

Between First and Fourth: Privacy and Speech on the Frontier of Technology

Privacy and free speech—two constitutional rights that often complement each other. In the information age, however, the tension between these values is increasingly apparent. Individuals, corporations, and governments create, use, store, and sometimes lose vast amounts of personal information. New technologies, databases, and systems—such as drones, Google Glass and biometrics—are being used at an increasing scale by both public and private actors. How can we use information without undermining privacy? How can we protect information without restricting free speech? These questions are not rhetorical. In this Study Group, we will explore the technologies, actors, and values at play in the space between speech and privacy in the information age.

The goal is to surface the legal and policy questions and gaps as these emerging technologies change the landscape, borrowing from an interdisciplinary perspective. Sessions will involve robust discussion and participation in a seminar-style format. Attorneys of the ACLU of Massachusetts will lead the conversation each week.

Week One: Introduction

When we talk about “free speech” and “the right to privacy,” what do we really mean? Why did the constitution restrict the government’s ability to infringe on those rights in the first place? What are the tensions between the First and Fourth Amendments? Within each Amendment? How do private actors fit into the framework of how we think about these rights?

- Required readings:
 - Excerpts from Neil M. Richards, *Intellectual Privacy*, 87 Tex. L. Rev. 387 (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108268
 - Excerpts from Barry P. McDonald, *The First Amendment and the Free Flow of Information: Towards A Realistic Right to Gather Information in the Information Age*, 65 Ohio St. L.J. 249 (2004), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1385430
 - Marvin Ammori, *Negative Liberty and What the First Amendment Ought to Be*, Concurring Opinions (Feb. 3, 2012), <http://concurringopinions.com/archives/2012/02/negative-liberty-and-what-the-first-amendment-ought-to-be-2.html>
 - Excerpts from Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1808071
 - Marjorie Cohn, *NSA Metadata Collection: Fourth Amendment Violation*, JURIST – Forum (Jan. 15, 2014), <http://jurist.org/forum/2014/01/marjorie-cohn-nsa-metadata.php>
- Optional readings (mainly for participants looking to familiarize themselves with the issues and legal rules we’ll be discussing in the reading group):
 - For a brief overview of the First and Fourth Amendments, see:
 - http://www.law.cornell.edu/wex/first_amendment
 - http://www.law.cornell.edu/wex/fourth_amendment
 - For resources on specific online speech and privacy topics, see:
 - <https://www.eff.org/issues/free-speech>

- <https://www.eff.org/issues/privacy>
- For more on the right to gather information, from a journalism perspective, see:
 - <http://www.rcfp.org/reporters-field-guide>

Week Two: Physical Surveillance

How do speech and privacy values come into conflict in the realm of physical surveillance technologies such as drones, Google Glass, surveillance cameras and automated license plate readers? What does it mean for private companies to have a First Amendment right to record video that may infringe on individual privacy? What are the privacy rights implicated by such surveillance? How does such surveillance implicate the First Amendment Right to Associate? Where do we—and where should we—draw a distinction between private and public actors?

- Required readings:
 - Excerpts from Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412
 - Excerpts from Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 Cal. L. Rev. Circuit 57 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257080
 - Ed Pilkington, *'We See Ourselves as the Vanguard': The Police Force Using Drones to Fight Crime*, The Guardian (Oct. 1, 2014), <http://www.theguardian.com/world/2014/oct/01/drones-police-force-crime-uavs-north-dakota>
 - Gary Mortimer, *Dallas Meat Packing Plant Investigated After Drone Images Reveal Pollution*, sUAS News (Jan. 23, 2012), <http://www.suasnews.com/2012/01/11389/dallas-meat-packing-plant-investigated-after-drone-images-reveal-pollution/>
 - Vigilant Solutions, *Lawsuit Challenges State of Utah Ban on License Plate Readers as Unconstitutional Censorship of Photography and Violation of 1st Amendment* (Feb. 13, 2014), http://vigilantsolutions.com/press/drn_vigilant_utah_lpr_federal_lawsuit
 - Tim Cushing, *License Plate Reader Company Sues Another State For 'Violating' Its First Amendment Right To Build A 1.8-Billion-Image Database*, TechDirt (June 18, 2014), <https://www.techdirt.com/articles/20140613/09224127569/license-plate-reader-company-sues-another-state-violating-its-first-amendment-right-to-build-18-billion-image-database.shtml>
 - Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, Ars Technica (Sept. 25, 2013), <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>
 - Dhruvi Shah, *CCTV Site Internet Eyes Hopes to Help Catch Criminals*, BBC (Oct. 4, 2010), <http://www.bbc.co.uk/news/uk-11460897>
- Optional reading:
 - Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2458076

