

WWS 586F / COS 586: Technology Policy and Law Spring 2020

This advanced graduate seminar will examine recurring, high-profile issues in technology policy and law. Each weekly meeting will explore a challenging topic, including consumer privacy, data security, electronic surveillance, net neutrality, online speech, algorithmic fairness, cryptocurrencies, election security, and offensive operations. The seminar will also cover foundational technical concepts that affect policy and law, including internet architecture, cryptography, systems security, privacy science, and artificial intelligence. Materials and discussion will draw extensively from current events and primary sources. Assignments are modeled on real-world policy work products.

Seminar Team

[Jonathan Mayer](#) – Assistant Professor of Computer Science and Public Affairs

[Jordan Holland](#) – Graduate Researcher, Center for Information Technology Policy

Materials

The [readings](#) for this seminar will span a diverse range of disciplines, including public policy, law, and computer science. Because of the broad subject matter, there will be more reading and sources than in a typical graduate seminar. I have significantly edited the assigned materials to focus on key concepts and passages.

Reading Notes

Participants will submit brief [reading notes](#) in advance of each meeting (except the first meeting) in order to further the seminar discussion. Reading notes are due at noon before each seminar meeting. You may opt out of reading notes for up to two meetings, no questions asked.

Participation

The course has a law and policy seminar format. Active participation is both encouraged and expected.

Missed Meetings

If you are unable to attend a seminar meeting owing to a professional or personal obligation, please send an explanation in advance and submit extended reading notes (about five pages). The extended notes should briefly summarize the materials and provide more complete responses to the entire set of prompts. The purpose of these extended notes is to roughly substitute for the seminar discussion; you may not use a reading note opt out for a missed seminar.

Assignments

The course will have three assignments, each intended to develop your public policy research skillset: an [individual project proposal memorandum](#) (due February 28), a group project proposal memorandum and briefing (due March 13), and a group research study (due May 12).

Electronic Devices

Notebooks, tablets, smartphones, and other electronic devices will not be welcome during the seminar, except for students with accessibility requirements.

Grading

Participation and Reading Notes: 25%

Individual Project Proposal Memorandum: 20%

Group Project Proposal Memorandum and Briefing: 20%

Group Research Paper: 35%

Each assignment is graded on a $\checkmark+$ / \checkmark / $\checkmark-$ scale, which approximately maps to A / B / C letter grades. Please reach out if you would like me to calculate your current letter grade at any point during the course.

February 4 – Net Neutrality

- Highly Recommended Material
 - John Oliver on Net Neutrality ([2014 Segment](#), [2014 Update](#), [2017 Segment](#), [2017 Update](#))
- Assigned Reading
 - Tim Wu & Christopher S. Yoo, *Keeping the Internet Neutral?*, 59 FED. COMM. L.J. 575 (2007)
 - The Communications Act of 1934 and the Telecommunications Act of 1996, 47 U.S.C. §§ 153, 201, 202, 1302
 - ANGELE A. GILROY, CONG. RESEARCH SERV., R40616, THE NET NEUTRALITY DEBATE (2017)
 - FCC, Protecting and Promoting the Open Internet, Report and Order, 30 FCC Rcd. 5601 (2015)
 - U.S. Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016)
 - FCC, Restoring Internet Freedom, Report and Order. 33 FCC Rcd. 311 (2017)
- Optional Reading – Judicial Opinions
 - Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005)
 - Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010)
 - Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014)
 - Mozilla v. FCC, 940 F.3d 1 (D.C. Cir. 2019)
- Optional Reading – Regulatory Action
 - FCC, Internet Policy Statement, 20 FCC Rcd. 14986 (2005)
 - Preserving the Open Internet, Report and Order, 25 FCC Rcd. 17905 (2010)
 - FCC, Policy Review of Mobile Broadband Operators' Sponsored Data Offerings (2017)
- Optional Reading – Law and Policy Scholarship
 - Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2003)
 - Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. TELECOMM. & HIGH TECH. L. 329 (2007)
 - BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2012)
 - SUSAN CRAWFORD, CAPTIVE AUDIENCE (2014)

