THE UNIVERSITY OF ARIZONA
COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Harvill Building
1103 E. Second Street
Tucson, Arizona 85721
Phone: 520.621.3565
Web: www.si.arizona.edu

Information Privacy with Applications

ESOC 488, Section 001

Fall 2017

Tue/Thu, 2:00pm - 3:15pm, Chavez 109

Instructor:	David Sidi
Office Location:	HARV 456
Office Hours:	Fridays at 10:30am
Telephone:	(520) 621-3565
Email:	dsidi@email.arizona.edu
OpenPGP:	4096R/0x84969123EEBA824
Home page:	https://u.arizona.edu/~dsidi/

Grades: Desire to Learn (D2L): https://d2l.arizona.edu/

COURSE DESCRIPTION

This course provides an introduction to the fundamentals of information privacy, with applications developing privacy-enhancing technologies (PETs). Topics include: formal and informal conceptions of privacy; best practices for PET development / privacy by design; anonymous communication; obfuscation; database privacy; privacy in authentication. The course treats privacy technology as tied to social issues, and invokes a variety of disciplinary perspectives---legal, political, psychological, economic, and ethical, among others---however, no background in these areas is presupposed; relevant material is introduced as needed.

Sections are marked with '(*)' to indicate that all text within the section is university-mandated boilerplate required for all syllabi.

COURSE OBJECTIVES AND EXPECTED LEARNING OUTCOMES

Objectives. After taking this course, the student should be able to:

- Provide a sophisticated comparative account of how 'privacy' is used in a variety of disciplinary contexts
- Communicate a particular technology's privacy characteristics to different audiences, including

engineers, lawyers, policy makers, users, and the public

- Analyze privacy technologies with reference to their historical context
- Design and implement systems for enhancing privacy benefits and/or mitigating privacy threats, making use of existing privacy-enhancing technologies

ABSENCE AND CLASS PARTICIPATION POLICY

The UA's policy concerning Class Attendance, Participation, and Administrative Drops is available at: http://catalog.arizona.edu/policy/class-attendance-participation-and-administrative-drop. I expect you to attend each class session, except when you email me to explain why you cannot attend.

The UA policy regarding absences for any sincerely held religious belief, observance or practice will be accommodated where reasonable, http://policy.arizona.edu/human-resources/religious-accommodation-policy.dd

Absences pre-approved by the UA Dean of Students (or Dean Designee) will be honored. See: https://deanofstudents.arizona.edu/absences

COURSE COMMUNICATIONS

You can contact me using my university email address, listed above.

SCHEDULE

Foundations of Privacy (start: Aug 22)

Topic	Reading
Course Logistics and Introduction	none
Intellectual History of Privacy I	Keenan, *Invasion of Privacy: A Reference Handbook*. Chapter 1.2: Origins of the Right to Privacy Smith, R.E. Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet, 'Introduction', and Chapter 1: 'Watchfulness'
Intellectual History of Privacy II	Bruce, *The Firm : The Inside Story of the Stasi*, 'In the Line of Sight'
Speaker: Robert Ellis Smith	TBD
Intellectual History of Privacy III	Matz, 'Libraries and the USA PATRIOT Act: Values in Conflict'

	Privacy and public libraries. ALA policy on privacy
Intellectual History of Privacy IV	Greenwald, No Place To Hide, 'The Harm of Surveillance' Optional: Pompeo and Rivkin. 'Time for a Rigorous National Debate About Surveillance.' Wall Street Journal. Optional: Soghoian, 'Stopping Law Enforcement Hacking.' (video)
Foundations of Privacy and the Law I	Solove, 'The Twentieth Century' up to 'Responses to the Rise of the Computer' in "A Brief History of Information Privacy Law" Optional: Warren and Brandeis. "The Right to Privacy". Optional: Fair Information Practice Principles Optional: Robert Gellman, Fair Information Practices: A Basic History (pp. 1 - 12)
Foundations of Privacy and the Law II	Solove. "A Brief History of Information Privacy Law" remainder (past "Responses to the Rise of the Computer") Solove and Schwartz. "Privacy Law Fundamentals". Optional: Ladar Levison v. USA. Optional: 'FBI Harassement.' Blog entry by Isis Agora Lovecruft.
Speaker: Jane Bambauer	TBD
Landscape of Privacy Technologies I	Claudia Diaz and Seda Gürses, 'Understanding the landscape of privacy technologies.' Cegłowsky, 'Haunted by Data' (video) Excerpt from Langdon Winner, Do Artifacts Have Politics? (1986) Optional: Cypherpunk's manifesto Optional: Bert-Jaap Koops et al. A Typology of Privacy, University of Pennsylvania Journal of International Law

