Privacy and Information Technology

Fall, 2017, UCLA Information Studies 289-2
Wednesday, 9am-12:20pm, IS Room 245
Christine L. Borgman, Distinguished Professor & Presidential Chair
235 GSE&IS bldg, 310-825-6164; Christine.Borgman@ucla.edu

Table of Contents

Course Structure and Logistics

Course Description

Privacy is a broad topic that covers many disciplines, stakeholders, and concerns. This course addresses the intersection of privacy and information technology, surveying a wide array of topics of concern for research and practice in the information fields. Among the topics covered are the history and changing contexts of privacy; privacy risks and harms; law, policies, and practices; privacy in searching for information, in reading, and in libraries; surveillance, networks, and privacy by design; information privacy of students; uses of learning analytics; privacy associated with government data, at all levels of government; information security, cyber risk; and how privacy and data are governed by universities. We will touch on relationships between privacy, security, and risk; on identification and re-identification of individuals; privacy-enhancing technologies; the Internet of Things; open access to data; drones; and other current issues in privacy and information technology.

Course Objectives

The course is intended for graduate students in information studies, social sciences, and technology who are interested in privacy, social behavior, policy, or professional practices. It may also be suitable for graduate students in law, health, humanities, and the many other fields in which privacy issues arise. We will survey professional issues suitable for master's students, and research and scholarly issues suitable to doctoral students.

Course Materials

Two books are required, each widely available in paperback and digital editions: (Lane, Stodden, Bender, & Nissenbaum, 2014; Solove, 2010).

Other readings are linked from or posted in the CCLE site for this course.

Office Hours

Thursdays, 2-4pm. For specific hours and dates, please sign up via the Doodle link: https://doodle.com/poll/tz254tka689uxz5d. Other office hours by appointment.

Assignments and Grading

As a graduate seminar, classroom time is devoted to discussion of the readings and presentations by guest speakers. Given the broad array of topics and issues covered in

one term, the reading list is extensive. At the end of each class session, the instructor will introduce the readings for the following week. Students are expected to read all of the required materials in advance of each session, and be prepared to discuss and compare their interpretations. Class participation is graded accordingly. The recommended readings augment the required readings for those who wish more depth on any topic, and as a starting point for developing term papers.

Please note that reading assignments are "front loaded," with more reading due in the first weeks of the term to lay foundations, and no reading required for Week 10. The last week of the term is devoted to student presentations of their term projects.

Weight of class assignments and activities:

Term paper: 40%
Two short assignments @ 20% each
Class participation: 20%

Summary of Assignment due dates

See individual documents for assignment details

Assignment 1: Tracking Online Activities

- October 4, Week 1: Assignment discussed in class.
- Tuesday, Oct 24, Week 4: Report due to CCLE.

Assignment 2: Data Breaches

- October 25, Week 4: Assignment discussed in class.
- Tuesday, Nov 21, Week 8: Report due to CCLE.

Term Project

- Oct 4 (week 1): Assignment discussed in class.
- Tuesday, Oct 17 (week 3): Proposal due to CCLE.
- Weeks 3-10: Meet with instructor during office hours.
- Tuesday, Nov 14 (week 7). Extended outline and bibliography due to CCLE.
- Dec 6 (week 10): Class presentation.
- Dec 12, 5pm (Tuesday of exam week). Paper due to CCLE.

Topics, Readings, and Guest Speakers

Short descriptions of the readings are presented in each week, with a full list of references at the end of this syllabus.

Week 1, Oct 4: Introduction to privacy and information technology

The course begins with a general overview of privacy in the context of information studies. Privacy is a broad topic that covers many disciplines, stakeholders, and concerns. We will focus on why privacy is so difficult to define concisely, and the history of the context. "Information privacy" will be distinguished from other kinds of privacy. We will also introduce relationships between privacy, security, and risk, while bounding the course discussion at the intersection of privacy and information technology. Week 1 readings are deliberately extensive to frame the course, as we will be returning to these topics throughout the term.

Assignment 1 and Term Project will be discussed in class.

Required readings:

(Acquisti, 2014) The economics and behavioral economics of privacy (in Lane, et al).

(Solove, 2010) Understanding Privacy [full book is required reading; not linked or posted on CCLE].

(Warren & Brandeis, 1890) The right to privacy.

("The world's most valuable resource is no longer oil, but data," 2017).

Recommended readings:

(Acquisti, Brandimarte, & Loewenstein, 2015) Privacy and human behavior in the age of information.

(J. E. Cohen, 2000) Examined lives: Informational privacy and the subject as object.

(R. Gellman, 2017) Fair information practices: a basic history.

(Kang, 1998) Information privacy in cyberspace transactions.

(McCreary, 2008) What was privacy?

(Nissenbaum, 2011) A contextual approach to privacy online.

Week 2, Oct 11: Privacy risks and harms; algorithmic privacy

In week 2 we address some of the risks and harms to individuals associated with privacy. Privacy can involve matters such as personal safety, health, financial harms, damage to social relationships, academic freedom, and human rights. Many of the individual data points collected may appear harmless on their own, but become much more valuable when aggregated. Algorithms that can collect, mine, and make decisions about people are a growth industry. This week's readings are a multi-disciplinary mix of short and long, drawn from computer science, law, and public policy. Later in the term we will return to questions of cyber-risk and information security.

Required Readings:

(Kirkpatrick, 2017) It's not the algorithm, it's the data.

(Kreuter & Peng, 2014) Extracting information from big data: Issues of measurement, inference, and linkage.

(Lane, Stodden, Bender, & Nissenbaum, 2014) Editors' introduction [required book].

(Solove, 2007) 'I've got nothing to hide' and other misunderstandings of privacy.

("Universal Declaration of Human Rights | United Nations,") See especially Article 12 http://www.un.org/en/universal-declaration-human-rights/.

Recommended readings:

(Berghel, 2014) Privacy informatics: a primer on defensive tactics for a society under siege.

(Calo, 2010) The boundaries of privacy harm.

(Kelley, Cranor, & Sadeh, 2013) Privacy as part of the app decision-making process.