- For information on the current state of drone legislation, see:
 - <https://www.aclu.org/blog/technology-and-liberty/year-drone-roundup-legislation-passed-year>
 - <https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states>
- For an overview of privacy tort law, see:
 - <http://www.rcfp.org/photographers-guide-privacy/primer-invasion-privacy>

Week Three: Infrastructure of the Internet

The government is increasingly involved in the provision of broadband internet access by becoming involved in the provision of municipal WiFi and municipal fiber or by regulating private service providers. To what extent should we be concerned with the ability of private internet providers to control what users see and access? What are the benefits and concerns if the government owns the Internet instead? Should the government regulate private service providers to protect privacy and speech? What system can we design that would best protect our constitutional rights of speech, privacy, and access to information in this changing landscape?

- Required reading:
 - Christina Pazzanese, *So, Who Owns the Internet?*, Harvard Gazette (Jan. 7, 2014), <http://news.harvard.edu/gazette/story/2014/01/so-who-owns-the-internet/>
 - Excerpts from Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 Berkeley Tech. L.J. 1115, 1115 (2005), <http://ssrn.com/abstract=1003415>
 - Jeremy Hsu, *Christopher Yoo Thinks Net Neutrality's End Might Not be So Bad*, IEEE Spectrum (Apr. 28, 2014), <http://spectrum.ieee.org/tech-talk/telecom/internet/why-net-neutralitys-end-may-not-be-so-bad>
 - Jeffery Rosen, *The Delete Squad*, New Republic, (Apr. 29, 2013), <http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules>
 - Grant Gross, *Groups: FCC Shouldn't Overturn State Laws Against Municipal Broadband*, PCWorld (Sep. 2, 2014), <http://www.pcworld.com/article/2601200/groups-fcc-shouldnt-overturn-state-laws-against-municipal-broadband.html>
 - Rebecca Chao, *FireChat Wasn't Meant For Protests. Here's How It Worked (Or Didn't) at Occupy Central*, TechPresident (Oct. 10, 2014), <http://techpresident.com/news/25304/firechat-wasn%E2%80%99t-meant-protests-here%E2%80%99s-how-it-worked-or-didn%E2%80%99t-occupy-central>
- Optional reading
 - For an more on current and proposed regulation of the Internet, see:
 - <http://www.fcc.gov/openinternet>
 - <http://www.whitehouse.gov/net-neutrality>
 - For more on alternatives to the private-provider Internet, see:
 - <http://www.muninetworks.org/content/key-points>
 - <http://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/>

Week Four: Data, Speech, and Privacy

Is there a line where data ceases to be protected speech, and if so, how do we draw that line? Are computer code or algorithms protected speech? Do arguments that data is not speech for the purposes of the First Amendment create tension with arguments that the same data contains information that triggers Fourth Amendment protections? What happens when data is a potential precursor to both protected speech and forbidden government searches?

- Required reading:
 - Orin Kerr, *D.C. Circuit Introduces “Mosaic Theory” Of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, The Volokh Conspiracy (Aug. 6, 2010), <http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/>
 - Lois Beckett, *Everything We Know About What Data Brokers Know About You*, ProPublica (June 13, 2014), <http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>
 - Excerpts from Jane Bambauer, *Is Data Speech?*, 66 Stan. L. Rev. 57 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231821
 - Stephen Wermeil, *Plain English*, SCOTUSblog (June 24, 2011), <http://www.scotusblog.com/2011/06/plain-english-2/>
 - Tim Wu, *Free Speech for Computers*, N.Y. Times (June 19, 2012), http://www.nytimes.com/2012/06/20/opinion/free-speech-for-computers.html?_r=0
 - Gabe Rottman, *Do Androids Dream of Electric Speech?*, ACLU Free Future Blog (June 21, 2012), <https://www.aclu.org/blog/free-speech-national-security-technology-and-liberty/do-androids-dream-electric-speech>
- Optional reading:
 - For more on private data collection, see:
 - <http://www.npr.org/blogs/alltechconsidered/2013/09/04/218889785/get-a-glimpse-of-the-data-marketers-have-about-you>
 - For more on the question of what constitutes speech, see:
 - <http://cyber.jotwell.com/from-google-to-tolstoy-bot-should-the-first-amendment-protect-speech-generated-by-algorithms/>.
 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2302786.
 - For one possible future of the data-as-speech question, see:
 - http://www.slate.com/blogs/future_tense/2014/05/15/robots_ai_deserve_first_amendment_protection.html