- Barbara van Schewick, *Network Neutrality and Quality of Service*, 67 STAN. L. REV. 1 (2015)
- Optional Reading – Net Neutrality at the State Level
 - Montana Executive Order No. 3-2018, Providing for Internet Neutrality Principles in State Procurement (Jan. 22, 2018)
 - California S.B. 822
- Optional Reading – Net Neutrality in the European Union
 - Commission Regulation 2015/2120 of Nov. 25, 2015, Laying Down Measures Concerning Open Internet Access, 2015 O.J. (L 310)
 - Board of European Regulators for Electronic Communications, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (2016)
- Optional Reading – Net Neutrality in India
 - Telecom Regulatory Authority of India, Prohibition of Discriminatory Tariffs for Data Services Regulation (2016)
 - Telecom Regulatory Authority of India, Recommendations on Encouraging Data usage in Rural Areas through Provisioning of Free Data (2016)
 - Telecom Regulatory Authority of India, Recommendations on Net Neutrality (2017)

February 11 – Data Security

- Assigned Reading
 - The Federal Trade Commission’s Data Security Authority
 - The Federal Trade Commission Act, 15 U.S.C. § 45
 - Pay close attention to the FTC’s “unfairness” and “deception” authorities, as well as its enforcement capabilities. These will come up throughout the course.
 - FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)
 - Reading Notes: Do you agree that the FTC’s “unfairness” authority includes data security regulation? Which argument do you find most persuasive for or against that position?
 - Complaint, FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016)
 - Reading Notes: How, exactly, did Ashley Madison violate the FTC Act? What is the FTC requesting as a remedy?
 - FTC, START WITH SECURITY: A GUIDE FOR BUSINESS AND LESSONS LEARNED FROM FTC CASES (2015)
 - Reading Notes: What is the FTC’s basis for identifying these particular security issues as essential for FTC Act compliance? Why do you think the FTC issued this guide?
 - Data Security Standards
 - FCC, Report and Order, 31 FCC Rcd. 13911 (2016) (Data Security Standard)
 - Reading Notes: Do you agree with the FCC’s approach to setting a data security standard? What are the alternatives?
 - The California Data Safeguard Statute, Cal. Civil Code § 1798.81.5

- Reading Notes: How does the California data security standard compare to the FCC's? Are they the same or different?
 - The California Consumer Privacy Act, Cal. Civil Code § 1798.150
 - Reading Notes: This provision in California's new privacy law has been widely acclaimed as a win for consumers. What exactly does the provision do, and do you agree with that analysis?
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Data Security Standard)
 - Reading Notes: How does the GDPR data security standard compare to the FTC and FCC standards?
- Breach Notification Requirements
 - The California Data Breach Notification Statute, Cal. Civil Code § 1798.82
 - As you read through the materials on data breach notification, think about why data breach notification does (or doesn't) make sense as a policy.
 - Reading Notes: What do you think is the best argument in favor of a data breach notification requirement?
 - Reading Notes: What do you think is the best argument against a data breach notification requirement?
 - Complaint, People v. Kaiser Foundation Health Plan, Inc., No. RG14711370 (Cal Sup. Ct. Jan. 24, 2014)
 - Reading Notes: Pay close attention to how the California Attorney General is enforcing the state's data breach notification law. What is the legal mechanism? Why do you think California brought this case?
 - FCC, Report and Order, 31 FCC Rcd. 13911 (2016) (Data Breach Notification)
 - Reading Notes: What are the elements of a data breach notification requirement that the FCC puzzles through? Do you agree with the FCC's policy decisions?
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Data Breach Notification)
 - Reading Notes: How does the GDPR breach notification provision compare to the California and FCC breach notification requirements?
 - OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEMORANDUM NO. M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (2017)
 - Reading Notes: In general, when is a federal agency that has been breached required to notify affected individuals? Does OMB's guidance provide sufficient direction to agencies?

February 18 – Data Privacy (Part 1)

Note: [Julie Cohen](#) from Georgetown Law will present at a lunch seminar before class. Highly

recommended.