(C. Landwehr, 2016) Privacy research directions.

(Tsai, 2009) The impact of salient privacy information on decision-making.

Week 3, Oct 18: Privacy law, policies, and practices

Privacy practices date back centuries, having evolved across countries and cultures. Privacy policies related to information technology began to be codified in the 1960s and 1970s under the general rubric of Fair Information Practices (FIPS). Policies in the U.S. tend to focus on social sectors (e.g., government, business, universities) or types of records (e.g., health, library circulation, video rentals), whereas Europe takes a broader view of a "right to privacy." This week we will survey these policies to provide a framework for the evolution of privacy practices in an era of "big data," social media, Internet of Things, cyber hacking, ransomware, and other recent developments. We have two distinguished speakers scheduled, both of whom are at the forefront of privacy law and policy in higher education.

Guest speakers: Amy Blum, Managing Counsel, Legal Affairs, UCLA; Kent Wada, Chief Privacy Officer, UCLA

Weeks 3-10: Meet with instructor during office hours to discuss you term project topic and proposal. We will brainstorm length and include the topic, working title, abstract, outline, preliminary biography, and target journal.

Term Paper Proposal due on CCLE by 12:00AM the night before class.

Required readings:

(Chin & Lin, 2017)). China's all-seeing surveillance state is reading its citizens' faces

(Elias, 2014) A European perspective on research and big data analysis.

("Nowhere to hide: What machines can tell from your face," 2017)

(Ohm, 2014) Changing the rules: general principles for data use and analysis.

(Solove, 2010) Understanding privacy [read for week 1; please review].

(Strandberg, 2014) Monitoring, datafication, and consent: legal approaches to privacy in the big data context.

(Sullivan, 2017) Your social security number isn't a secret.

(University of California, Office of the President, 2017b) EU General Data Protection Regulation; 1-page summary of recommendations to universities

Review these major privacy policy documents:

(EU Data Directive, 2016) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016). Retrieved from http://data.europa.eu/eli/dir/2016/680/oj.

(Family Educational Rights and Privacy Act of 1974, n.d.) e-CFR: Title 34: Education, Title 34: Education, and Electronic Code of Federal Regulations § Part 99—Family Educational Rights and Privacy. Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33.

(*Fair Information Practice Principles (FIPPS) | Homeland Security*, 2008). Retrieved from https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

(Health Insurance Portability and Accountability Act of 1996, 1996) An act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes., Pub. L. No. 104–191 (1996). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191.

("Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission," 1977) Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission. (1977, July). Retrieved August 11, 2017, from https://epic.org/privacy/ppsc1977report/.

("Rules and Policies - Protecting PII - Privacy Act," n.d.) Rules and Policies - Protecting PII - Privacy Act. (n.d.). Retrieved from https://www.gsa.gov/portal/content/104256

Recommended readings:

(Allen & Rotenberg, 2015) Privacy, law, and society.

(Bamberger & Mulligan, 2011) Privacy on the books and on the ground.

(Cranor, 2012) Necessary but not sufficient: standardized mechanisms for privacy notice and choice.

(Leon et al., 2011) Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising (Revised May 10, 2012).

(Lessig, 2000) Code: and other laws of cyberspace.

(Office of the Press Secretary, The White House, 2012) Fact sheet: plan to protect privacy in the internet age by adopting a consumer privacy bill of rights.

(Reidenberg et al., 2014) Disagreeable privacy policies: mismatches between meaning and users' understanding.

(Rotenberg, 2016) Privacy law sourcebook 2016.

(Solove & Hartzog, 2013) The FTC and the new common law of privacy.

Week 4, Oct 25: Information searching, reading, and libraries

Individual privacy is at risk when searching for information; reading online or downloading files; reading documents on eReaders; or purchasing or borrowing books and materials. Libraries established an ethic of protecting the information seeking and reading behaviors of their patrons long before digital technology and information networks. State laws that protect library circulation records, for example, do not transfer easily to electronic publishing and ebooks. Similarly, the "right to read anonymously" has been eroded in the current marketplace for digital content, including scholarly and trade publishing. This week will survey the past, present, and potential future of privacy exposure and protection in the course of searching and reading, especially as they apply to broader social concerns in access to information. Our readings include a classic legal article and an extensive new analysis of the current environment of library privacy.

Assignment 1 due on CCLE by 12:00AM the night before class.

Assignment 2 will be discussed in class.

Required readings, organized by category:

Library privacy issues:

(J. E. Cohen, 1997) A right to read anonymously: a closer look at "copyright management" in cyberspace.

(Harper & Oltmann, 2017) Big data's impact on privacy for librarians and information professionals.

(Lynch, 2017) The rise of reading analytics and the emerging calculus of reader privacy in the digital world.

FBI Library Awareness Program:

(Ault, 1990) The FBI's library awareness program: is big brother reading over your shoulder?

(Bowers, 2006) Privacy and library records.

(H. Cohen & Minow, 2006) Intellectual freedom in libraries: then and now.

Library, information, and archives codes of conduct:

(ALA, 2006) Privacy: an interpretation of the library bill of rights.

(ARMA, n.d.) Code of professional responsibility.

(SAA, n.d.) Core values statements and code of ethics.

(SLA, n.d.) SLA Professional ethics guidelines.

Sites to visit:

("EPIC - Electronic Privacy Information Center," n.d.) https://www.epic.org/.

("Freedom to Read Foundation," n.d.) http://www.ftrf.org/.

Recommended readings:

(Library Bytegeist, n.d.) #6 Talking privacy with librarians.

Week 5, Nov 1: Surveillance, Networks, and Privacy by Design

The ability to surveil individuals in their daily activities is among the most common threats to privacy. Early designs of computer networks focused much more on efficiency than on security and privacy, as these were not considered significant threats at the time. Recent work to redesign computer networks, such as progress on Named Data Networks, and design of new applications, devices, and protocols to enhance privacy are necessary – if rarely sufficient – steps toward more private and secure online activities. We will touch on the use of technical devices to observe individuals in public and private spaces, such as drones and security cameras, as these also create digital records.

