Tentative Syllabus

IS 97: Variable Topics Seminar in Information Studies

Invasion of the data snatchers: Privacy and surveillance in the digital age

Instructor Diana L. Ascher

Time Tuesdays & Thursdays, 1pm – 3:05pm **Location** GSEIS 111

Office Hours Tuesdays, 3:30pm – 4:30pm; schedule via http://doodle.com/sigxdc7im94cdfc8 **Email** dianaascher@ucla.edu

---

Description

In a recent study from the Pew Research Center, more than 48,000 adults around the globe were asked about their perceptions of America's national security activities. A majority of the respondents in nearly all of the 44 countries polled said they oppose the U.S. government's monitoring of emails and phone calls of foreign leaders and citizens. Most of the Americans surveyed said the email and phone surveillance of foreign leaders is acceptable, but they are divided on whether eavesdropping on other nations' average citizens is appropriate. Most of those surveyed (from the United States and the 43 other nations) support surveillance of suspected terrorists and disapprove of spying on American citizens.

Following Edward Snowden's revelations about U.S. National Security Administration (NSA) surveillance, sentiment about the nation's reputation as a defender of civil liberties began to sour. In Brazil and Germany, America's reputation plummeted after it was revealed that the United States had listened to the telephone conversations of both nations' leaders. Pew reports that, in nearly two thirds of the nations surveyed in both 2013 and 2014, respondents were much less inclined to believe that the U.S. government respects individual liberties.

Even though public support for these American national security strategies continues to fall, a median of 65% of the people in 43 countries hold the United States in relatively high regard, with overall approval scores much the same as last year. How is it that the American government can engage in surveillance activities of which most people disapprove, yet maintain a relatively positive public image?

The primary aim of this course is to familiarize you with the multiple, complex forces that contribute to this perplexing phenomenon. We will examine the history of privacy and surveillance to establish what expectations citizens have with regard to their personal information, and then explore how those expectations are shaped over time, particularly with the advent of new technology. In the process, you will also learn to evaluate information requests and agreements from a critical perspective at a time when "the Internet of things" is expanding rapidly, and it appears that one must sacrifice privacy in return for information access and social engagement.

Instructional Objectives

At the end of this course, you will be able to:

1. Describe the relevance of the First and Fourth Constitutional Amendments to contemporary notions of freedom and privacy rights.
    a. Distinguish between freedom of speech and free information access, and understand why some people conflate these ideas.
    b. Delineate the legislation that enabled the U.S. government to conduct surveillance without the oversight ensured by the Fourth Amendment.
2. Articulate the reasons why government and corporate entities want to access your personal digital information and the ways in which they have been able to motivate citizens to part with their data voluntarily.
    a. Explain how companies entice people to work for them for free, and describe the tradeoff between Internet affordances and privacy.
    b. Describe how powerful authorities employ the "triple appeal principle" and information control to minimize the relative value of citizens' privacy.
    c. Recognize common misconceptions about the seriousness of privacy breaches and voluntary disclosure.
3. Explain the filter bubble and its potential effects on information seekers.
4. Argue both sides of the privacy/surveillance debate, drawing from course readings and class discussions.
5. Describe the nature and implications of privacy policies, terms of service, and third-party cookies in both personal and work contexts.
    a. Identify and distinguish between innocuous legalese and significant ceding of privacy rights in a variety of situations.
6. Recount an experience in which you felt compelled to provide personal information that, in retrospect, you did not want to give or should not have given.
    a. Suggest appropriate strategies to prevent, avoid, and mitigate the effects of surveillance strategies based on the class discussions and course readings.
    b. Offer strategies for self-regulation of personal information.
    c. Refrain from transmitting naked selfies via Snapchat, Instagram, and other social media networks.

Resources

http://dianaascher.com/privacy-and-surveillance
https://ccle.ucla.edu/course/view/151A-INFSTD97-1

Requirements and Evaluation

Assignment	Expectation	Proportion of Final Grade
Weekly blog entry	Select a current privacy or surveillance issue and report on at least two perspectives, citing scholarly articles; APA style. Your final blog entry must be a reflection on one or two of the group presentations, excluding yours.	25%
Group project	Projects will be assigned according to ranked topic preference. The final two class sessions will be devoted to your presentations. You must attend both sessions.	25%
Class preparation and participation	Readings must be completed prior to class. They're fun readings. You are encouraged to engage during class, but if that's not your thing, you also may contribute to the discussion forum to fulfill this requirement. Contributions in both forms must be thoughtful and substantive.	25%
Exam	In order to reserve time at the end of the course for your group presentations, the final exam will be unorthodox, like your Snapchats. Each week you'll have one short essay question to answer based on the readings. Don't freak out; it's open book.	25%

