INLS 490.151 Privacy by Design

Spring 2013

Instructor
Fred Stutzman, Ph.D.
Visiting Assistant Professor
UNC School of Information and Library Science

Email: fred_stutzman@unc.edu
Phone: (415) 968-9172
Website: http://fredstutzman.com/

Meeting Place and Time
Tuesday/Thursday, 12:30PM – 1:45PM, Davie Hall 101

Office Hours
Wednesday, 11:00AM – 12:00PM, Manning Hall 202. Other times by appointment.

Class Website
https://sakai.unc.edu/portal/site/inls490151s13

Important Dates

January 31	Case 1	**April 4**	Case 3
February 7	Quiz 1	**April 11**	Quiz 3
February 28	Case 2	**April 25**	Case 4
March 7	Quiz 2	**May 6**	Final Exam

Course Description
Within organizations, the management of privacy has typically been addressed through the lens of regulatory compliance. For this reason, privacy is often confused with security, or treated as a set of static compliance practices. In recent years, the mainstreaming of ubiquitous social technologies, the widespread adoption of behavioral tracking and targeting, and the turn towards "Big Data" informatics have illustrated the challenges with, and failings of a compliance-based approach to privacy within organizations. A quick scan of the headlines will reveal these failings: large-scale data breaches, mobile apps leaking personal information, social media sites exposing users. For these failings, organizations lose esteem in the marketplace and are exposed to both civil and criminal penalties.

In recent years, the *Privacy by Design* movement has sought to address these failings by advocating a strong, centrally embedded role for privacy within organizations. By designing *for* privacy, organizations are able to maintain regulatory compliance, provide a positive experience for stakeholders, and advance competitively in a marketplace that values privacy. A central challenge of implementing the Privacy by Design approach is a lack of human capital; the goal of this course is to provide exposure and training to individuals interested in advocating for privacy within diverse organizations (e.g., libraries, IT firms, health care, government, NGO's). In taking this course, students will be exposed to a highly interdisciplinary perspective on privacy, with readings from philosophy, economics, sociology, law, and the computer and information sciences, among others. Students will learn the fundamentals of privacy, and through group-based case study, analyze the application of privacy in design and policy. In doing so, students will develop a framework for understanding, implementing, and advocating for privacy within organizations.

Learning Objectives
The primary objectives of this course are as follows:

1. Develop a substantive understanding of privacy as it relates to the design and implementation of information technology.
2. Identify and understand critical aspects of privacy law, policy, and behaviors in order to develop a multi-faceted comprehension of privacy.
3. Use your understanding of privacy to analyze cases where privacy and technology intersect; provide analysis and feedback in the form of case analysis.
4. Develop a working understanding of Privacy by Design that you can bring to design, policy, research, and other applications.

In a nutshell, this class is focused on understanding the relationship between technology and privacy, and giving you a set of tools to analyze and implement organizational, design, and policy approaches to privacy. To give you as much hands-on experience as I can, the bulk of the course deliverables will be devoted to your group-based analysis of privacy cases. When analyzing these cases and preparing your reports and presentations, you should think of yourselves as consultants trying to proactively identify and solve privacy problems.

Course Requirements
Nearly all of the other material we will use is electronic, and will cover a wide range of media. Our course material will be a mix of readings (pdf's, news articles, websites) and media (videos, radio programs, social media). There is no textbook required.

As this is the first time this course is being taught, readings and lecture topics will be developed over the course of the semester. All of the course material will be available through the course website, hosted on Sakai. Materials will be linked from the Sakai syllabus (Sakai->Workspace->Syllabus). If you are having any trouble with the course website, please contact me as soon as possible.

Grading Policy
In-class participation and attendance: 10%
Cases: 60%
    Case 1: 15%
    Case 2: 15%
    Case 3: 15%
    Case 4: 15%
Quizzes: 15%
Final Exam: 15%

In-Class Participation and Attendance
First and foremost, participation and active discussion are essential for the success of this class. To this extent, I expect you to come to every class prepared and ready to think critically about the issues presented. Attendance is required at each class. Students with two or more unexcused absences will be penalized a half-grade for each subsequent absence.

Cases
Over the course of the semester, you will read and analyze four privacy cases. For your deliverable, you and your group will produce a report and presentation that reflects an analysis of a specific aspect of the case. I have defined the four aspects as: *design, policy, behavior*, and *public relations*. I have established the following schedule that illustrates how the analysis revolves:

	Group 1	**Group 2**	**Group 3**	**Group 4**
Case 1	Design	Policy	Behavior	Public Relations
Case 2	Public Relations	Design	Policy	Behavior
Case 3	Behavior	Public Relations	Design	Policy
Case 4	Policy	Behavior	Public Relations	Design

The schedule is structured in a revolving fashion so that for each case, we analyze all four aspects, and each group gets to analyze a different aspect for each case. In doing so, there is maximum exposure to the core concepts of the class. The case report deliverable includes both a case report and 10-minute presentation that summarizes the highlights of the report. The particulars of the case report format will be discussed in class.