Prof. Shilton, our guest speaker for this week, conducts research on ethics, values, and design of privacy enhancing computer networks.

Guest speaker (by video): Prof. Katie Shilton, University of Maryland

Required readings:

(Bennett, 2010) Privacy advocates and surveillance; Introduction and chapter 1, p. ix-23.

(Cavoukian, 2011) Privacy by design: The 7 foundational principles.

(Doe, 2014) With genetic testing, I gave my parents the gift of divorce.

(Greene & Shilton, 2017) Platform privacies: governance, collaboration, and the different meanings of "privacy" in iOS and Android development.

(Harris, 2013) Privacy on the go - recommendations for the mobile ecosystem.

(Klarreich, 2012) Privacy by the numbers: a new approach to safeguarding data.

(Mulligan, Koopman, & Doty, 2016) Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy.

(Rubinstein & Good, 2012) Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents.

(Stark, 2016) UC Unmanned Aircraft System Safety | UCOP.

Recommended readings:

(Acquisti, Gross, & Stutzman, 2014) Face recognition and privacy in the age of augmented reality.

(Angwin, 2014) Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance.

(B. Gellman & Soltani, 2013) NSA collects millions of e-mail address books globally.

(Bamberger & Mulligan, 2015) Privacy on the Ground: Driving Corporate Behavior in the United States and Europe.

(Bamford, 2014) Edward Snowden: the untold story.

(Bennett, 2010) The privacy advocates: resisting the spread of surveillance.

(Fung, Wang, Chen, & Yu, 2010) Privacy-preserving data publishing: a survey of recent developments.

(Greenwald, MacAskill, Poitras, Ackerman, & Rushe, 2013) Microsoft handed the NSA access to encrypted messages.

(Gymrek, McGuire, Golan, Halperin, & Erlich, 2013) Identifying personal genomes by surname inference.

(Jarvis, 2014) National park system unmanned aircraft – interim policy.

(Mayer, 2012) Third-party web tracking: policy and technology.

(Montjoye, Radaelli, Singh, & Pentland, 2015) Unique in the shopping mall: On the reidentifiability of credit card metadata.

(Schneier, 2000) Secrets and lies: digital security in a networked world.

(Schneier & Banisar, 1997) The electronic privacy papers: documents on the battle for privacy in the age of surveillance.

(Shilton, 2009) Four billion little brothers?: privacy, mobile, phones, and ubiquitous data collection.

(Shilton, Burke, Claffy, & Zhang, 2016) Named data networking; CACM

(Shilton & Greene, 2017) Linking platforms, practices, and developer ethics: levers for privacy discourse in mobile application development.

(Timberg, 2014) For sale: Systems that can secretly track where cellphone users go around the globe.

(Wang et al., 2011) "I regretted the minute I pressed share": A qualitative study of regrets on Facebook.

Week 6, Nov 8: Privacy in the Internet of Things

The *Internet of Things*, also called the *Internet of Everything*, has been emergent for a decade or two. The general idea is that most "things," from thermostats to children's toys, will be connected to the Internet, each with its own unique identifier. Such technologies are sufficiently advanced that many of today's technologies are internet-enabled, often sending information in the background. Consumers may be unaware of the information that their devices know them, or about the information being delivered to manufacturers, stores, or third-party vendors. Once networked, these data can be combined to build rich profiles of individuals, households, workplaces, and companies. Similarly, these devices are being hacked as they were not designed with security in mind. Voice controlled systems such as Amazon Echo / Alexa and Google Home offer convenience at an unknown price for privacy.

Required readings:

(Berman & Cerf, 2017) Social and ethical behavior in the internet of things.

(Burns, Johnson, & Honeyman, 2016) Medical device security.

(Lindqvist & Neumann, 2017) The future of the internet of things.

(Peppet, 2014) Regulating the internet of things: first steps toward managing discrimination, privacy, security, & consent.

(Madrigal, 2017) The mysterious printer code that could have led the FBI to Reality Winner.

(Spinks, 2017) Using a physical fitness app taught me the scary truth about why privacy settings are a feminist issue.

Baby Monitors and Alexa (read at least two of these):

(Darrow, 2017) Amazon may share your Alexa conversations with developers.

(Barrett, 2017) Amazon's 'Echo Look' could snoop a lot more than just your clothes.

(Edwards, 2017) Alexa takes the stand: listening devices raise privacy issues.

(Edwards, 2016) How web cams helped bring down the internet, briefly.

(Jordan, 2016) From toasters to baby monitors, IoT's role in cyberattacks.

(Moynihan, 2016) Alexa and Google home record what you say. But what happens to that data?

Recommended readings:

(Dutton & Borgman, 2014) Society and the Internet of Things.

(Howard, 2015) How the Internet of Things may set us free or lock us up.

Week 7, Nov 15: Privacy and Government Data

Early concerns about privacy and surveillance in databases focused on government information. While much of the concern has shifted to business surveillance, government information on individuals and individuals' access to government information continue to raise substantial privacy issues. New uses of government information, such as city services to customize public transportation based on transit patterns, pose new kinds of tradeoffs in access and privacy. Prof. Washington is an expert on government information, information retrieval, and access to information by and about government.

Guest speaker: Prof. Anne Washington, School of Public Policy, George Mason University and Visiting Fellow, Data and Society

Term paper extended outline and bibliography due on CCLE by 12:00AM the night before class.

Required readings:

(Ardia & Klinefelter, 2015) Privacy and court records.

(Goerge, 2014) Data for the public good: challenges and barriers in the context of cities.

(Koonin & Holland, 2014) The value of big data for urban science.

(McCarthy & Yates, 2010) The use of cookies in Federal agency web sites: privacy and recordkeeping issues.

(R. Gellman, 1995) Public records—access, privacy, and public policy.

(Washington, 2014) Government information policy in the era of big data.

Recommended Readings:

(Agre, 1994) Surveillance and capture: two models of privacy.

(Bamford, 2007) Body of secrets: anatomy of the ultra-secret National Security Agency: from the Cold War through the dawn of a new century.

(Bamford, 2014) Edward Snowden: The untold story.