- Assigned Reading
 - Conceptions of Privacy
 - Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002)
 - Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006)
 - James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004)
 - Reading Notes: Which conception of privacy is most similar to your own? Why do you think about privacy that way?
 - The Behavioral Economics and Psychology of Privacy
 - Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015)
 - Reading Notes: If you were advising a federal policymaker on data privacy, how would you encourage them to incorporate behavioral economics and psychology into federal privacy policy?
 - Privacy Policies and Transparency Requirements
 - Cal. Bus. & Professions Code §§ 22575, 22577
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Transparency Requirements)
 - Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 3 (2008)
 - Reading Notes: Are privacy policies worthwhile, even if consumers ignore them?
 - Reading Notes: What are the competing incentives for online services that post privacy policies?
 - Individual, Entity, and Territorial Coverage
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Territorial Scope)
 - The California Consumer Privacy Act, Cal. Civil Code § 1798.140 (Individual and Entity Coverage)
 - Reading Notes: GDPR, in general, only applies to entities established in the EU or when a non-EU entity is directing business into the EU that involves data about individuals in the EU. CCPA, in general, only applies when a firm meets certain size thresholds and collects or sells data about California residents. What do you think the effects of GDPR and CCPA will be for individuals who aren't in the EU and who aren't California residents?
 - Reading Notes: Suppose that you were advising the European Commission during GDPR's drafting. The Commission recognizes that European companies often transfer data to U.S. businesses that adhere to EU-like privacy protections, and it would like to accommodate those transfers. How would you recommend that GDPR account for those transfers?
 - The Federal Trade Commission's Data Privacy Authority (Part 1)
 - *In re Turn, Inc.*, 152 F.T.C. 3099 (2017)

- You may find it helpful to reference the prior week's reading on the Federal Trade Commission Act.
- Reading Notes: What is the federal privacy law that Turn violated? Are you persuaded that that law is sufficient to address modern data privacy problems?

February 25 – Data Privacy (Part 2)

Note: [Aleksandra Korolova](#) from USC will present at a lunch seminar before class. Highly recommended.

- Assigned Reading
 - The Federal Trade Commission's Data Privacy Authority (Part 2)
 - Complaint, *United States v. Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. July 24, 2019)
 - Reading Notes: What do you think is the strongest argument in favor of the FTC's position that Facebook misrepresented its privacy practices for third-party developers (Counts 1-3)? What do you think is the strongest argument against the FTC's position?
 - Reading Notes: The FTC and Facebook settled this case for a record-setting \$5 billion penalty and a new order that requires Facebook to not misrepresent its privacy practices, maintain a comprehensive privacy program, obtain biennial independent privacy audits, report compliance incidents to the FTC, and establish a privacy committee of the corporate board. In your view, is the outcome of the case likely to significantly change Facebook's privacy practices?
 - Data Rights
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Data Rights)
 - The California Consumer Privacy Act, Cal. Civil Code §§ 1798.100, .105, .110, .115 (Data Rights)
 - Reading Notes: How do the GDPR and CCPA data rights provisions compare?
 - Reading Notes: What do you think the effects of the GDPR and CCPA data rights provisions will be for consumers and businesses?
 - Consumer Choice Requirements
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Processing and Consent)
 - The California Consumer Privacy Act, Cal. Civil Code §§ 1798.120, .125 (Consumer Choice)
 - Reading Notes: GDPR is often characterized as imposing an opt-in requirement for data collection, retention, use, and sharing. After reading the relevant provisions of GDPR, do you agree with that characterization?
 - Reading Notes: One possible direction for federal privacy policy is an across-the-board opt-in requirement for data collection, retention, use, and sharing. What do you think the consequences of a universal opt-in requirement would be? Do you think that would be good policy?

- Personally Identifiable Information, De-Identification, and Re-Identification
 - Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010)
 - FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012) (Personally Identifiable Information and Deidentification)
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Personal Data)
 - Reading Notes: Imagine that you are a congressional staffer developing comprehensive consumer privacy legislation. How would you define the concept of personally identifiable information, and why would you adopt that definition?

- Optional Reading – Consumer Choice Requirements
 - FCC, Protecting the Privacy of Broadband, Report and Order, 31 FCC Rcd. 13911 (2016) (Opt-in and Opt-out Consumer Choice Provisions)

- Optional Reading – Personally Identifiable Information, De-Identification, and Re-Identification
 - FCC, Protecting the Privacy of Broadband, Report and Order, 31 FCC Rcd. 13911 (2016) (Personally Identifiable Information Provisions)

March 3 – Law Enforcement and National Security Surveillance

This meeting of the seminar will be more lecture-like than usual, owing to the volume and legal intricacy of the material.