Quizzes
There are three short quizzes throughout the semester, each one accounting for 5% (15% total) of your final grade. These quizzes are designed to assess your mastery of the material we are reading and discussing in class.

Final Exam
The final exam accounts for 15% of your overall grade. The final is cumulative and will assess your comprehension of the material we have covered over the course of the semester. Specifics of the final exams, including policies and materials, will be covered in class.

Grade Distribution
Undergraduates are graded on the A-F scale. Please note that no A+ or D- grades exist in the UNC-CH letter grading system. Graduates are graded on the H/P/L/F scale. Please refer to the UNC Faculty Council report on grade definitions if you have questions about what the letter grades stand for.

Points Earned	*Graduate Grade Range*	*Undergraduate Grade Range*
95-100%	H	A
85-94%	P+	B
80-84%	P	C
74-79%	P-	C-
70-73%	L	D
< 70%	F	F

Assignment Policy
The primary deliverable for the class are the four case reports. The case deliverable involves the class presentation (Powerpoint or PDF only) and the case report. Each group should email both the presentation and write-up to me no later than the end of class in which they are due. If you have any trouble with this, please contact me immediately. Late work will result in a one-letter grade per day penalty assessed to the group for the assignment.

Group Work Policy
Class groups are purposefully structured to include both graduate and undergraduate students, of varying skills and interests. This approach maximizes opportunities for interdisciplinary collaboration and bringing new thinking to problems. I expect that groups manage the workload internally, and I expect that student work is commensurate with student status (e.g., doctoral students should expect to carry a heavier load than undergraduates). Group grades will apply to each of the members; there are no individual grades or effort evaluations. I expect you to manage individual effort within your group. Should a problem within a group arise, please inform me sooner, rather than later, so I can step in and make appropriate adjustments as I see fit.

Absence Policy
You are expected to come to every class, and notify me in advance if you need to miss class. You are allowed one unexcused absence. After your first unexcused absence, you will be penalized a half-grade for each subsequent absence. For example, if you have an A-/H-, and miss two classes, your grade becomes a B+/P+. On the third unexcused absence, the grade becomes a B/P. Students who miss an unacceptable amount of class will be expected to withdraw.

Laptop Policy
Out of respect for the class, non-academic computing, Facebooking, texting, etc. during class should be strictly limited. On discussion-intensive days, I will utilize a “laptops closed” policy. When we are in a laptops closed class, students are expected to be offline – with laptops closed, phones stashed away, iPads off, etc.

Social Media Policy
This class may involve participation in social media. I give you extensive latitude in how you identify yourself and protect your content when using these services.

Statement on Academic Integrity
Students are expected to conform to the Honor Code in all academic manners. For more information about the Honor Code, please visit the following URL: http://honor.unc.edu/honor/.

Special Needs
Reasonable accommodations are provided to students who are identified with the Department of Accessibility Resources and Services (DARS), and have provided documentation that supports the need for reasonable accommodations so they may, as independently as possible, meet the demands of university life. These accommodations cannot be provided until I have received notice from DARS. Therefore, if you would benefit from special accommodations, please coordinate with DARS as early as possible.

Administrative
I reserve the right to amend this syllabus.

Course Schedule
As this is the first time this course is being taught, readings and lecture topics will be developed over the course of the semester. You can use this schedule for important dates, but for readings and lecture slides, please consult Sakai.

Date	Topic	Assignment Due	Readings Due
1/10			
1/15	**Module one: History and Theories of Privacy** Current Issues; Defining Privacy		Solove, Daniel (2011) Why Privacy Matters Even if You Have 'Nothing to Hide'. Chronicle of Higher Education, May 15, 2011. Garfield B. and Gladstone, B. (2013) The Privacy Show. [On the Media Radio Broadcast]
1/17	Social and Legal History of Privacy	Case 1 Distributed	Glancy, D. J. (1979). The Invention of the Right to Privacy. Ariz. L. Rev., 21, 1. Prosser, W. L. (1960). Privacy. California Law Review, 48, 383. (Pages 383-403) Westin, A. F. (2003). Social and Political Dimensions of Privacy. Journal of Social Issues, 59(2), 431--453. Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193--220.
1/22	Approaches to Privacy Part I		Solove, D. J. (2002). Conceptualizing Privacy. California Law Review, 1087--1124. Allen, A. L. and Mack, E. (1989). How Privacy Got Its Gender. N. Ill. UL Rev., 10, 441.
1/24	Approaches to Privacy Part II		Solove, D. J. (2002). Conceptualizing Privacy. California Law Review, 1124--1154. Keller, B. (2013). Invasion of the Data Snatchers. New York Times, January 13, 2103. Margulis, S. T. (2003). Privacy as a Social Issue and Behavioral Concept. Journal of Social Issues, 59(2), 243-261.
1/29	Modern Privacy Theories		Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review,

			79(1), 119-158. Rosen, J. (2011). Protect Our Right to Anonymity. New York Times, September 12, 2011. Liptak, A. (2012). Justices Say GPS Tracker Violated Privacy Rights. New York Times, January 23, 2102. Calabresi, M. (2012). Privacy in Public. Time Magazine, March 12, 2012.
1/31		Case 1	Case 1 Presentation and Discussion – **Google Buzz**
2/5	Psychological Privacy	Case 2 Distributed	Altman, I. (1976). Privacy: A Conceptual Analysis. Environment and Behavior, 8(1), 7--29. Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples. Communication Theory, 1(4), 311-335.
2/7	**Module Two: Privacy Policy and Regulation** Fair Information Practices	Quiz 1	Gellman, R (2012). Fair Information Practices: A Basic History. Federal Trade Commission. Fair Information Practice Principles [Reference] Federal Trade Commission. Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books [Discussion] Federal Trade Commission. FTC Path case helps app developers stay on the right, er, path. [Discussion]
2/12	Approaching Privacy Regulation		Solove, D. J. (2006). A Brief History of Information Privacy Law. In Solove, Rotenberg & Schwartz, Information Privacy Law. [Pages 23-46] Lessig, L. (2006). Code and Other Laws of Cyberspace (v2). New York, NY: Basic Books.

2/14	**No Meeting – Privacy Law Salon**		
2/19	The Federal Trade Commission and Privacy Regulation		Federal Trade Commission. (2012) Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. [Pages i, iv-ix, 15-35]
2/21	Privacy by Design		Federal Trade Commission. (2012) Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. [Pages 36-72] Cavoukian, A. (2011) Privacy by Design: The Seven Foundational Principles. International Association of Privacy Professionals (2011). Privacy Enforcement Case Studies Guide.
2/26	Privacy Impact Analysis		Jeselon, P. & Fineberg, A. (2012) A Foundational Framework for a Privacy by Design-Privacy Impact Assessment. Federal Trade Commission. (2013) Privacy Impact Assessment – Twitter Federal Trade Commission. (2013) Privacy Impact Assessment - Facebook
2/28		Case 2	Case 2 Presentation and Discussion – **Facebook Graph Search**
3/5	EU and APEC Data Protection Frameworks	Case 3 Distributed	Robinson, N., Graux, H., Botterman, M., and Valeri, L. (2009) Review of the European Data Protection Directive. RAND Corporation Technical Report. [Chapter 1] Knijpenga, A. (2012) The Modernization of European Data Protection Rules. Deloitte Technical Report. European Commission (2012). Safeguarding Privacy in a Connected World. Export.gov. U.S.-EU Safe Harbor Overview. European Commission (2012). General

			Data Protection Regulation. [41-99 for full text] APEC (2005). APEC Privacy Framework.
3/7	**Module Three: Privacy and Technology Design** Privacy Behavior	Quiz 2	Kumaraguru, P. and Cranor, L. F. (2005). Privacy indexes: A survey of Westin's studies. Technical Report: CMU-ISRI-5-138. Westin, A. (2001) Opinion surveys: What consumers have to say about information privacy. Statement to The House Committee on Energy and Commerce, Trade, and Consumer Protection, Washington, DC. Ackerman, M. S., Cranor, L. F., and Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. In Proceedings of the 1st ACM conference on Electronic commerce. Berendt, B., Gunther, O., and Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. Communications of the ACM, 48(4), 101--106. Spiekermann, S., Grossklags, J., and Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In Proceedings of the 3rd ACM conference on Electronic Commerce, New York, NY, USA, 2001 (pp. 38--47). ACM.
3/12 3/14	**No Meeting – Spring Break**		
3/19	Privacy Enhancing Technologies		Review the Privacy Enhancing Technologies wikipedia page. Study on the Economic Benefits of Privacy-enhancing Technologies (PETs): Final Report to The European Commission, DG Justice, Freedom and Security. London