(Bamford, 2017) Washington's ministry of preemption.

(Munson et al., 2012) Sunlight or sunburn: a survey of attitudes toward online availability of US public records.

(Ramirez, 2016) Protecting consumer privacy in the digital age: reaffirming the role of consumer control.

(Solove, 2001) Access and aggregation: public records, privacy and the constitution.

(Yaco, 2010) Balancing privacy and access in school desegregation collections: a case study.

Week 8, Nov 22: Privacy, Information Security, and Cyber Risk

Security and risks to privacy is a huge area of study and practice. For the purposes of this week's discussion, we narrow the scope to focus on threats to information privacy and ways to mitigate those threats through practice, policy, and technology. We consider anonymity, confidentiality, and reidentification, and address relationships between privacy and security. Additional background material on data breaches is provided in Assignment 2.

Assignment 2 due on CCLE by 12:00AM the night before class.

Required Readings:

(Barocas & Nissenbaum, 2014) Big data's end run around anonymity and consent.

(Kerr & Reiter, 2014) Using statistics to protect privacy.

(Montjoye et al., 2015) Unique in the shopping mall: on the reidentifiability of credit card metadata.

(Minow, 2002) The USA PATRIOT Act.

(Relyea, 2004) Homeland security and information sharing: federal policy considerations.

(S. J. Landwehr, 2014) Engineered controls for dealing with big data.

(Schneier, 2000) Secrets and Lies: Digital Security in a Networked World, Preface, Chapter 1 (introduction), Chapter 2 (threats).

(Sweeney, 2013) Matching known patients to health records in Washington State data.

("UCOP Privacy and Information Security Initiative," 2013)

(Wilbanks, 2014) Portable approaches to informed consent and open data.

Recommended Readings:

(Dwork, 2014) Differential privacy: a cryptographic approach to private data analytics.

(Kugler, 2015) Online privacy: regional differences.

(Mason, 1986) Four ethical issues of the information age

(Treese, 2005) Once collected, data isn't private.

(Vascellaro, 2010) Google agonizes on privacy as ad world vaults ahead.

Week 9, Nov 29: Governing Privacy in the University

Universities face a complicated array of privacy issues. While they are as responsible for protecting the privacy of students, faculty, staff, and other constituents as are schools, businesses, government agencies, and other organizations, they also are concerned about academic freedom, free speech, intellectual freedom, and transparency. Universities have extensive reporting responsibilities to state and federal agencies, accreditation bodies, funding sources, and other entities. Universities also are rich targets for hacking and data breaches. Universities tend to be open by design, welcoming students, visitors, and partners from around the world, yet must protect some of their information (and computer networks) as securely as do banks. They maintain protected spaces for intellectual pursuit, including research and scholarship that maybe closely held until the time of publication. Yet they also are subject to open records laws and to funding agency requirements for open access to publications and data.

Universities, colleges, and K-12 schools collect vast amounts of data on their students. These include not only courses and grading, but may include transactions associated with learning management systems (e.g., CCLE), student ID cards (e.g., library, food services, debit records, spending, door access), social media, and more. Universities have come to recognize the value in aggregating these data to make decisions about student progress, problems, and success. Private companies also wish to have access to data about students. Companies and other third parties are acquiring student data directly via their own services or through partnerships with universities. Exploiting these data effectively and ethically, while maintaining student privacy rights, is a frontier concern of privacy protection.

The University of California is a leader in addressing this complex array of privacy and security issues, and several of the UC-wide initiatives in this area began at UCLA. This week we will read several notable reports from these initiatives and discuss current issues with UCLA's Chief Privacy Officer.

Guest speaker: Kent Wada, Chief Privacy Officer, UCLA

Required readings; general, plus read those in the sections below:

("Data Governance Task Force: Final report and recommendations," 2016)

(Ho, 2017) Naked in the Garden

(Powles & Hodson, 2017) Google DeepMind and healthcare in an age of algorithms

(Ritvo, 2016) Privacy and student data: an overview of federal laws impacting student information collected through networked technologies.

(Selinger, 2015) With big data invading campus, universities risk unfairly profiling their students

(UCLA Academic Personnel Office, 2012) Scholarly Research and Public Records Requests

(UCLA Office of the Chancellor, 2014) Public records requests policy

Readings on academic freedom:

(Cole, 2016) The triumph of America's research university.

(Schram, 2014) The future of higher education and American democracy: introduction.

Readings on role of chief privacy officers in organizations:

(Nathan, 2017) A day in the life of a chief privacy officer.

(Vogel, 2015) The chief privacy officer in higher education.

Asilomar conferences on learning analytics and student privacy:

("The Asilomar Convention for Learning Research in Higher Education," 2014)

("Home | Asilomar II: Student Data and Records in the Digital Era," 2016)

Recommended Readings:

(Biemiller, 2017) Big data for student success still limited to early adopters.

(Borgman, 2017) Academic senate engagement in governance of IT and cyber risk.

(Brown, 2017) Where every student is a potential data point.

(Daniel, 2017) Big data in higher education: the big picture.

(Electronic Privacy Information Center, n.d.) EPIC - EPIC student privacy project.

("Family Educational Rights and Privacy Act (FERPA)," 2015)

(Gasser, Solow-Niederman, & Nolan, 2013) Student privacy in the cloud computing ecosystem - state of play & potential paths forward.

(Greenwood, Stopczynksi, Sweatt, Hardjono, & Pentland, 2014) The new deal on data: a framework for institutional controls. (In Lane, et al)

(Ren & Li, 2013) Academic freedom and university autonomy: a higher education policy perspective.

(Rotenberg, 2013) Amassing student data and dissipating privacy rights.

(Stodden, 2014) Enabling reproducibility in big data research: balancing confidentiality and scientific transparency. (In Lane, et al)

(University of California, Office of the President, 2017a) Appendix on Data Security and Privacy

Week 10, Dec 6: Course wrapup, Student presentations

We will use the last session of the term to learn from the students in the course. Student term paper topics will be grouped into panel sessions. Each student will present issues from his or her paper in 5 to 7 minutes, with discussion at the end of each panel session. We will conclude with a general summary of the topics covered in the course.