Course Schedule

Session	Topic	Required Reading
1	Getting to know you What is privacy? Types of privacy History of privacy Why should I care?	Complete the survey at http://dianaascher.com/privacy-and-surveillance-wk1-survey; save your confirmation number Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101-127. Solove, D. J. (2006). *A Taxonomy of Privacy*. 154. Warren, S. D., Brandeis, L. D. (1890). The right to privacy. *Harvard Law Rev 4*(5), pp. 93–220.
2	Power and surveillance	So Are We Living in 1984? (2013, June 11). *The New Yorker*. Balkin, J. M. (2008). The Constitution in the National Surveillance State. *Minnesota Law Review*, 93(1), 2008; Yale Law School, Public Law Working Paper No. 168. Hsinchun, C., et al. (2009). Intelligence and security informatics. In *Encyclopedia of Library and Information Sciences, (3rd Ed.)*. New York, NY: Taylor and Francis. Morozov, E. (2011). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs. (Introduction) Nissenbaum, H. (In press). Assuring a role for 'respect for context' in protecting privacy. In M. Rotenberg, et al. (Eds.), *Visions of Privacy in the Modern Age*. EPIC.

Session	Topic	Required Reading
3	Right to be forgotten Management of personal digital assets	Amann, M., et al. (2014, May 20). EU court ruling a victory for privacy. (D. Lindsey & J. Paulick, Trans.). *Spiegel Online*. Retrieved from: http://www.spiegel.de/international/business/court-imposes-right-to-be-forgotten-on-google-search-results-a-970419.html Draper, N. A. (2014). The new reputation custodians: Examining the industrialization of visibility in the reputation society. In L. Lievrouw (Ed.), *Challenging Communication Research*. New York, NY: Peter Lang. Hill, K. (2013, April 11). Will you use Google's death manager to let loved ones read your email when you die? *Forbes*. Retrieved from: http://www.forbes.com/sites/kashmirhill/2013/04/11/google-death-manager-new-feature-to-tell-the-company-what-to-do-with-your-data-when-you-die/
4	Corporate data collection and sale Algorithm cognizance	Mager, A. (2012). *Algorithmic ideology*. Information, Communication & Society, 15(5), pp. 769-787. Stanford. (2011, September 16). The Googlization of everything (and why we should worry [Video file]. Retrieved from: https://www.youtube.com/watch?v=AwLwaB7pJC4 Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin. Resnick, P., et al. (2013). *Bursting your (filter) bubble: Strategies for promoting diverse exposure*. In Proceedings of the 2013 conference on Computer supported cooperative work companion (CSCW '13). New York, NY: ACM.
5	Policy tradeoffs Global variance	ACLU. (2015, February 9). Tech Industry Stands with Sen. Leno to Modernize Digital Privacy Protections. Retrieved from: https://www.aclunc.org/news/tech-industry-stands-sen-leno-modernize-digital-privacy-protections Conley, A., et al. (2014). Making smart decisions about surveillance: A guide for communities. Sacramento, CA: ACLU.
6	Whistleblowers	PBS Frontline. (2014, May 13 & May 21). *United States of secrets* [video]. Retrieved from: http://www.pbs.org/wgbh/pages/frontline/united-states-of-secrets/
7	Technology's regulatory role	Camenisch, J. (2015, January 28). Protecting your personal data using the cloud [video]. Retrieved from: http://asmarterplanet.com/blog/2015/01/protecting-data-using-cloud.html Elkin-Koren, N. (2001). Let the crawlers crawl: On virtual gatekeepers and the right to exclude indexing. *University of Dayton Law Review*, 26, pp. 180-209.
8	Ethics & Big Data International challenges	Bamberger, K., & Mulligan, D. (2011). Catalyzing privacy: New governance, information Practices, and the business organization. *Law & Policy*, 33. OR Bamberger, K. A., & Mulligan, D. K. (forthcoming 2015). *Catalyzing privacy: Lessons from regulatory choices and corporate decisions on*

Session	Topic	Required Reading
		both sides of the Atlantic. MIT Press. Crawford, K., et al. (2014). Critiquing big data: Politics, ethics, epistemology. *International Journal of Communication* 8, pp. 1663–1672. Richards, N. M., & King, J. H. *Big data and the future for privacy.* [Working paper.] (October 19, 2014). Available at SSRN: http://ssrn.com/abstract=2512069 or http://dx.doi.org/10.2139/ssrn.2512069
9	Internet of things Technology on the horizon	Cellan-Jones, R. (2015, January 26). Office puts chips under staff's skin. *BBC News.* http://www.bbc.com/news/technology-31042477 Cunningham, McKay, Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm (January 14, 2015). Groningen Journal of International Law, Vol. 2, Ed. 2, 2014. Available at SSRN: http://ssrn.com/abstract=2549849 Roman, R., et al. (2011) Securing the Internet of Things. *IEEE Comput 44*(9), pp. 51–58.
10	Cyberterrorism Data breaches	Abelson, R., & Creswell, J. (2015, February 6). Data breach at Anthem may lead to others. *The New York Times.* Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication: The International Journal of Media and Culture, 13*(1), pp. 74-86. Shakarian, J., et al. (2015). Cyber attacks and public embarrassment: A survey of some notable hacks. Excerpt from *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* http://www.sciencedirect.com/science/book/9780124078147
11	Presentations	
12	Presentations	