Spring 2022

CPSC 310 and PLSC 369 /CPSC 210 /EP&E 365: SyllabusV3

Elizabeth Acorn
epe.yale.edu/people/elizabeth-acorn

Joan Feigenbaum
www.cs.yale.edu/homes/jf

This document contains the schedule for lectures, homework, and exams and a tentative set of reading assignments for the Spring 2022 iteration of CPSC 310 and PLSC 369 /CPSC 210 /EP&E 365.

Twenty-first century societies are faced with both threats and opportunities that combine sophisticated computation with politics and international relations in critical ways. Examples include cyber warfare; cyber espionage; cyber crime; the role of social media in democratic self-governance, authoritarian control, and election "hacking"; cryptocurrencies; and mass surveillance. CPSC 310 and PLSC 369 /CPSC 210 /EP&E 365 examine some of the political challenges wrought by massive increases in the power of information and communication technologies and the potential for citizens and governments to harness those technologies to solve problems. They are co-taught by Professors Joan Feigenbaum (CPSC) and Elizabeth Acorn (EP&E).

The two courses will have common lectures but separate sections. The CPSC 310 sections are aimed at STEM students, and CPSC 310 has CPSC 223 or the equivalent as a prerequisite. CPSC 310 may be applied towards Yale College's Quantitative Reasoning distribution requirement or its Social Sciences distribution requirement but not both. The PLSC 369 /CPSC 210 /EP&E 365 sections are aimed at social science students, and PLSC 369 /CPSC 210 /EP&E 365 has no formal course prerequisites (but assumes Internet literacy). PLSC 369 /CPSC 210 /EP&E 365 may be applied towards Yale College's Social Sciences distribution requirement. **Students may earn credit for CPSC 310 or for PLSC 369 /CPSC 210 /EP&E 365 but not both.**

The two courses will have common reading assignments. There will be four written homework assignments. Three of the CPSC 310 HW assignments will be problem sets, and three of the PLSC 369 /CPSC 210 /EP&E 365 HW assignments will be short response papers. One HW assignment will combine QR and SS methodology and will be assigned to students in both courses.

Students in both courses will take the same in-class exams, each worth 20% of the course grade, one on March 10 and the other on April 28. There will be no final during exam period. Two HW assignments will be due before the midterm break, and two will be due after the break. **Only the top three of four HW grades will count in the calculation of the course grade.** Thus, the final course grade will be based on two exam grades and three HW grades, each worth 20%.

Throughout the semester, the policy for late HWs submitted without Dean's excuses is that, for seven days after the due date, a 5% per day penalty is imposed. After seven days, the HW is no longer accepted, and the student receives a grade of zero for the assignment.

Preliminary schedule and reading assignments (subject to revision)

January 25, Lecture 1: Course overview (Feigenbaum and Acorn)

- Administrative matters, including novel course structure
- Brief "teaser" on a representative topic: lawful surveillance vs. ubiquitous encryption

Section 0: Technology basics

January 27, Lecture 2: Internet basics (Feigenbaum)

- Required reading
  - "Networks: How the Internet Works," by Scott Bradner
  - "Rethinking the Design of the Internet: The End-to-End Arguments vs. The Brave New World," by Marjory S. Blumenthal and David D. Clark
  - "Degrees of Freedom, Dimensions of Power," by Yochai Benkler
- Optional reading
  - "The Design Philosophy of the DARPA Internet Protocols," by David D. Clark
  - "End-to-end Arguments in System Design," by Jerome H. Salter, David P. Reed, and David D. Clark

February 1, Lecture 3: Crypto and security basics (Feigenbaum)

- Required reading
  - "A Brief Introduction to Information Security," by Rainer Böhme and Tyler Moore
- Optional reading
  - "The Moral Character of Cryptographic Work," by Phillip Rogaway

Section 1: Power

February 3, Lecture 4: Effect of the Internet on US democracy part I: Social-scientific take on the interplay of political polarization and the Internet (Acorn)

- Required reading
  - Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017), Chapter 1, "The Daily Me," required pages: 1-12 (remainder is optional)

    - Jaime E. Settle, *Frenemies: How Social Media Polarizes America* (Cambridge University Press, 2018), Chapter 1, "A Fundamental Change in Political Communication," pp. 1-19
    - Kathleen Hall Jamieson, "How Russian Hackers and Trolls Exploited US Media in 2016," *Proceedings of the American Philosophical Society*, 163 (2019): pp. 122-135
- Optional reading
    - Joshua A. Tucker, Yannis Theocharis, Margaret E. Roberts, and Pablo Barberá, "From Liberation to Turmoil: Social Media And Democracy," *Journal of Democracy* 28 (2017): 46–59
    - Julian E. Barnes, "Russian Interference in 2020 Included Influencing Trump Associates, Report Says," *New York Times* (March 16, 2021)

February 4: Homework 1 posted on Canvas.