Exam Week, Dec 12

5pm (Tuesday). Paper due to CCLE.

Other course background material:

(Agre & Rotenberg, 1997) Technology and privacy: the new landscape.

(Bennett & Raab, 2006) The governance of privacy: policy instruments in global perspective.

(Diffie & Landau, 2007) Privacy on the line: the politics of wiretapping and encryption.

(Gymrek et al., 2013) Identifying personal genomes by surname inference.

(Rosen, 2001) The unwanted gaze: the destruction of privacy in America.

(Smith, 2004) Ben Franklin's web site: privacy and curiosity from Plymouth Rock to the Internet.

(Zittrain, 2009) The future of the Internet--and how to stop it.

References:

Acquisti, A. (2014). The economics and behavioral economics of privacy. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 76–95). New York, NY: Cambridge University Press.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., Gross, R., & Stutzman, F. (2014). Face recognition and privacy in the age of Augmented Reality. *Journal of Privacy and Confidentiality*, *6*(2), 1–20.

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101–127.

Agre, P. E., & Rotenberg, M. (Eds.). (1997). *Technology and Privacy: The New Landscape* (First Edition edition). Cambridge, Mass: The MIT Press.

ALA. (2006, July 7). Privacy: An interpretation of the Library Bill of Rights [Text]. Retrieved from http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Allen, A., & Rotenberg, M. (2015). *Privacy Law and Society* (3 edition). St. Paul, MN: West Academic Publishing.

An act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other

purposes., Pub. L. No. 104–191 (1996). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191

Angwin, J. (2014). Chapter 2. In *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books.

Ardia, D. S., & Klinefelter, A. (2015). Privacy and Court Records: An Empirical Study. *Berkeley Technology Law Journal*, *30*(2), 1807. https://doi.org/10.15779/Z38TR9C

ARMA. (n.d.). Code of Professional Responsibility. Retrieved August 12, 2017, from http://www.arma.org/who-we-are/code-of-professional-responsibility

Ault, U. E. (1990). The FBI's Library Awareness Program: Is Big Brotehr Reading over Your Shoulder. *NYUL Rev.*, *65*, 1532.

Bamberger, K. A., & Mulligan, D. K. (2011). *Privacy on the books and on the ground* (SSRN Scholarly Paper No. ID 1568385). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1568385

Bamberger, K. A., & Mulligan, D. K. (2015). Privacy on the Ground. Retrieved September 24, 2017, from https://mitpress.mit.edu/books/privacy-ground

Bamford, J. (2007). *Body of secrets: anatomy of the ultra-secret National Security Agency : from the Cold War through the dawn of a new century*. New York: Doubleday. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=717166

Bamford, J. (2014, August). Edward Snowden: The untold story. Retrieved May 8, 2017, from https://www.wired.com/2014/08/edward-snowden/

Bamford, J. (2017, June 5). Washington's Ministry of Preemption. Retrieved from https://foreignpolicy.com/2017/05/31/washington-ministry-of-preemption-united-states-intelligence/

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 44–75). New York, NY: Cambridge University Press.

Barrett, B. (2017, April 28). Amazon's 'Echo Look' Could Snoop a Lot More Than Just Your Clothes. Retrieved from https://www.wired.com/2017/04/amazon-echo-look-privacy/

Bennett, C. J. (2010). *The Privacy Advocates: Resisting the Spread of Surveillance*. The MIT Press.

Bennett, C. J., & Raab, C. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, Mass: The MIT Press.

Berghel, H. (2014). Privacy Informatics: A Primer on Defensive Tactics for a Society under Siege. *Computer*, *47*(1), 78–82.

Berman, F., & Cerf, V. G. (2017). Social and ethical behavior in the internet of things. *Communications of the ACM*, *60*(2), 6–7. https://doi.org/10.1145/3036698

Biemiller, L. (2017, April 9). Big Data for Student Success Still Limited to Early Adopters. *The Chronicle of Higher Education*. Retrieved from http://www.chronicle.com/article/Big-Data-for-Student-Success/239713/

Borgman, C. L. (2017, March). *Academic Senate Engagement in Governance of IT and Cyber Risk*. Presented at the Cyber Risk Governance Committee, UC Office of the President, Oakland, CA.

Bowers, S. L. (2006). Privacy and Library Records. *The Journal of Academic Librarianship*, *32*(4), 377–383. https://doi.org/10.1016/j.acalib.2006.03.005

Brown, S. (2017, April 9). Where Every Student Is a Potential Data Point. *The Chronicle of Higher Education*. Retrieved from http://www.chronicle.com/article/Where-Every-Student-Is-a/239712/?key=XaMJFpx9opKst2jyIKXWQpi8JX0GyvLMNVYAxV9y9pXyC_92KHaSoA5Qd0GjdcZhNWlvd25TNzZyOGFpOVd3QmNlYUVMVTQ3NVVoQXNSQk83MVByVHoyVkk1SQ

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66–72. https://doi.org/10.1145/2890488

Calo, R. (2010). *The boundaries of privacy harm* (SSRN Scholarly Paper No. ID 1641487). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1641487

Cavoukian, A. (2011, January). Privacy by Design: The 7 foundational principles. Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chin, J., & Lin, L. (2017, June 26). China's All-Seeing Surveillance State Is Reading Its Citizens' Faces; In vast social-engineering experiment, facial-recognition systems crunch data from ubiquitous cameras to monitor citizens. *Wall Street Journal*

(Online); New York, N.Y., p. n/a. Retrieved from https://search.proquest.com/docview/1913392450/citation/E0DBCB1AAB3F4111PQ/1

Cohen, H., & Minow, M. (2006). Intellectual freedom in libraries: Then and now. In *Advances in Librarianship* (pp. 73–101). Emerald Group Publishing Limited.

Cohen, J. E. (1997). *A right to read anonymously: A closer look at "copyright management" in cyberspace* (SSRN Scholarly Paper No. ID 17990). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=17990

Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, *52*(5), 1373–1438. https://doi.org/10.2307/1229517

Cole, J. R. (2016, September 20). The Triumph of America's Research University. *The Atlantic*. Retrieved from https://www.theatlantic.com/education/archive/2016/09/the-triumph-of-americas-research-university/500798/

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, *10*, 273.