Week Five: Free Speech on the Internet

How and why does the Internet raise particular, unique tensions between speech and privacy? How do we balance access to public information against the “right to be forgotten”? How do we balance the right to free speech on the internet against cyber-bullying concerns, particularly with respect to schools? Should the speech/privacy balance play out differently on the Internet?

- Required reading

- Excerpt from Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012), <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>
- Eric Posner, *We All Have the Right to Be Forgotten*, Slate (May 14, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html
- Alison Frankel, *California Finds 'Right to Privacy' for Anonymous Online Commenters*, Reuters (May 16, 2014), <http://blogs.reuters.com/alison-frankel/2014/05/16/california-finds-right-to-privacy-for-anonymous-online-commenters/>
- Matt Peckham, *The New York Bill that Would Ban Anonymous Online Speech*, Time (May 24, 2012), <http://techland.time.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/>
- Frank LoMonte, *UM Cries Wolf over Johnson Privacy Issue*, Great Falls Tribune (Nov. 17, 2014), <http://www.greatfallstribune.com/story/opinion/guest-opinions/2014/11/17/um-cries-wolf-johnson-privacy-issue/19195761/>
- David R. Wheeler, *Do Students Still Have Free Speech in School?*, The Atlantic (Apr. 7, 2014), <http://www.theatlantic.com/education/archive/2014/04/do-students-still-have-free-speech-in-school/360266/>
- Optional reading
 - For more on anonymization, identification, and preservation technologies, see:
 - <http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/>
 - <http://mashable.com/2011/09/02/supercookies-internet-privacy/>
 - <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>
 - http://mirrorasyoulink.org/?page_id=2
 - For a variety of views on the anonymity and bullying debate, see:
 - <http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls>

Week Six: The Relationship between Government, Corporations, and Individuals

How do the interactions between these three actors raise distinct speech and privacy issues? For example, ever since Snowden's disclosures created an uproar over the extent to which private companies were willingly handing over users' data to the government, some companies have been racing to one-up one another in demonstrating their commitment to privacy. At the same time, many of these companies continue to collect such sensitive information for themselves. What do we think about these simultaneous trends? What does this mean for future relationships between the government and corporations? Can individuals choose to give data to private companies but not the government (or vice versa)? Relatedly, to what extent might the use of privacy tools such as Tor affect the Fourth Amendment calculus of whether users have reasonable expectation of privacy in their information?

- Required reading:
 - Jack Balkin, *Old-School/New-School Speech Regulation*, Harvard Law Review (June 20, 2014), <http://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/>

- Steven Levy, *How the NSA Almost Killed the Internet*, Wired (Jan. 7, 2014), <http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/>
- Mike Masnick, *NSA: If Your Data is Encrypted, You Might be Evil, So We'll Keep It Until We're Sure*, TechDirt (June 21, 2013), <https://www.techdirt.com/articles/20130620/15390323549/nsa-has-convicted-fisa-court-that-if-your-data-is-encrypted-you-might-be-terrorist-so-itll-hang-onto-your-data.shtml>
- Dana Liebelson, *Google, Yahoo, Facebook and Twitter Have a New Lobbying Target—the NSA*, Mother Jones (Nov. 15, 2012), <http://www.motherjones.com/politics/2013/11/nsa-bills-google-facebook-yahoo-twitter-lobbying>
- Kim Zetter, *Twitter Sues the Government for Violating its Free Speech Rights*, Wired (Oct. 7, 2014), <http://www.wired.com/2014/10/twitter-sues-government/>
- Samuel Gibbs, *Privacy watchdog files complaint over Facebook emotion experiment*, The Guardian (July 4, 2014), <http://www.theguardian.com/technology/2014/jul/04/privacy-watchdog-files-complaint-over-facebook-emotion-experiment>
- Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 Yale L.J. F. 73 (2014), <http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud>