Privacy and Security in a Networked World

INST-611 | Spring 2015

Instructor: Jessica Vitak, Assistant Professor, College of Information Studies
Office: Hornbake 2117G
Email: jvitak@umd.edu
Class time: Wednesdays, 2-5pm
Class location: Plant Sciences (PLS) 1162 (campus map)
Office hours: Wednesdays, 11am-12pm, or by appointment

Catalog Description:

Examining evolving conceptualizations of privacy and security in light of technological developments of 21st century. Analysis of legal, ethical, design, and socially constructed challenges organizations and individuals face when developing privacy and security solutions.

Course Description:

Technological innovations in how individuals, organizations, and governments collect and share personal information have raised myriad concerns regarding how that information can be best protected. In today's highly networked world, individuals must acquire the knowledge and skills to engage with technologies in a safe and secure manner. This course provides an interdisciplinary exploration of the social, legal, ethical, and design challenges that arise when it comes to securing personal information and helping individuals maintain desired levels of privacy at home, work, and everywhere in between.

Student Learning Outcomes:

- Demonstrate broad understanding of major privacy and security challenges faced by organizations, groups, and individuals.
- Define and describe current privacy and security paradigms.
- Describe differences in privacy and security practices across different cultures and contexts.
- Evaluate organizations' privacy and security practices and identify strengths and shortcomings.
- Propose design solutions for various privacy and security issues.
- Identify the social, legal, and ethical implications surveillance policies in the workplace and in public spaces.

- Propose policy changes at the organizational and government level to enhance end-user privacy and security.

Course Materials:

There is no required textbook for this course.

On Canvas (https://elms.umd.edu/), you will find the course syllabus and schedule, presentation materials, announcements, assignment details, and .pdfs of assigned readings.

Please read the required readings before the date for which they are listed. Getting the most out of readings is an important skill for understanding and responding to policy issues. Whether reading theoretical perspectives, persuasive arguments, or implementation studies, "close reading" is a valuable technique to learn for information policy and graduate school. Terri Senft has put together a wonderful primer on close reading, available here: http://tsenft.livejournal.com/413651.html

Syllabus Change Policy:

This syllabus is a guide for the course and is subject to change with advance notice.

Assignments and Grading:

The grading scale (including corresponding GPA) for the final grade is as follows:

A (4.0) 95-100	A- (3.7) 90-94.9	B+ (3.3) 85-89.9
B (3.0) 80-84.9	B- (2.7) 75-79.9	C+ (2.3) 70-74.9
C (2.0) 65-69.9	D (1.0) 60-64.9	F (0.0) Less than 60

Your grade in this class will be based on the following components:

- Class participation (10%)
- Weekly topic leader (15%)
- Conceptualizing privacy and security (10%)
- Privacy policy analysis (15%)
- Designing for enhanced privacy and security (15%)
- Final paper (25%)
- Final presentation (10%)

Note: Grading rubrics are available on Canvas for written/oral assignments.

Class participation (10%): This class is structured to be discussion-centered, with the professor leading discussion and providing topics and students actively participating. This will require that you finish all assigned readings **prior** to each class session. Participation forms an integral part of your own learning experience, as well as that of your classmates. Class participation grades will take into account both the quantity and quality of your contributions to class discussions; however, the quality of your contributions (whether questions, viewpoints, responses to

others' questions, etc.) to a meaningful, ongoing discussion will be much more heavily weighted.

Weekly topic leader (15%): By Week 2, each student should review the course topics for the semester and send the professor a ranking of their **top three** choices to be that week's topic leader (for Weeks 3-14). Topic leaders are responsible for the following components:

(1) Creating a one-page handout that summarizes the key topics from that week and includes at least three high-level discussion questions for the class
(2) Identifying and sharing a current events news story that is related to the topic through the discussion board for their week (posted by Sunday at noon the week before class)
(3) Leading class discussion of the article's importance and facilitating conversation in class. Students should demonstrate they're very familiar with their topic and are able to clearly articulate the arguments presented in the articles.

Conceptualizing networked privacy and security (10%)—Due Week 3: The words "privacy" and "security" are common terms in modern society, especially in discussions of technology use. But how do people's individual perceptions of these concepts vary? Understanding the commonalities and differences in our understanding of these concepts is essential to both theory and design.

For this assignment, students should conduct **brief** interview four people regarding what privacy and security mean to them. Students should attempt to get a diverse sample of perspectives across age, sex, and other demographic characteristics. In a 2-3 page (single-spaced) paper, they should reflect on their own understanding of these concepts (i.e., through pre-existing understanding as well as any new insights derived from the first weeks of class), how their perceptions are similar and different to the people they interviewed, and identify and discuss perceived gaps in understanding. The goal is to get you to "think deeply" about these highly complex concepts and begin to understand how your own background, beliefs, and behaviors influence the way you think about privacy and security.

Privacy policy analysis (10%)—DUE WEEK 7: Students will select a website, review its privacy policy and critically analyze it through application of the FTC's five Fair Information Practice principles: Transparency, Choice, Information Review and Correction, Information Protection, and Accountability (for a review: https://security.berkeley.edu/sites/default/files/uploads/FIPPs.pdf). Address areas where the site's policy is strong, where it falls short, and make suggestions for how the website could improve its privacy practices. Finally, consider the ethical and legal ramifications of the policy as it currently stands. Papers should be a minimum of 3 pages (single-spaced) and should cover the following:

- Brief overview of the organization being evaluated and its history (especially anything that relates to privacy and security of user information)
- Analysis of how the site's privacy policy meets (or falls short) for each of the FTC Fair Information Practice Principles

- Evaluate potential ethical/legal issues related to the company's privacy policy and offer recommendations for how to address these issues.

It's probably a good idea to pick a more prominent company than one that is obscure. Consider the types of information that company collects and the types of information people share when visiting the site. Do background research on the company's privacy policy to see how it has been covered in the media.

Designing for enhanced privacy and security (15%)—DUE WEEK 11: Throughout the semester, we will identify a large number of privacy and security-related problems and concerns that consumers have when sharing personal information online. Select one of the issues/concerns from the below list (or get approval from the professor on another topic) and write a 4-6 page paper (single-spaced) that (1) identifies and provides background on the issue, (2) outlines three potential solutions that have already been implemented by organizations, have been proposed by researchers, or are your own, and (3) discuss the benefits and drawbacks of each solution**. At least one solution must be of the student's design.** Images and/or mock-ups of solutions are encouraged but not required and should be included as an Appendix (they do not count toward page requirements). References (minimum 5) should be included on a separate page and do not count toward page requirements.

Potential topics:

- Low tech skills among older users of social media
- Context collapse leading to difficulties regulating self-presentation
- Securing data shared through cloud computing technologies
- Organizational security breaches
- The de-anonymization of user identities in online forums, blogs, and news sites
- Privacy paradox (mismatch between desired and actual privacy/disclosure behaviors)
- Big data and ethical research
- Privacy challenges in mobile applications

Final Paper (30%)—MULTIPLE DEADLINES: In pairs or individually, students will choose a privacy and/or security topic related to the class, define a specific research question related to that topic, and write an 10-12 page paper (single-spaced) that critically analyzes the issue. This paper must include a review of related literature; data collection, analysis (e.g., surveys, interviews, analysis of existing datasets, content analysis), discussion; and theoretical and/or design implications.

Students/pairs must propose their topic by **Week 5** of the course, including their research question, a brief description of its importance to our understanding of privacy and security in a networked world, and an overview of data collection methods (1 page minimum). Students planning on conducting more detailed data collections (e.g., with the intent to publish findings) should submit their proposal earlier to ensure that they can complete data collection. If

publication is an eventual intention for the paper, students are advised to talk to the professor about the project early in the semester for advice and tips.

Students are highly encouraged to submit drafts of any research protocols and versions of their final paper prior to the due date (**Week 15**). Review and feedback from the professor (and subsequent implementation of suggestions) **will** increase your final grade and will ensure there is no confusion between the project expectations and their interpretation.

Proposal—DUE WEEK 5: 5% of final grade
Final Paper—DUE WEEK 15: 25% of final grade

Final Presentation (10%)—DUE WEEK 15
During the final class, students will present an 8-10 minute summary of their study to the class. Discussion and slides should overview the research question(s) being studied, why it is an important topic in today's networked world, the findings from data collection, and implications of the findings.

Review of Graded Material:

I aim to grade all assignments within 1-2 weeks of their due date and post those grades to ELMS. I try very hard to evaluate each assignment fairly, but I can only evaluate what you submit. I don't have the benefit of knowing all of the time and effort you have put into an assignment. Therefore, you need to make that effort stand out.

Because there may be times when I misinterpret what you have written, I am always willing to clarify how I graded your assignment. If you have any questions about a grade you received, you have **two weeks** from receipt of the grade to contact me (in class, through a meeting, or via email) to discuss your grade. After two weeks have passed, that grade is "locked" and I will not re-evaluate it. Before asking me to review an assignment, however, it is important that you carefully read the feedback and grade justification I have provided.

Please also review the grading templates on ELMS before writing each assignment, as this will provide you with a framework through which I will be grading your submission.

Academic Integrity:

What is academic dishonesty?
Academic dishonesty is a corrosive force in the academic life of a university. It jeopardizes the quality of education and depreciates the genuine achievements of others. Apathy or acquiescence in the presence of academic dishonesty is not a neutral act. All members of the University Community - students, faculty, and staff - share the responsibility to challenge and make known acts of apparent academic dishonesty.

Students have a responsibility to familiarize themselves with violations of the Code of Academic Integrity. Among these include:

1. **Cheating**
"Intentionally using or attempting to use unauthorized materials, information, or study aids in any academic exercise."
2. **Fabrication**
"Intentional and unauthorized falsification or invention of any information or citation in an academic exercise."
3. **Facilitating Academic Dishonesty**
"Intentionally or knowingly helping or attempting to help another to commit an act of academic dishonesty."
4. **Plagiarism**
"Intentionally or knowingly representing the words or ideas of another as one's own in an academic exercise."

For further clarification or information on the Code of Academic Integrity:
http://www.studenthonorcouncil.umd.edu/code.html

Plagiarism in any course assignment will not be tolerated. Students who submit an assignment containing plagiarized text (including lack of proper attribution, including quoted material with encasing copied text in quotes, copying part of an assignment from another student, or insufficiently paraphrasing content from another source) will have their assignment returned, ungraded, and they will have three (3) days to re-submit the assignment with the plagiarism issues addressed. Students will also receive a penalty of up to 50% of the assignment grade. If a second case of plagiarism is detected, students will automatically receive an F in the class and will be referred to the university for disciplinary action.

Students are encouraged to check their assignments prior to submission using one of the free online plagiarism checkers (e.g., www.grammarly.com).

Attendance and Expectations of Student Participation

This class meets once a week. The course will include lecture, discussion, and group work. It is essential that every student participates in the discussions of course materials. Participation means active involvement in class discussions. Students are expected to question, challenge, argue, and discuss issues and topics related to that session's readings.

Regular attendance and participation in this class is the best way to grasp the concepts and principles being discussed. However, in the event that a class must be missed due to an illness, a reasonable effort should be made to notify the instructor in advance of the class. If a student is absent more than 2 times due to illness, please meet with the instructor to discuss plans for make-up work. If a student is absent on days when papers are due, he or she is required to notify the instructor in advance and turn in the paper via email. Please see the extensions policy below if extra time is needed due to illness.

Classroom Environment

As a graduate seminar, the classroom environment should be professional and respectful. Discussions should be based on course readings and critical thinking. Issues of policy can involve strongly held beliefs and current political controversies. Remember--your classmates may have different perspectives on issues than you, but they still deserve your respect. As another aspect of respect in the classroom environment, turn off or mute all phones and other communication devices during each class session. If you use your laptop in the classroom, limit the usage of the computer to course-related reasons (i.e., taking notes).

Students with Disabilities

Students with disabilities needing academic accommodation should: (1) register with and provide documentation to the Disability Support Services office, and (2) discuss any necessary academic accommodation with their teachers. This should be done at the beginning of the semester.

Learning Assistance

If you are experiencing difficulties in keeping up with the academic demands of this course, contact the Learning Assistance Service, 2202 Shoemaker Building, 301-314-7693. Their educational counselors can help with time management, reading, math learning skills, note-taking and exam preparation skills. All their services are free to UMD students.

Extensions

Timeliness is an essential component of graduate work, and extensions will only be available during personal emergencies. Students who need to request an extension should discuss the matter **in advance** with the professor. If an extension is granted, the work must be submitted within the extension period to avoid grade penalties. Unexcused delays in submission of the paper will result in a deduction of a letter grade for each day the paper is late, while unexcused delays in presentations will result in a deduction of a letter grade for each class meeting the presentation is late.