- Assigned Viewing – videos are [available online](#)
Please note: while these recordings were part of a Stanford Law online course, they are directed at a non-law audience.
 - Demands for Testimony and Evidence (Individual Subpoenas)
 - Physical Intrusions (Search and Seizure Warrants)
 - Wiretapping (Wiretap Orders)
 - Historical Call Records and Account Information (Provider Subpoenas)
 - Prospective Call Records (Pen/Trap Orders)
 - Email and Other Electronic Messaging (SCA D Orders and Provider Warrants)
 - Search Engines, Social Networks, and Cloud Storage
 - Reading Notes: A key component of U.S. surveillance law and policy is the distinction between communications content and metadata. What do you think is the best argument in favor of drawing that distinction and applying lesser protections to metadata?

- Assigned Viewing – videos are [available online](#)
 - The Fourth Amendment in Extraterritorial and National Security Contexts
 - The Foreign Intelligence Surveillance Act (FISA)
 - Reading Notes: A foundation of foreign intelligence surveillance (in the U.S. and worldwide) is that citizens and residents deserve greater privacy protections than extraterritorial foreigners. What do you think is the best rationale for that

distinction? Do you agree with that perspective?

- Assigned Reading
 - Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (2014)
 - Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014)
 - Reading Notes: Based on what you've read about Section 215, do you believe that the telephone records program struck an appropriate balance between national security and privacy interests? If you don't think it did, how would you revise the program? If you aren't certain, what questions would you ask of the Intelligence Community?
 - Reading Notes: Section 215 and Section 702 placed the federal judiciary in a new role—supervising entire surveillance programs, rather than approving individual instances of surveillance. What do you think are the tradeoffs associated with this new role?
 - Reading Notes: When investigating a U.S. person for possible criminal activity, the FBI is authorized to query communications content that was initially collected under Section 702. What do you think are the right procedural safeguards for these types of queries?

- Optional Reading
 - Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (2013)
 - Privacy and Civil Liberties Oversight Board, Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities (2017)
 - Privacy and Civil Liberties Oversight Board, Report on the USA Freedom Act Telephone Call Records Program (2020)
 - Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004)
 - Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Questions*, 37 HARV. J.L. & PUB. POL'Y 757 (2014)
 - Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015)
 - Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015)

March 10 – Artificial Intelligence and Fairness (Part 1)

Note: [Rediet Abebe](#) from Harvard will present at a lunch seminar the day before class. Highly recommended.

- Assigned Reading

- A (Relatively) Gentle Overview of Machine Learning
 - Google, Introduction to Machine Learning (2018)
 - Reading Notes: Imagine you are serving in the White House Office of Science and Technology Policy, and the President (not necessarily the current President) asks you to draft an executive order that addresses the promise of artificial intelligence. What do you include in the executive order?
- Algorithmic Fairness
 - Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016)
 - EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS (2016)
 - Reading Notes: Imagine you are advising a member of Congress on technology matters, and the member has asked you to develop legislation about algorithmic fairness. What do you include in the bill?
- Criminal Justice Algorithms
 - Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016)
 - Sam Corbett-Davies et al., *A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear.*, WASH. POST. (Oct. 17, 2016)
 - Reading Notes: California recently abolished money bail in favor of pretrial risk assessment algorithms. Imagine you are advising the California Judicial Council on what safeguards to require as the state courts adopt these algorithms. What recommendations do you make?

March 17 – Spring Recess, Enjoy!

March 24 – Artificial Intelligence and Fairness (Part 2), Cryptocurrencies and Blockchains

- Assigned Reading – Artificial Intelligence and Fairness (Part 2)
 - Technical Responses
 - Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017)
 - Reading Notes: Which of the technical responses to algorithmic fairness that Kroll et al. discuss do you think is most promising? Which do you think is least promising?
 - Regulatory Responses
 - The General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) (Automated Decision-Making)
 - The Equal Credit Opportunity Act, 15 U.S.C. § 1691
 - Dillon Reisman et al., AI NOW, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability (2018)
 - Reading Notes: In your view, is the GDPR's right to appeal an effective response to algorithmic fairness concerns?