			Economics, 2010. [Chapter 2] Shen, Y., & Pearson, S. (2011). Privacy Enhancing Technologies: A Review. HP Laboratories. Weinstein, L., & Neumann, P. G. (2003). Privacy issues and privacy enhancing technologies. A Report of Research on Privacy for Electronic Government, 15. Phillips, D. J. (2004). Privacy policy and PETs The influence of policy regimes on the development and social implications of privacy enhancing technologies. New Media & Society, 6(6), 691-706. Gurses, S. (2010). PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. Identity in the Information Society, 3(3), 539-563. Wang, Y., & Kobsa, A. (2009). Privacy-enhancing technologies. Social and Organizational Liabilities in Information Security. IGI Global, 203-227. Van Blarkom, G., Borking, J., and Olk, J. (2003). Handbook of Privacy and Privacy-Enhancing Technologies. The Hague: Privacy Incorporated Software Agent (PISA) Consortium.
3/21	Economics of Privacy		Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (Eds.). (2007). Digital privacy: theory, technologies, and practices. Auerbach Publications. [Chapter 18] Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. Security & Privacy, IEEE, 7(6), 82-85.

			Acquisti, A., John, L., & Loewenstein, G. (2009, December). What is privacy worth. In Twenty First Workshop on Information Systems and Economics (WISE) [Skim] Zhan, J., & Rajamani, V. (2008, April). The Economics of Privacy-Privacy: People, Policy and Technology. In Information Security and Assurance, 2008. ISA 2008. International Conference on (pp. 579-584). IEEE.
3/26	Privacy and Human-Computer Interaction		Ackerman, M. S. and Mainwaring, S. D. (2005). Privacy issues and Human-computer interaction. Computer, 27(5), 19--26. Hong, J. I., Ng, J. D., Lederer, S., and Landay, J. A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. Sengupta, S. (2013). Web Privacy Becomes a Business Imperative. New York Times, March 13, 2013. Brandimarte, L., Acquisti, A., and Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. Social Psychological and Personality Science. [Short version pp. 8-9] Whitten, A. and Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium.
3/28	Privacy Notice		McDonald, A., Reeder, R., Kelley, P., and Cranor, L. (2009). A Comparative Study of Online Privacy Policies and Formats. In Proceedings of Privacy Enhancing Technologies (pp. 37--55).

			Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. (2009). A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security. McDonald, A. M. and Cranor, L. F. (2009). The Cost of Reading Privacy Policies. ISJLP, 4. [Skim]
4/2	Pervasive Computing and Privacy		Palen, L. and Dourish, P. (2003). Unpacking ``Privacy'' for a Networked World. In CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, 2003 (pp. 129--136). ACM Press. Lederer, S., Hong, I., Dey, K., and Landay, A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. Personal Ubiquitous Comput., 8, 440--454. Hardy, Q. (2013). Technology turns to tracking people offline. New York Times, March 7 2013. Markoff, J. (2008). You're Leaving a Digital Trail. What About Privacy?. New York Times, November 29, 2008.
4/4		Case 3	Case 3 Presentation and Discussion – **Apple iOS Privacy Protections**
4/9	**Module Four: Applied Privacy by Design** Criticisms of Privacy by Design	Case 4 Distributed	Rubinstein, I. (2012). Regulating Privacy by Design. Berkeley Technology Law Journal, 26, 1409. [Skim, focus on 1421-1431] Rubinstein, I. and Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. NYU School of Law, Public Law Research Paper. [Skim]
4/11	Implementing Privacy by Design in Social Media	Quiz 3	Mulligan, D. K. and King, J. (2012). Bridging the Gap Between Privacy and Design. U. Pa. J.

			Const. L., 14, 989. [1017-1034] Hartzog, W. and Stutzman, F. (2013). Obscurity by Design. University of Washington Law Review. [Skim]
4/16	Privacy by Design and Big Data		Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57, 1701. [1703-1731] Narayanan, A. and Shmatikov, V. (2010). Myths and fallacies of personally identifiable information. Communications of the ACM, 53(6), 24--26. Barth-Jones, D. (2012) The Debate Over 'Re-Identification' Of Health Information: What Do We Risk? Health Affairs, August 10, 2012. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05), 557--570. Dwork, C. (2006). Differential privacy. Automata, languages and programming, 1--12.
4/18	Surveillance by Design		Calo, M. R. (2011). The drone as privacy catalyst. Stanford Law Review Online, 64, 29. Cavoukian, A. (2012). Privacy and Drones: Unmanned Aerial Vehicles. Information and Privacy Commissioner, Ontario, Canada. [Skim] McNeal, G. (2103). North Carolina's Poorly Worded Drone Killing Privacy Bill. Forbes, March 21, 2013.
4/23	Privacy and Face Recognition Technologies		Acquisti, A., Gross, R. and Stutzman, A. (2012). Privacy in the Age of Augmented Reality.
4/25		Case 4	Case 4 Presentation and Discussion – Google Glass
5/6	Final Exam	12PM in Davie 101	