Daniel, B. K. (2017). Big Data in Higher Education: The Big Picture. In B. Kei Daniel (Ed.), *Big Data and Learning Analytics in Higher Education: Current Theory and Practice* (pp. 19–28). Cham: Springer International Publishing. Retrieved from http://dx.doi.org/10.1007/978-3-319-06520-5_3

Darrow, B. (2017, July 13). Shhhh. Amazon May Share Your Alexa Conversations With Developers. Retrieved from http://fortune.com/2017/07/13/amazon-alexa-conversations/

Data Governance Task Force: Final report and recommendations. (2016). Retrieved November 18, 2016, from http://evc.ucla.edu/reports/DGTF-report.pdf

Diffie, W., & Landau, S. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption* (updated and expanded edition edition). Cambridge, Mass: The MIT Press.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016). Retrieved from http://data.europa.eu/eli/dir/2016/680/oj

Doe, G. (2014, September 9). With genetic testing, I gave my parents the gift of divorce. Retrieved May 8, 2017, from https://www.vox.com/2014/9/9/5975653/with-genetic-testing-i-gave-my-parents-the-gift-of-divorce-23andme

Dutton, W. H., & Borgman, C. L. (2014). Society and the Internet of Things. Retrieved September 22, 2017, from http://www.voicesfromoxford.org/video/society-and-the-internet-of-things/423

Dwork, C. (2014). Differential privacy: A cryptographic approach to private data analytics. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy,*

Big Data, and the Public Good: Frameworks for Engagement (1 edition, pp. 296–322). New York, NY: Cambridge University Press.

e-CFR: Title 34: Education, Title 34: Education, and Electronic Code of Federal Regulations § Part 99—Family Educational Rights and Privacy. Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33

Edwards, H. S. (2016, October 25). How Web Cams Helped Bring Down the Internet, Briefly. Retrieved from http://time.com/4542600/internet-outage-web-cams-hackers/

Edwards, H. S. (2017, May 4). Alexa Takes the Stand: Listening Devices Raise Privacy Issues. Retrieved from http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues/

Electronic Privacy Information Center. (n.d.). EPIC - EPIC Student Privacy Project. Retrieved May 8, 2017, from https://epic.org/privacy/student/

Elias, P. (2014). A European perspective on research and big data analysis. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 173–191). New York, NY: Cambridge University Press. Retrieved from https://doi.org/10.1017/CBO9781107590205.011

EPIC - Electronic Privacy Information Center. (n.d.). Retrieved May 8, 2017, from https://www.epic.org/

Fair Information Practice Principles (FIPPS) | Homeland Security. (2008). Retrieved from https://www.dhs.gov/publication/fair-information-practice-principles-fipps

Family Educational Rights and Privacy Act (FERPA). (2015, June 26). [Guides]. Retrieved May 8, 2017, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Freedom to Read Foundation. (n.d.). Retrieved May 8, 2017, from http://www.ftrf.org/

Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, *42*(4), 14:1–14:53. https://doi.org/10.1145/1749603.1749605

Gasser, U., Solow-Niederman, A., & Nolan, C. (2013). *Student privacy in the cloud computing ecosystem - State of play & potential paths forward* (SSRN Scholarly Paper No. ID 2354366). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2354366

Gellman, B., & Soltani, A. (2013, October 14). NSA collects millions of e-mail address books globally. Retrieved May 8, 2017, from https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

Gellman, R. (1995). Public records—access, privacy, and public policy: A discussion paper. *Government Information Quarterly*, *12*(4), 391–426. https://doi.org/10.1016/0740-624X(95)90077-2

Gellman, R. (2017). *Fair information practices: a basic history* (SSRN Scholarly Paper No. ID 2415020). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2415020

Goerge, R. M. (2014). Data for the public good: Challenges and barriers in the context of cities. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 153–172). New York, NY: Cambridge University Press.

Greene, D., & Shilton, K. (2017). Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society*, 146144481770239. https://doi.org/10.1177/1461444817702397

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013, July 12). Microsoft handed the NSA access to encrypted messages. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Greenwood, D., Stopczynksi, A., Sweatt, B., Hardjono, T., & Pentland, A. (2014). The new deal on data: A framework for institutional controls. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 192–210). New York, NY: Cambridge University Press.

Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science*, *339*(6117), 321–324. https://doi.org/10.1126/science.1229566

Harper, L. M., & Oltmann, S. M. (2017, April 2). Big Data's Impact on Privacy for Librarians and Information Professionals. Retrieved from https://www.asist.org/publications/bulletin/aprilmay-2017/big-datas-impact-on-privacy-for-librarians-and-information-professionals/

Harris, K. D. (2013, January). Privacy on the go - recommendations for the mobile ecosystem. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf

Ho, L. (2017). Naked in the Garden: Privacy and the Next Generation Digital Learning Environment. Retrieved September 27, 2017, from https://er.educause.edu:443/articles/2017/7/naked-in-the-garden-privacy-and-the-next-generation-digital-learning-environment

Home | Asilomar II: Student Data and Records in the Digital Era. (2016). Retrieved August 12, 2017, from https://sites.stanford.edu/asilomar/

Howard, P. N. (2015). *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven : London: Yale University Press.

Jarvis, J. B. (2014, June 19). National Park System Policy Memorandum 14-05. Retrieved August 12, 2017, from https://www.nps.gov/policy/PolMemos/PM_14-05.htm

Jordan, C. (2016, November 11). From toasters to baby monitors, IoT's role in cyberattacks [Text]. Retrieved from http://thehill.com/blogs/congress-blog/technology/305571-from-toasters-to-baby-monitors-iots-role-in-cyberattacks

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, *50*(4), 1193–1294. https://doi.org/10.2307/1229286

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3393–3402). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2466466

Kerr, A. F., & Reiter, J. P. (2014). Using statistics to protect privacy. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 276–295). New York, NY: Cambridge University Press.