February 8, Lecture 5: Effect of the Internet on US democracy part II: Computer-scientific take on the interplay of political polarization and the Internet (Feigenbaum)

- Required reading
    - "Under the Hood: Building out the infrastructure for Graph Search," by Sriram Sankar, Soren Lassen, and Mike Curtiss
    - "Exposure to opposing views on social media can increase political polarization," by Christopher A. Bail, Lisa P. Argyle, Taylor W. Brown, John P. Bumpus, Haohan Chen, M. B. Fallin Hunzaker, Jaemin Lee, Marcus Mann, Friedolin Merhout, and Alexander Volfovsky
    - "Algorithmic Amplification of Politics on Twitter," by Ferenc Huszár, Sofia Ira Ktena, Conor O'Brien, Luca Belli, Andrew Schlaikjera, and Moritz Hardt. Pages 1 - 7 are required. The rest is optional.
    - "Exposure to ideologically diverse news and opinion on Facebook," by Eytan Bakshy, Solomon Messing, Lada A. Adamic
    -
- Optional reading
    - "What Facebook Did to American Democracy and Why it Was so Hard to See it Coming," by Alex Madrigal
    - "How Facebook Works for Trump," by Alex Madrigal

February 10, Lecture 6: Effect of the Internet on power of authoritarian regimes (Acorn)

- Required reading
    - Seva Gunitsky, "Corrupting the Cyber-commons: Social Media As a Tool of Autocratic Stability," *Perspectives on Politics*, 13 (2015): pp. 42–54
    - Elizabeth Nugent and Chantal Berman, "Ctrl-Alt-Revolt? Online and Offline Networks during the 2011 Egyptian Uprising," *Middle East Law and Governance*, 10 (2018): required pages: 60-63, 67-71, 81-83 (remainder is optional)
    - Evelyn Douek, "Facebook's Role in the Genocide in Myanmar: New Reporting Complicates the Narrative," *Lawfare*, October 22, 2018 (approx. 4 pages)

February 14: Homework 1 due

February 15, Lecture 7: Effect of the Internet on corporate power (Acorn)

- Required reading
  - Kate Klonick, "The New Governors: The People, Rules and Processes Governing Online Speech," *Harvard Law Review* 131 (2018): required pages: 1599-1609, 1615-1618, 1625-1630 (remainder is optional)
  - Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (Yale University Press, 2021) Chapter 2, "Earth," required pages 23-46 (remainder is optional) (Yale Online Book)
- Optional reading
  - Peter Dauvergne, "Is Artificial Intelligence Greening Global Supply Chains? Exposing the Political Economy of Environmental Costs." *Review of International Political Economy* (2020): 1-23

February 17, Lecture 8: Tech platforms' power and antitrust law (Feigenbaum)

- Required reading
  - "Amazon's Antitrust Paradox," by Lina M. Khan. Introduction; Sections 1, 2, 3, and 6; and Conclusion are required. The rest is optional.
  - "Why 'Breaking up' Big Tech Probably Won't Work," by Fiona M. Scott Morton
- Optional viewing
  - "Lawyers and Monopoly Power" (YouTube video), speech by Matt Stoller at the Harvard Law Forum

Section 2: Surveillance

February 21: Homework 2 posted on Canvas

February 22, Lecture 9: Privacy (or lack thereof) in the Internet Age (Feigenbaum)

- Required reading
  - "Engineering Privacy," by Sarah Spieckerman and Lorrie Faith Cranor
  - "Myths and Fallacies of 'Personally Identifiable Information'," by Arvind Narayanan and Vitaly Shmatikov
  - Chapter 1 ("The Promise of Differential Privacy") of *The Algorithmic Foundations of Differential Privacy*, by Cynthia Dwork and Aaron Roth
- Optional reading
  - "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research," by Gary Marx
  - "A Taxonomy of Privacy," by Daniel J. Solove
  - "A Precautionary Approach to Big Data Privacy," by Arvind Narayanan, Joanna Huey, and Edward W. Felten.