- Reading Notes: In your view, are algorithmic impact assessments an effective response to algorithmic fairness concerns?
- Assigned Reading – Cryptocurrencies and Blockchains
 - ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES* (2016)
 - SEC, Release No. 81207 (July 25, 2017)
 - Internal Revenue Service, Notice 2014-21(2014)
 - Executive Order 13,827 (Mar. 19, 2018)
 - Reading Notes: Can you think of a public policy or legal problem that would benefit from blockchain technology? What is the problem, how would blockchain technology help, and why would it be better than other approaches?
 - Reading Notes: Voatz, a Boston-based startup, is developing a voting platform that uses a smartphone app and blockchain technology. If you were advising a state election official, would you recommend using Voatz (or a similar blockchain-based platform) for voting? Why or why not?
- Optional Reading – Artificial Intelligence and Fairness
 - NIST, Face Recognition Vendor Test
 - Danielle Keats Citron, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014)
 - Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503
 - Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008)
- Optional Reading – Cryptocurrencies and Blockchains
 - Shanaan Cohney et al., *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019)
 - SEC
 - SEC v. PlexCorps, No. 1:17-cv-07007-DLI-RML, 2017 WL 6398722 (E.D.N.Y. Dec. 14, 2017)
 - CFTC
 - Coinflip Order (2015)
 - CFTC v. My Big Coin Pay, Inc., 334 F. Supp. 3d 492 (D. Mass. 2018)
 - CFTC v. McDonnell, 287 F. Supp. 3d 213 (E.D.N.Y. 2018)
 - FTC
 - Workshop on Decrypting Cryptocurrency Scams (2018)
 - Enforcement Action Against Bitcoin Funding Team (2018)
 - Enforcement Action Against Butterfly Labs (2016)
 - Enforcement Action Against Equiliv Investments (2015)
 - CFPB
 - Consumer Advisory on Virtual Currencies (2014)
 - IRS
 - United States v. Coinbase, No. 17-cv-01431-JSC (Nov. 28, 2017, N.D. Cal.)
 - DOJ

- Prosecution of OneCoin (2019)
- Prosecution of Jacob Campos (2018)
- Prosecution of Blue Bit Banc (2018)
- Prosecution of Joseph Kim (2018)
- Prosecution of BTC-e (2017)
- Prosecution of Renwick Haddow (2017)
- Settlement with Ripple Labs (2015)
- NYDFS
 - BitLicense Regulations

March 31 – Online Speech and Intermediary Liability

- Assigned Reading – Regulating Offensive Speech
 - *Reno v. ACLU*, 521 U.S. 844 (1997)
 - *Ashcroft v. ACLU*, 535 U.S. 564 (2002)
 - Reading Notes: The Supreme Court’s decision in *Ashcroft* rested on predictions about offensive online speech and tools for countering it. How well do you think those predictions have held up?
- Assigned Reading – Internet Access as a Speech Right
 - *Packingham v. North Carolina*, 582 U.S. __ (2017)
 - Reading Notes: Do you think Internet access is a fundamental or human right? Why or why not?
- Assigned Reading – Intermediary Liability in the U.S.
 - *Stratton Oakmont v. Prodigy*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)
 - The Communications Decency Act, 47 U.S.C. § 230
 - *Zeran v. America Online* (129 F.3d 327 (4th Cir. 1997)
 - The Digital Millennium Copyright Act, 17 U.S.C. § 512 (notice and takedown provisions)
- Assigned Reading – Intermediary Liability in the EU
 - The Electronic Commerce Directive, Commission Directive 2000/31, 2000 O.J. (L 178) (EU)
 - The Network Enforcement Act (NetzDG), Sept. 1, 2017, Bundesgesetzblatt, Teil I [BGBl I] at 3352
 - Jennifer Daskal, *Speech Across Borders*, 105 VA. L. REV. 1605 (2019)
 - The Directive on Copyright in the Digital Single Market, Commission Directive 2019/790, 2019 O.J. (L 130) (EU)
 - Reading Notes: The CJEU has taken the position that requiring a platform to remove “equivalent” offending content is distinct from requiring a platform to “monitor” for offending content. Do you agree with that distinction?
 - Reading Notes: Countries differ in their approaches to free speech and intermediary liability. Online speech, though, is inherently international. How should courts reconcile country-specific speech restrictions with international online speech?