Late Work

Unless approved by the professor in advance of the due date, late work will automatically be graded down by one step (i.e., 5%) for each day it is late (unless otherwise noted in the syllabus). For example, an assignment that would normally receive an A- if submitted on time would receive a B if it was submitted two days late. Assignments more than five days late will not be accepted.

Emergency Preparedness:

Please see the University's Emergency Preparedness Website (http://www.umd.edu/emergencypreparedness/) for information about the current status of the campus. If a class session needs to be rescheduled, I will e-mail you as soon as possible.

Inclement Weather: In the event of inclement weather, students should check the UMD homepage (umd.edu) or call 301-405-SNOW (7669) to determine if there are delays or closures. Closures and

delays will also be sent over the e2 Campus notification system. Follow the link to sign up for alerts: www.alert.umd.edu. Also make sure you either check your UMD email regularly or forward UMD emails to an account you do check regularly, in case the professor emails out a class cancellation.

Weekly Topics Overview

- Week 1: Historical overview of privacy and security in the U.S. and abroad
- Week 2: Major paradigms for understanding privacy and security
- Week 3: Legal issues in privacy and security
- Week 4: Contextual influences on privacy attitudes and behaviors
- Week 5: The evolution of privacy and security concerns with networked technologies
- Week 6: Anonymity in a networked world
- Week 7: Boundary regulation processes
- Week 8: Privacy paradoxes
- Week 9: Designing privacy-enhancing solutions in HCI
- Week 10: Nudging privacy and security behaviors
- Week 11: Privacy, security, and ethics
- Week 12: Surveillance in the workplace
- Week 13: Surveillance "in the wild"
- Week 14: Big data and privacy
- Week 15: Final presentations and course wrap-up

Course Schedule

Note: Where appropriate, students will also be assigned mainstream media articles on current events related to upcoming topics. Readings may also change as new research is released.

Week # **Date**	**Topics, Readings, and Due Dates**
1 Jan 28	**Historical overview of privacy and security in the U.S. and abroad** • Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review.* • Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35,* 989-1015.
2 Feb 4	**Major paradigms for understanding privacy and security** • Altman I (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues* 33: 66–84. • Margulis ST (2003). "On the status and contribution of Westin's and Altman's Theories of Privacy". *Journal of Social Issues* **59** (2): 411–429. • Petronio, S., & Durham, W. T. (2015). Communication Privacy Management Theory: Significance for interpersonal communication. In D. O. Braithwaite & P. Schrodt (Eds.),

Week # Date	Topics, Readings, and Due Dates
	Engaging theories in interpersonal communication: Multiple perspectives (pp. 335-347). Thousand Oaks, CA: Sage. • Scheiner, B. (2008). The psychology of security. *AFRICACRYPT 2008, LNCS 5023* (pp. 50-79). Springer-Verlag. **DUE:** Email list of topic choices for weekly discussion leader & course survey.
3 Feb 11	**Legal issues in privacy and security** • Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press. (Chapter 5—How governments rule the Net) • Solove, D. J. (2007). *The future of reputation*. New Haven, CT: Yale University Press. (Chapter 5—The role of law). • Bennett, S. C. (2012). The "Right to Be Forgotten": Reconciling EU and US Perspectives. *Berkeley Journal of International Law, 30,* 161-195. **DUE:** Conceptualizing networked privacy and security brief due.
4 Feb 18	**Contextual influences on privacy attitudes and behaviors** • Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In *Privacy Online* (pp. 221-234). Berlin: Springer. • Maab, W. (2011). The elderly and the Internet: How senior citizens deal with online privacy. In *Privacy Online* (pp. 235-250). Berlin: Springer. • Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10,* 28-45. • Beach, S., Schulz, R., Downs, J., Matthews, J., Barron, B., & Seelman, K. (2009). Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey. *ACM Transactions on Accessible Computing, 2*(1), Article 5.
5 Feb 25	**The evolution of privacy and security concerns with networked technologies** • Solove, D. J. (2008). *Understanding privacy.* Cambridge, MA: Harvard University Press. (Chapter 5) • Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *Proc CHI*. New York: ACM • Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computing Systems, 28*, 583–592. • de Montjoye, Y-A., Radaelli, L., Singh, V. K., & Pentland, A. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, 347(6221), 536-539. **DUE:** Final project proposal