Kirkpatrick, K. (2017). It's not the algorithm, it's the data. *Communications of the ACM*, *60*(2), 21–23. https://doi.org/10.1145/3022181

Klarreich, E. (2012, December 31). Privacy by the numbers: A new approach to safeguarding data. Retrieved May 8, 2017, from https://www.scientificamerican.com/article/privacy-by-the-numbers-a-new-approach-to-safeguarding-data/

Koonin, S. J., & Holland, M. J. (2014). The value of big data for urban science. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 137–152). New York, NY: Cambridge University Press.

Kreuter, F., & Peng, R. D. (2014). Extracting information from big data: Issues of measurement, inference, and linkage. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 257–275). New York, NY: Cambridge University Press.

Kugler, L. (2015). Online Privacy: Regional Differences. *Communications of the ACM*, *58*(2), 18–20. https://doi.org/10.1145/2693474

Landwehr, C. (2016). Privacy Research Directions. *Communications of the ACM*, *59*(2), 29–31. https://doi.org/10.1145/2856451

Landwehr, S. J. (2014). Engineered controls for dealing with big data. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 211–233). New York, NY: Cambridge University Press.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2014). *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition). New York, NY: Cambridge University Press.

Leon, P. G., Ur, B., Balebako, R., Cranor, L. F., Shay, R., & Wang, Y. (2011, October 31). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising (Revised May 10, 2012) - Carnegie Mellon University CyLab. Retrieved May 8, 2017, from http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html

Lessig, L. (2000). *Code: And Other Laws of Cyberspace*. New York: Basic Books.

Library Bytegeist. (n.d.). *#6 Talking Privacy with Librarians*. Retrieved from https://soundcloud.com/librarybytegeist/6-talking-privacy-with-librarians

Lindqvist, U., & Neumann, P. G. (2017). The future of the internet of things. *Communications of the ACM*, *60*(2), 26–30. https://doi.org/10.1145/3029589

Lynch, C. (2017). The rise of reading analytics and the emerging calculus of reader privacy in the digital world. *First Monday*, *22*(4). https://doi.org/10.5210/fm.v22i4.7414

Madrigal, A. C. (2017, June 6). The Mysterious Printer Code That Could Have Led the FBI to Reality Winner. *The Atlantic*. Retrieved from

https://www.theatlantic.com/technology/archive/2017/06/the-mysterious-printer-code-that-could-have-led-the-fbi-to-reality-winner/529350/

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

Mayer, J. (2012, March 13). Third-party web tracking: Policy and technology. Retrieved May 8, 2017, from /publications/third-party-web-tracking-policy-and-technology

McCarthy, L., & Yates, D. (2010). The use of cookies in Federal agency web sites: Privacy and recordkeeping issues. *Government Information Quarterly*, *27*(3), 231–237.

McCreary, L. (2008, October). What was privacy? - Harvard Business Review. Retrieved February 19, 2017, from zotero://attachment/25116/

Minow, M. (2002). The USA PATRIOT Act. *Library Journal*, *127*(16), 52.

Montjoye, Y.-A. de, Radaelli, L., Singh, V. K., & Pentland, A. "Sandy." (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536–539. https://doi.org/10.1126/science.1256297

Moynihan, T. (2016, December 5). Alexa and Google Home Record What You Say. But What Happens to That Data? Retrieved from https://www.wired.com/2016/12/alexa-and-google-record-your-voice/

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Munson, S. A., Avrahami, D., Consolvo, S., Fogarty, J., Friedman, B., & Smith, I. (2012). Sunlight or sunburn: A survey of attitudes toward online availability of US public records. *Information Polity*, *17*(2), 99–114.

Nathan, G. (2017, January 30). A Day in the Life of a Chief Privacy Officer. Retrieved from https://er.educause.edu:443/blogs/2017/1/a-day-in-the-life-of-a-chief-privacy-officer

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Nowhere to hide: What machines can tell from your face. (2017, September 9). *The Economist*. Retrieved from https://www.economist.com/news/leaders/21728617-life-age-facial-recognition-what-machines-can-tell-your-face

Office of the Press Secretary, The White House. (2012, February 23). Fact sheet: Plan to protect privacy in the Internet Age by adopting a Consumer Privacy Bill of Rights. Retrieved May 8, 2017, from https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Ohm, P. (2014). Changing the rules: General principles for data use and analysis. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 96–111). New York, NY: Cambridge University Press. Retrieved from https://doi.org/10.1017/CBO9781107590205.006

Peppet, S. R. (2014). *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent* (SSRN Scholarly Paper No. ID

2409074). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2409074

Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission. (1977, July). Retrieved August 11, 2017, from https://epic.org/privacy/ppsc1977report/

Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*. https://doi.org/10.1007/s12553-017-0179-1

Ramirez, E. (2016, August 22). Protecting consumer privacy in the digital age: Reaffirming the role of consumer control | Federal Trade Commission. Retrieved May 8, 2017, from https://www.ftc.gov/public-statements/2016/08/protecting-consumer-privacy-digital-age-reaffirming-role-consumer-control

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., … Schaub, F. (2014). *Disagreeable privacy policies: Mismatches between meaning and users' understanding* (SSRN Scholarly Paper No. ID 2418297). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2418297

Relyea, H. C. (2004). Homeland security and information sharing: Federal policy considerations. *Government Information Quarterly*, *21*(4), 420–438. https://doi.org/10.1016/j.giq.2004.08.007

Ren, K., & Li, J. (2013). Academic Freedom and University Autonomy: A Higher Education Policy Perspective. *Higher Education Policy*, *26*(4), 507–522. https://doi.org/10.1057/hep.2013.31

Ritvo, D. T. (2016). Privacy and student data: An overview of federal laws impacting student information collected through networked technologies. Retrieved from https://dash.harvard.edu/handle/1/27410234

Rosen, J. (2001). *The Unwanted Gaze: The Destruction of Privacy in America* (1st Vintage Books ed edition). New York: Vintage.