- Reading Notes: Foreign terrorist organizations have used major online platforms for fundraising and recruiting. Imagine that you're working for a member of Congress who wants to address this challenge. What policies do you recommend?
- Reading Notes: The recent Copyright in the Digital Single Market Directive has been exceptionally controversial. Having read the key provisions, what do you think the consequences of the Directive will be?
- Optional Reading – Regulating Offensive Speech
 - United States v. American Library Ass'n, 539 U.S. 194 (2003)
- Optional Reading – Internet Access as a Speech Right
 - UN Human Rights Council Statement (June 30, 2016)
 - UN Special Rapporteur Report on Free Speech Online (May 16, 2011)
- Optional Reading – Intermediary Liability
 - JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019)
 - Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2019)
 - TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET: PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA (2018)
 - Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401 (2017)
 - Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435 (2011)
 - David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010)
 - Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010)

April 7 – Online Censorship and Speech Suppression

- Assigned Reading – Policies and Practices for Censorship and Speech Suppression
 - Freedom House, *Freedom on the Net: China Country Report* (2019)
 - Freedom House, *Freedom on the Net: Russia Country Report* (2019)
 - Reading Notes: Compare China's approach and Russia's approach to restricting online speech. What are the differences that stand out? Which do you think is more sustainable?
- Assigned Reading – U.S. Foreign Policy
 - William J. Clinton, *Remarks on U.S.-China Relations* (2000)
 - Hillary Clinton, *Remarks on Internet Freedom* (2010)
 - Reading Notes: President Clinton famously predicted that internet censorship was "like trying to nail Jell-O to the wall." How well has his prediction held up?

- Reading Notes: Imagine that you're advising the Secretary of State, and he or she has just asked for your top policy recommendation for responding to online censorship. What do you recommend?
- Assigned Reading – Self-Regulation
 - Global Network Initiative, Principles on Freedom of Expression and Privacy (2017)
 - Reading Notes: Why do you think leading technology and telecom firms established the self-regulatory GNI principles? Do you think the principles will be effective in addressing foreign internet censorship?
- Assigned Reading – Business Responses
 - Ryan Gallagher, *Google China Prototype Links Searches to Phone Numbers*, THE INTERCEPT (Sept. 14, 2018)
 - Reading Notes: Why do you think Google was experimenting with Project Dragonfly? What does Dragonfly suggest about technology sector responses to internet censorship?
- Assigned Reading – Technical Means of Censorship and Circumvention
 - Freedom House, *Leaping over the Firewall: A Review of Censorship Circumvention Tools* (2011)
- Optional Reading – Policies and Practices for Censorship and Speech Suppression
 - For an explanation of foreign policies and practices, I recommend Freedom House's country-specific [Freedom on the Net reports](#), the (slightly out of date) [Open Net Initiative reports](#), and the (also slightly out of date) *Access Denied* book series.
 - MARGARET E. ROBERTS, *CENSORED: DISTRACTION AND DIVERSION INSIDE CHINA'S GREAT FIREWALL* (2018)
- Optional Reading – Self-Regulation
 - Sundar Pichai, *AI at Google: Our Principles*, GOOGLE BLOG (June 7, 2018)
- Optional Reading – Business Responses
 - Ranking Digital Rights, *Corporate Accountability Index* (2018)
- Optional Reading – Technical Means of Censorship and Circumvention
 - The Citizen Lab at the University of Toronto has posted a number of accessible [reports](#) about foreign government censorship and use of spyware.