February 24, Lecture 10: National attitudes and regional policies about surveillance (Acorn)

- Required reading

    - Abraham Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press, 2008), Chapter 3, "The Computer Age: Similar Problems, Different Solutions," pp. 42-73 (Yale Online Book)
    - Nikhil Kalyanpur and Abraham Newman, "Today, A New E.U. Law transforms Privacy Rights for Everyone. Without Edward Snowden, It Might Never Have Happened," *Monkey Cage* (May 25, 2018) (approx. 3 pages)
    - "Public Split over Impact of NSA Leak, But Most Want Snowden Prosecuted," *Pew Research Center* (June 17, 2013) (approx. 7 pages)
- Optional reading
    - David Wright and Reihard Kreissl, "European Responses to the Snowden Revelations," in Wright and Kreissl, eds. *Surveillance in Europe* (Routledge, 2015) pp.6-44 (on Canvas)

March 1, Lecture 11: Surveillance in China (Guest lecturer: Emile Dirks, read more about his work here)

- Required reading
    - Margaret Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton University Press, 2018), Chapter 5, "The Powerful Influence of Information Friction," pp. 147-189, Chapter 6, "Information Flooding: Coordination as Censorship," pp. 190-221
    - "What's the T on China's Social Credit System? – Jeremy Daum Explains," Interview with Jeremy Daum (Yale Law School), listen (or read) both parts

March 3: Homework 2 due

March 3, Lecture 12: Encryption and surveillance, Part 1 (Feigenbaum)

- Required reading
    - "Encryption and Surveillance: Why the law-enforcement access question will not just go away," by Joan Feigenbaum
    - "Apple is Selling You a Phone, Not Civil Liberties," by Susan Hennessey and Benjamin Wittes
    - "The Dangerous All Writs Act Precedent in the Apple Encryption Case," by Amy Davidson Sorkin
- Optional reading
    - Government's Motion to Compel
    - Apple's Motion to Vacate
    - (technically oriented) "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," by Stefan Savage
    - (technically oriented) "Crypto Crumple Zones: Enabling Limited Access Without Mass Surveillance," by Charles V. Wright and Mayank Varia

March 8, Lecture 13: Encryption and surveillance, Part 2 (Feigenbaum)

- Required reading

    - "Reining in Online Abuses," by Hany Farid. Although this article has some technical content, much of it is aimed at an educated general audience, and all students will benefit from reading it.
    - "Can end-to-end encrypted systems detect child sexual abuse imagery?," by Matthew Green
    - Introduction and System Overview (pages 3 and 4) of "CSAM Detection: Technical Summary," by Apple.com
    - "The Apple PSI Protocol" (1.5 page, high-level abstract), by Mihir Bellare
    - "Here's Why Apple's New Child Safety Features are So Controversial" (podcast and transcript), featuring Riana Pfefferkorn and Jennifer King
- Optional reading (technically oriented)
    - The remaining parts of "CSAM Detection: Technical Summary," by Apple.com
    - "A Concrete Security Analysis of the Apple PSI Protocol," by Mihir Bellare
    - "The Apple PSI System," by Abhishek Bhowmick, Dan Boneh, Steve Myers, Kunal Talwar, and Karl Tarbe

March 10: Exam 1

March 15, Lecture 14: Internet of Things (Feigenbaum)

- Required reading and viewing
    - "Click Here to Kill Everyone," by Bruce Schneier
        - NY Magazine Intelligencer article
        - Talk at Google (YouTube video)
    - "The Internet of Things and the Fourth Amendment of Effects," by Andrew Gurthrie Ferguson. Parts II and III are required. The rest is optional.
- Optional reading (technically oriented)
    - "Internet of things: Vision, applications and research challenges," by Daniele Miorandia, Sabrina Sicarib, Francesco De Pellegrini, and Imrich Chlamtaca
    - "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," by Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster

March 17, Lecture 15: Internet of Things, Surveillance Capitalism, and the Global South (Acorn)

- Required reading
    - Tim Wu, "Review of Shoshana Zuboff's *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*," *New York Times Review of Books* (April 9, 2020) (approx. 12 pages)
    - Michael Pisa and John Polcari, "Governing Big Tech's Pursuit of the 'Next Billion Users,'" *Center for Global Development Policy Paper* 138 (2019): 1-26

March 17: Grades on Exam 1 and HWs 1 and 2 will be available.