Week # Date	Topics, Readings, and Due Dates
6 Mar 4	**Anonymity in a networked world** • Solove, D. J. (2007). *The future of reputation*. New Haven, CT: Yale University Press. (Chapter 6—Free speech, anonymity, and accountability) • Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7,* 321-326. • Narayanan, A. & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." *Communications of the ACM, 53*(6)*,* 24-26. • Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57,* p. 1701.
7 Mar 11	**Boundary regulation processes** • boyd, d. (2014). *It's complicated: The social lives of networked teens.* New Haven, CT: Harvard University Press. (Chapter 2) • Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting and Electronic Media, 56,* 451-470*.* • Donath, J. (2014). *The social machine: Designs for living online.* MIT Press. (Chapter 7) **DUE:** Privacy policy analysis
	MARCH 18: SPRING BREAK—NO CLASS MEETING
8 Mar 25	**Privacy paradoxes** • Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30,* 13-28. • Utz, S., & Kramer, N. C. (2009), The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2). Available: http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1 • Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. Oxford: Global Cyber Security Capacity Centre: Working Paper.
9 Apr 1	**Designing privacy-enhancing solutions in HCI** • Fischer-Hubner, S., Pettersson, J. S., Bergmann, M., Hansen, M., Peason, S., & Mont, M. C. (2008). HCI designs for privacy enhancing identity management. In *Digital privacy: Theory, technologies, and practices* (Eds. A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati), pp. 229-252. New York: Auerbach Publications. • Martin, K. (2013). Transaction costs, privacy, and trust: The laudable goals and

Week # Date	Topics, Readings, and Due Dates
	ultimate failure of notice and choice to respect privacy online. *First Monday*, *18*(12). • Goldberg, I. (2008). Privacy enhancing technologies for the Internet III: Ten years later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 3-18). New York: Auerbach Publications.
10 Apr 8	**Nudging privacy and security behaviors** • Acquisti, A., & Grossklags, J. (2008). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 363-380). New York: Auerbach Publications. • Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013). Privacy nudges for social media: An exploratory Facebook study. *Proceedings of the 22nd international conference on World Wide Web* (pp. 763-770). New York: ACM. • Grossklags, J., Radosavac, S., Cardenas, A. A., & Chuang, J. (2010). Nudge: Intermediaries' role in interdependent network security. *Trust and Trustworthy Computing Lecture Notes in Computer Science, 6101,* 323-336.
11 Apr 15	**Privacy, security, and ethics** • Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In *Privacy Online* (pp. 47-60). Berlin: Springer. • Flores, A., & James, C. (2013). Morality and ethics behind the screen: Young people's perspectives on digital life. *New Media & Society, 15,* 834-852. • Zimmer, M. (2010). ''But the data is already public'': On the ethics of research in Facebook. *Ethics and Information Technology, 12,* 313-325. **DUE:** Designing for privacy & security paper
12 Apr 22	**Surveillance in the workplace** • Nippert-Eng, C. (1996). Home and work: Negotiating boundaries through everyday life. Chicago: University of Chicago Press. (Chapter 3—Structural complaints and personal discretion: Work states its claim) • Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? *Academy of Management Perspectives, 23,* 33-48. • Ball, K. (2010). Workplace surveillance: An overview. *Labor History, 51*, 87-106.

Week # Date	Topics, Readings, and Due Dates
13 Apr 29	**Surveillance "in the wild"** • Slobogin, C. (2011). Is the Fourth Amendment Relevant in a Technological Age? Vanderbilt Public Law Research Paper No. 10-64. • Albrechtslund , A. (2008). Online Social Networking as Participatory Surveillance. *First Monday, 13*(3). • Robinson, N., Potoglou, D., Patil, S., Patruni, B., & Lu, H. (2014). *Privacy, security and surveillance: New insights into preferences of European citizens.* Rand Working Paper Series.
14 May 5	**Big data and privacy** • Tene, O., Polonestsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11,* 242-273. • boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication, & Society, 15,* 662-679. • Crawford, K., & Schultz, J. (2012). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review, 55,* 93-128. • Keller, M., & Neufeld, J. (2015). Terms of Service: Understanding our role in the world of big data. [This is a graphic novel written by staff at Al Jazeera. Find it here: http://projects.aljazeera.com/2014/terms-of-service/digital-editions/terms-of-service-al-jazeera.pdf]
15 May 12	**Final presentations and course wrap-up** **DUE:** Final paper and presentation