April 14 – Information Operations and Election Security

- Assigned Reading – Information Operations
 - U.S. Intelligence Community, *Assessing Russian Activities and Intentions in Recent U.S. Elections* (2017)

- Senate Select Committee on Intelligence, Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election (2019) (Volume 2: Russia's Use of Social Media)
- Special Counsel's Office, Report on the Investigation into Russian Interference in the 2016 Presidential Election (2019)
- Senate Foreign Relations Committee Minority Staff, Report on Russian Interference in Democracies (2018)
- Reading Notes: Going forward, what policies would you recommend for countering foreign information operations directed at the U.S.?
- Reading Notes: What policies would you recommend for the U.S. to assist allies in countering information operations?
- Assigned Reading – Election Interference and Security
 - Jeh Johnson, Testimony on Russian Interference in the 2016 U.S. Elections (2018)
 - National Academies, Securing the Vote: Protecting American Democracy (2018)
 - Reading Notes: How would you evaluate the Obama administration's response to Russian interference in the 2016 elections?
 - Reading Notes: Imagine that you are advising a member of Congress on election security legislation. What policies would you recommend for the bill?
- Optional Reading – Russian Information Operations
 - Special Counsel Indictment of IRA Operatives (2017)
 - Special Counsel Indictment of GRU Operatives (2018)
 - Philip N. Howard et al., The IRA, Social Media, and Political Polarization in the United States, 2012-2018 (2018)
 - Renee DiResta et al., The Tactics and Tropes of the Internet Research Agency (2018)
 - MICHAEL McFAUL, FROM COLD WAR TO HOT PEACE (2018)
- Optional Reading – Disinformation in the 2016 Election
 - Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSPECTIVES 211 (2017)
 - Andrew Guess et al., Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 U.S. Presidential Campaign (2018)
 - Gordon Pennycook et al., *Prior Exposure Increases Perceived Accuracy of Fake News*, 147 J. EXPERIMENTAL PSYCH. 1865 (2018)
 - Andrew Guess et al., *Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook*, 5 SCI. ADVANCES (2019)
- Optional Reading – Chinese Information Operations
 - Gary King et al., *Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation*, 345 SCI. (2014)
 - Gary King et al., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, 111 AM. POL. SCI. REV. 484 (2017)

- Optional Reading – Election Security
 - Center for American Progress, Election Security in All 50 States (2018)
 - Center for Internet Security, A Handbook for Elections Infrastructure Security (2018)
 - Robby Mook et al., The State and Local Election Cybersecurity Playbook (2018)
 - Robby Mook et al., Cybersecurity Campaign Playbook (2017)
 - Stanford Cyber Policy Center, Securing American Elections (2019)
 - U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-20-267, DHS PLANS ARE URGENTLY NEEDED TO ADDRESS IDENTIFIED CHALLENGES BEFORE THE 2020 ELECTIONS (2020)

April 21 – Offensive Operations

Note: [Seny Kamara](#) from Brown will present at a lunch seminar before class. Highly recommended.

- Assigned Reading – Recent Events
 - Center for Strategic and International Studies, Significant Cyber Incidents Since 2006 (2020)
 - Reading Notes: For over a decade, some cybersecurity experts have warned of a devastating “digital Pearl Harbor” attack on the United States. How do you think that prediction of cyberwar compares to the reality of recent events?
- Assigned Reading – Deterrence and Attribution
 - David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT’L SEC. J. 531 (2011)
 - Reading Notes: Some policymakers have urged a redesign of the Internet with stronger identity mechanisms, to assist with attributing offensive operations. Do you think that is a worthwhile direction for federal policy? Do you think it is a feasible policy direction?
- Assigned Reading – U.S. Authorities
 - Department of Defense Authorities and Notification Requirements, 10 U.S.C. §§ 394-396, 484
 - The National Security Act, 50 U.S.C. § 3093
 - Reading Notes: Federal law draws a distinction between military offensive cybersecurity operations (under Title 10) and intelligence offensive operations (under Title 50). Do you think that distinction is clearly delineated in the provisions you read?
- Assigned Reading – U.S. Operational Structure
 - Department of Defense, Joint Chiefs of Staff, Doctrine on Cyberspace Operations (2018)
 - Reading Notes: The Department of Defense has a notoriously convoluted organizational structure for cybersecurity operations. How would you improve the structure?

- Assigned Reading – U.S. Policy
 - White House, National Cyber Strategy of the United States of America (Sept. 2018)
 - U.S. Department of Defense, Department of Defense Cyber Strategy Summary (Sept. 2018)
 - Reading Notes: A number of members of Congress (most prominently the late Senator McCain) have urged the Department of Defense to adopt a precise declaratory policy on how the United States will respond to offensive cybersecurity operations. DoD has responded with repeated delays and malleable policy statements (like you’ve just read). Why do you think that is? Do you think a precise declaratory policy is a good idea?