March 18: Last date for students to withdraw and not have the course on their transcripts

March 19 – 28: Spring recess

March 29, Lecture 16: Electoral data science (Guest lecturer: David Shor)

- Required reading
  - "Political Campaigns and Big Data," by David W. Nickerson and Todd Rogers

March 31: Homework 3 posted on Canvas

March 31, Lecture 17: Machine-learning fairness (Feigenbaum)

- Required reading
  - "Big Data's Disparate Impact," by Solon Barocas and Andrew D. Selbst. Only the following sections are required, and the rest is optional:
    - Introduction (pp. 673-677)
    - Examples from Part I (first full paragraph of 682 to 684, first full paragraph of 685 to 687, first full paragraph of 689 to 690)
    - Disparate Impact section (pp. 701-712)
    - Part III (pp. 714-728)
  - "A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear," by Avi Feller, Emma Pierson, Sam Corbett-Davies, and Sharad Goel
  - "How big data is unfair," by Moritz Hardt
- Optional reading (technically oriented)
  - "Fairness through Awareness," by Cynthia Dwork, Moritz Hardt, Toniann Pitassi, Omer Reingold, Richard Zemel
  - "Calibration for the (Computationally Identifiable) Masses," by Úrsula Hébert-Johnson, Michael P. Kim, Omer Reingold, and Guy N. Rothblum

Section 3: Security

April 5, Lecture 18: Cyber war, cyber espionage, and cyber crime, Part 1 (Feigenbaum)

- Required reading
  - The UN Charter. Article 2(4), Article 51, and Chapter VII are required. The rest is optional.
  - The Law of Cyber Attack, by Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel
- Optional reading
  - "Keeping the Wrong Secrets: How Washington Misses the Real Security Threat," by Oona A. Hathaway
  - "Cyber War I: Estonia Attacked from Russia," by Kertu Ruus

April 7, Lecture 19: Cyber war, cyber espionage, and cyber crime, Part 2 (Feigenbaum)

- Required reading
  - "To Kill A Centrifuge," by Ralph Langner
  - "An International Legal Framework for Surveillance," by Ashley Deeks. Part I is required. The rest is optional.

April 10: Homework 3 due

April 12, Lecture 20: New technologies and international security (Acorn)

- Required reading:

    - Michael C. Horowitz, "Do Emerging Military Technologies Matter for International Politics?" *Annual Review of Political Science,* 23(1) (2020): 385–400
    - Michael C. Horowitz and Paul Scharre, "The Morality of Robotic War," *New York Times* (May 26, 2015)
- Optional reading:
    - Jack Goldsmith,. "How Cyber Changes the Laws of War," *European Journal of International Law*, 24(1) (2013): 129-138.
    - Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (Norton, 2018), Ch.12, "Failing Deadly: The Risk of Autonomous Weapons" and Ch.14, "The Invisible War: Autonomy in Cyberspace" (on Canvas)

April 14, Lecture 21: Corporate influence on cyber war and cyber espionage (Acorn)

- Required reading:
    - Jacquelyn Schneider, "The Cyber Apocalypse Never Came. Here's What We Got Instead," *Politico* (July 27, 2021)
    - "The Lawfare Podcast: Orin Kerr and Asaf Lubin on Apple v. NSO Group," *Lawfare* (December 3, 2021)

April 15: Homework 4 posted on Canvas

April 19, Lecture 22: Electronic voting (Guest lecturer: Josh Benaloh)

- Required reading
    - "End-to-end Verifiability," by Josh Benaloh, Ron Rivest, Peter Y. A. Ryan, Philip Stark, Vanessa Teague, and Poorvi Vora
    - "Simple Verifiable Elections," by Josh Benaloh. Although this article has some technical content, much of it is aimed at an educated general audience, and all students will benefit from reading it.
- Optional reading
    - (technically oriented) "Public Evidence from Secret Ballots," by Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach
    - "The Future of Voting: Accessible, Reliable, Verifiable Technology," National Academies Report. (The free pdf is available at Guest Login | National Academies Press (nap.edu).)
    - (technically oriented) "ElectionGuard": An open-source software-development kit "designed for election-system vendors to incorporate end-to-end verifiability into their systems and any interested organization to perform and publish post-election audits."

April 21, Lecture 23: Blockchains and cryptocurrencies, Part 1 (Feigenbaum)

- Required reading
    - "A Short Introduction to the World of Cryptocurrencies," by Aleksander Berentsen and Fabian Schär

    - The “Ethereum” and “Applications” sections of the Ethereum Whitepaper
- Optional reading
    - “Why Bitcoin is destined to become a niche asset: A cryptocurrency reality check,” by Teunis Brosens

April 25: Homework 4 due

April 26, Lecture 24: Blockchains and cryptocurrencies, Part 2 (Feigenbaum)

- Required reading
    - “How NFTs Create Value,” by Steve Kaczynski and Scott Duke Kominers
    - “My First Impressions of Web 3,” by Moxie Marlinspike

April 28: Exam 2