	(Forthcoming 2017) ,
Speaker: Laura Brandimarte	None
Landscape of Privacy Technologies II	Daniel Le Métayer, 'Whom to trust? Using technology to enforce privacy' in *Enforcing Privacy*
Landscape of Privacy Technologies III	Nissenbaum and Lowe. Obfuscation: A User's Guide. 'Why is obfuscation necessary?' Optional: Nissenbaum and Lowe. Obfuscation: A User's Guide. 'Core Cases.'

Layer 8+ Privacy

Topic	Reading
Introduction	Practical Packet Analysis, 'The Seven Layer OSI Model' PGP Manual: How it Works, The Gnu Privacy Handbook - GnuPG. 'Beware of Snakeoil.' Thompson, 'Reflections on Trusting Trust'
Biometrics	Anderson. "Biometrics" (in *Security Engineering*, 2nd edition, 2008). Geer, 'Identity as Privacy.' IEEE Security Privacy 11(1). Optional: The Perpetual Line-Up: Unregulated Police Face Recognition in America Optional: Unique in the Crowd: The Privacy Bounds of Human Mobility
Analog Hole Problems	Narayanan and Shmatikov, 'A Scanner Darkly: Protecting User Privacy from Perceptual Applications' Sicker et al., 'The Analog Hole and Cost of Music.' Section II. DRM And and the Analog Hole, Part A. Technical Overview. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions

Anonymous Communication and Traffic Analysis (start: ca. Oct. 19)

Topic	Reading
Background I	Torra, Data Privacy 1.3.2: Terminology--Anonymity and Unlinkability George Danezis and Claudia Diaz, 'A Survey of Anonymous Communication Channels' Optional: DNS background Optional: All About Networks Optional: TCP and UDP Ports Explained Optional: Understanding and Using Firewalls Optional: There and back again: a packet's tale (video)
Mix nets, Onion Routing (Tor)	Tor Overview Chaum, Mix nets Isis Agora Lovecruft, 'Anonymity Systems' (video) Optional: Danezis and Clulow, 'Compulsion resistent anonymous communications.'
Traffic Analysis	How To: Use mitmproxy to read and modify HTTPS traffic

Communication Privacy Systems (start: ca. Oct. 31)

Topic	Reading
Introduction	Diffie et al., Privacy on the Line, 'Cryptography'
Paradigms of Cryptography	Diffie and Hellman. 'New Directions in Cryptography.' Grigoriev and Shpilrain, 'Yao's Millionaires' Problem and Decoy-Based Public Key Encryption by Classical Physics'
PGP	PGP Manual: How it Works, The Gnu Privacy Handbook - GnuPG (up to PGP Quick Reference)

TLS and Certificate Transparency	Schmiedecker, ‘Everything you always wanted to know about Certificate Transparency but were afraid to ask’

Integrity, Authenticity, and Privacy (start: ca. Nov. 14)

Topic	Reading
Zero Knowledge Proof I	Claus-Peter Schnorr: Efficient Identification and Signatures for Smart Cards. CRYPTO 1989: 239-252
Zero Knowledge Proof II	Amos Fiat, Adi Shamir: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. CRYPTO 1986: 186-194

Database Privacy (start: ca. Nov 21)

Topic	Reading
Data anonymization	Simson L. Garfinkel, De-Identification of Personal Information, NISTIR 8053 (Oct. 2015), Torra, Data Privacy 1.3.3: Terminology--Disclosure Narayanan and Shmatikov. "Myths and Fallacies of 'Personally Identifiable Information'".
k-anonymity, l-diversity, t-closeness	Li et al., ‘t-closeness.’
cryptographic obfuscation	Narayanan and Shmatikov, ‘Uncircumventable Enforcement of Privacy Policies via Cryptographic Obfuscation’
De-anonymization attacks	Robust De-anonymization of large sparse datasets Golle, ‘Revisiting the uniqueness of simple demographics in the US population’ Denning et al. "The tracker: A threat to statistical database security." ACM Transactions on Database Systems 4.1 (1979): 76-96.