Rotenberg, M. (2013, January 28). Amassing student data and dissipating privacy rights. Retrieved May 8, 2017, from http://er.educause.edu/articles/2013/1/amassing-student-data-and-dissipating-privacy-rights

Rotenberg, M. (2016). *Privacy Law Sourcebook 2016*. United States: Electronic Privacy Information Center.

Rubinstein, I., & Good, N. (2012). *Privacy by Design: A counterfactual analysis of Google and Facebook privacy incidents* (SSRN Scholarly Paper No. ID 2128146). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2128146

Rules and Policies - Protecting PII - Privacy Act. (n.d.). Retrieved from https://www.gsa.gov/portal/content/104256

SAA. (n.d.). Core Values Statement and Code of Ethics | Society of American Archivists. Retrieved August 12, 2017, from https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World* (1 edition). Indianapolis, IN: Wiley.

Schneier, B., & Banisar, D. (1997). *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (1 edition). New York: Wiley.

Schram, S. F. (2014). The Future of Higher Education and American Democracy: Introduction. *New Political Science*, *36*(4), 425–437. https://doi.org/10.1080/07393148.2014.954805

Selinger, E. (2015, January 13). With big data invading campus, universities risk unfairly profiling their students. *Christian Science Monitor*. Retrieved from https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0113/With-big-data-invading-campus-universities-risk-unfairly-profiling-their-students

Shilton, K. (2009). Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, *52*(11), 48. https://doi.org/10.1145/1592761.1592778

Shilton, K., & Greene, D. (2017). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-017-3504-8

SLA. (n.d.). SLA Professional Ethics Guidelines. Retrieved from https://www.sla.org/about-sla/competencies/sla-professional-ethics-guidelines/

Smith, R. E. (2004). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (First Edition edition). Providence, RI, USA: Privacy Journal.

Solove, D. J. (2001). Access and Aggregation: Public Records, Privacy and the Constitution. *Minnesota Law Review*, *86*(6), 1137.

Solove, D. J. (2007). *"I've got nothing to hide" and other misunderstandings of privacy* (SSRN Scholarly Paper No. ID 998565). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=998565

Solove, D. J. (2010). *Understanding Privacy* (2/28/10 edition). Cambridge, Mass.: Harvard University Press.

Solove, D. J., & Hartzog, W. (2013). *The FTC and the new common law of privacy* (SSRN Scholarly Paper No. ID 2312913). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2312913

Spinks, R. (2017, August 1). Using a physical fitness app taught me the scary truth about why privacy settings are a feminist issue — Quartz. Retrieved August 12, 2017, from https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/

Stark, B. (2016, September 23). UC Unmanned Aircraft System Safety | UCOP. Retrieved August 15, 2017, from http://www.ucop.edu/enterprise-risk-management/resources/centers-of-excellence/unmanned-aircraft-systems-safety.html

Stodden, V. (2014). Enabling reproducibility in big datta research: Balancing confidentiality and scientific transparency. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 112–135). New York, NY: Cambridge University Press.

Strandberg, F. (2014). Monitoring, datafication, and consent: Legal approaches to privacy in the big data context. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 5–43). New York, NY: Cambridge University Press. Retrieved from https://doi.org/10.1017/CBO9781107590205.003

Sullivan, B. (2017, September 13). Opinion | Your Social Security Number Isn't a Secret. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/13/opinion/your-social-security-number-isnt-a-secret.html

Sweeney, L. (2013). Matching known patients to health records in Washington State data. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2289850

The Asilomar Convention for Learning Research in Higher Education. (2014, June). Retrieved August 12, 2017, from http://asilomar-highered.info/

The world's most valuable resource is no longer oil, but data. (2017). Retrieved May 16, 2017, from http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

Timberg, C. (2014, August 24). For sale: Systems that can secretly track where cellphone users go around the globe. Retrieved May 8, 2017, from https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

Treese, W. (2005). Once Collected, Data Isn't Private. *NetWorker*, *9*(3), 13–15. https://doi.org/10.1145/1086762.1086772

Tsai, J. Y. (2009). *The impact of salient privacy information on decision-making*. Carnegie Mellon University Pittsburgh, PA. Retrieved from https://pdfs.semanticscholar.org/96dc/494116849d1fa34d207bf8630f2de07d5165.pdf

UCLA Academic Personnel Office. (2012). Academic Freedom | UCLA Academic Personnel Office. Retrieved September 27, 2017, from https://apo.ucla.edu/policies-forms/academic-freedom

UCLA Office of the Chancellor. (2014). Principles of Scholarly Research and Public Records Requests. UCLA. Retrieved from https://chancellor.ucla.edu/messages/principles-of-scholarly-research-and-public-records-requests/

UCOP Privacy and Information Security Initiative. (2013). Retrieved November 18, 2016, from http://ucop.edu/privacy-initiative/

Universal Declaration of Human Rights | United Nations. (n.d.). Retrieved May 8, 2017, from http://www.un.org/en/universal-declaration-human-rights/

University of California, Office of the President. (2017a). Appendix-Data Security and Privacy.

University of California, Office of the President. (2017b). General Data Protection Regulation (EU), UC Summary.

Vascellaro, J. E. (2010, August 10). Google Agonizes on Privacy as Ad World Vaults Ahead. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052748703309704575413553851854026

Vogel, V. (2015, May 11). The Chief Privacy Officer in Higher Education. Retrieved from http://er.educause.edu/articles/2015/5/the-chief-privacy-officer-in-higher-education

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 10:1–10:16). New York, NY, USA: ACM. https://doi.org/10.1145/2078827.2078841

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193–220.

Washington, A. L. (2014). Government Information Policy in the Era of Big Data. *Review of Policy Research*, *31*(4), 319–325. https://doi.org/10.1111/ropr.12081

Wilbanks, J. (2014). Portable approaches to informed consent and open data. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (1 edition, pp. 234–252). New York, NY: Cambridge University Press.

Yaco, S. (2010). Balancing Privacy and Access in School Desegregation Collections: A Case Study. *The American Archivist*, *73*(2), 637–668.

Zittrain, J. (2009). *The Future of the Internet--And How to Stop It*. New Haven, Conn.: Yale University Press.