- Assigned Reading – International Law and Norms
 - NATO CCD COE International Group of Experts, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017)
 - Reading Notes: According to news reports, the U.S. and Israel collaborated to develop Stuxnet, malware that disabled centrifuges in the Iranian nuclear program. Having read the relevant Tallinn Manual provisions, do you believe the U.S. and Israel engaged in a “use of force” against Iran?

- Assigned Reading – Vulnerability Stockpiles
 - White House National Security Council, Vulnerabilities Equities Policy and Process for the United States Government (Nov. 15, 2017)

- Optional Reading – Significant Incidents
 - DAVID SANGER, *THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE* (2018)
 - KIM ZETTER, *COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD’S FIRST DIGITAL WEAPON* (2014)

- Optional Reading – Deterrence and Attribution
 - Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUDIES 4 (2015)
 - BEN BUCHANAN, *THE CYBERSECURITY DILEMMA* (2017)
 - HERBERT LIN & AMY ZEGART, *BYTES, BOMBS, AND SPIES* (2019)

- Optional Reading – Operational Practice
 - Fact Sheet on Presidential Policy Directive 20 (2013)
 - Note that PPD-20 and the successor executive order remain classified.
 - BEN BUCHANAN, *THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS* (2020)

- Optional Reading – International Law
 - Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012)
 - THOMAS RID, *CYBER WAR WILL NOT TAKE PLACE* (2013)

- Optional Reading – Vulnerability Stockpiles
 - UK GCHQ, The Equities Process (2019)
 - Canada CSE, Equities Management Framework (2019)

April 28 – Cybersecurity Defense

- Assigned Reading – Federal Cybersecurity Defense
 - GAO, Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions (2018)
 - The Federal Information Security Modernization Act of 2014 (FISMA), 6 U.S.C. §§ 3552, 3553, 3556
 - NIST’s Cybersecurity Authorities, 40 U.S.C. § 11331 and 15 U.S.C. §§ 272, 278g–3
 - There is an unusual volume of intricate statutory reading for this topic, since the material is so new and there are not (yet) good secondary sources.
 - Reading Notes: Starting from a blank slate, how would you structure responsibility within the federal government for defending federal systems?
 - Reading Notes: The five-part NIST Cybersecurity Framework has been very influential within the federal government. What do you think the value of the framework is? Do you think the value might be overstated?
- Assigned Reading – Critical Infrastructure Security
 - Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (2013)
 - The Homeland Security Act, 6 U.S.C. § 652 (Cyber and Infrastructure Security Agency Provisions)
 - The Cybersecurity Information Sharing Act, 6 U.S.C. §§ 1501, 1503, 1505
 - Reading Notes: What problems do you think the Cybersecurity Information Sharing Act aims to address? Do you think it will address those problems?
 - Reading Notes: Do you think CISA has the authorities needed to protect critical infrastructure? If not, what new authorities would you recommend providing?
- Assigned Reading – The U.K. Approach
 - U.K. National Cyber Security Centre, Guidance on the EU Directive on Network and Information Systems (2018)
 - Reading Notes: Compare and contrast how the U.K. has allocated responsibility for cybersecurity defense with the U.S. approach. Which do you think is preferable?
- Optional Reading – Executive Orders
 - National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, Cybersecurity Policy (2008)
 - Executive Order 13,636, Improving Critical Infrastructure Cybersecurity (2013)
 - Executive Order 13,691, Promoting Private Sector Cybersecurity Information Sharing (2015)

- Executive Order 13,800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)
- Executive Order 13,870, Strengthening America’s Cybersecurity Workforce (2019)
- Executive Order _____, Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services (2020)

- Optional Reading – Federal Civilian Agency Requirements
 - Please see the [Cybersecurity and Infrastructure Security Agency website](#) for a list of current requirements for federal civilian agencies (termed Binding Operational Directives and Emergency Directives).

- Optional Reading – Defense Sector Requirements
 - Department of Defense, Cybersecurity Maturity Model Certification (2020)

- Optional Reading – The EU Approach
 - The Directive on Security of Network and Information Systems, Commission Directive 2016/1148, 2016 O.J. (L 194) (EU)