COURSE MATERIALS

There is no textbook for this course; see the schedule for readings selected from a variety of sources.

SPECIAL MATERIALS

- Live Question Tool: Rather than raising a hand to ask a question, we will use an online tool that allows questions to be posted (anonymously, if you wish) and voted on by the class.
- To participate in class activities, you must bring a laptop

ASSIGNMENTS

- Assignments will be turned in via d2L.
- There wil be two assignments during the semester, and one final project on a topic of your choosing.
- Each Tuesday there will be a small quiz on the readings.

FINAL PROJECT

There is a final project in this class, but no final exam. The final project is due the day and time of the final exam, which is found at http://www.registrar.arizona.edu/schedules/finals.htm.

GRADING SCALE AND POLICIES

- Grading policy: 25% for each assignment, 35% final project, 15% class participation.
- (*) Requests for incomplete (I) or withdrawal (W) must be made in accordance with University policies, which are available at http://catalog.arizona.edu/policy/grades-and-grading-system#incomplete and http://catalog.arizona.edu/policy/grades-and-grading-system#Withdrawal respectively.
- (*) Dispute of Grade Policy: Provide the acceptable time period for disputing a grade on a paper, project, or exam.

HONORS CREDIT (*)

Students wishing to contract this course for Honors Credit should email me to set up an appointment to discuss the terms of the contract. Information on Honors Contracts can be found at https://www.honors.arizona.edu/honors-contracts.

THREATENING BEHAVIOR POLICY (*)

The UA Threatening Behavior by Students Policy prohibits threats of physical harm to any member of the University community, including to oneself. See http://policy.arizona.edu/education-and-student-affairs/threatening-behavior-students.

ACCESSIBILITY AND ACCOMMODATIONS (*)

Our goal in this classroom is that learning experiences be as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, please let me know immediately so that we can discuss options. You are also welcome to contact the Disability Resource Center (520-621-3268) to establish reasonable accommodations. For additional information on the Disability Resource Center and reasonable accommodations, please visit http://drc.arizona.edu.

If you have reasonable accommodations, please plan to meet with me by appointment or during office hours to discuss accommodations and how my course requirements and activities may impact your ability to fully participate.

Please be aware that the accessible table and chairs in this room should remain available for students who find that standard classroom seating is not usable.

ACADEMIC INTEGRITY AND STUDENT CODE OF CONDUCT (*)

Students are encouraged to share intellectual views and discuss freely the principles and applications of course materials. However, graded work/exercises must be the product of independent effort unless otherwise instructed. Students are expected to adhere to the UA Code of Academic Integrity as described in the UA General Catalog. See: http://deanofstudents.arizona.edu/academic-integrity/students/academic-integrity.

UNIVERSITY NONDISCRIMINATION AND ANTI-HARASSMENT POLICY (*)

The University is committed to creating and maintaining an environment free of discrimination; see http://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy

ADDITIONAL RESOURCES FOR STUDENTS (*)

- Office of Diversity: http://diversity.arizona.edu/
- Counseling and psychological Services: http://www.health.arizona.edu/counseling-and-psych-services
- Oasis: http://oasis.health.arizona.edu/

CONFIDENTIALITY OF STUDENT RECORDS (*)

http://www.registrar.arizona.edu/personal-information/family-educational-rights-and-privacy-act-1974-ferpa?topic=ferpa

UNIVERSITY PRONOUN NAME POLICY (*)

Instructors and students will use names and pronouns as requested, and instructors will update their rosters to accommodate students who modify their names and/or pronouns after course registration. Instructors will make specific reference to the name and pronoun usage statement in the syllabus on the first day of class and model correct name and pronoun usage in the classroom.

SUBJECT TO CHANGE STATEMENT (*)

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.