,” Carnegie Endowment for International Peace, April 26, 2019. Available from <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985> (Links to an external site.).
- Arvind Narayanan, “What Happened to the Crypto Dream?” *IEEE Security & Privacy*, March 2013. Available from <http://randomwalker.info/publications/crypto-dream-part1.pdf> (Links to an external site.).
- Mark Zuckerberg, “A Privacy-Focused Vision for Social Networking,” Facebook, March 6, 2019. Available from <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/> (Links to an external site.).
- David Brin, “The Transparent Society,” *Wired*, Dec. 1, 1996. Available from <https://www.wired.com/1996/12/fftransparent/> (Links to an external site.).

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%