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

Privacy Technologies in Context

ESOC 488, Section 001

Fall 2018

Tue/Thu, 2:00pm - 3:15pm, Harvill 332C

Instructor:	David Sidi
Office Location:	HARV 456 / HARV 454
Office Hours:	Fridays at 10:30am
Telephone:	(520) 621-5703
Email:	dsidi@email.arizona.edu
PGP Fingerprint:	9FB6 167B D4BD 44FE 90F7 51D0 87B6 0D65 3A14 517D
Home page:	https://u.arizona.edu/~dsidi/

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

COURSE DESCRIPTION

This course provides a hands-on introduction to computer privacy technologies. This will involve not only the making and breaking privacy technologies, but cultivation of a broader understanding of privacy from a variety of disciplinary perspectives. Topics will include citizen and consumer privacy, ethics and privacy, privacy and trust, obfuscation, anonymous communication and traffic analysis, communications privacy, and privacy and smart devices.

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, and a nontechnical general audience

- Analyze privacy technologies with reference to their historical context
- Recognize flaws in computer privacy technologies, and know how to fix them
- 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

If you don't appear in my office hours (or by appointment), I will be less likely to be sympathetic if you find you are struggling with an assignment.

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.

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

COURSE COMMUNICATIONS

Email is the preferred method for contacting me. Responses may take up to 24 hours during the week. For more urgent matters, please use the lab phone given above.

SCHEDULE

Why Care about Privacy?

	Topic	Reading
08/21	Course Logistics and Introduction	none
08/23	Consumer privacy I	Stephens-Davidowitz, *Everybody lies* (excerpt) Maciej Cegłowsky, 'Haunted by Data' (video) Optional: NY Times, 'What 7 Creepy Patents Reveal about Facebook'
08/28	Consumer privacy II	Pasquale, *Blackbox Society* (excerpt)

		‘Privacy and Commercial Data Collection.’ Discussion moderated by Laura Brandimarte. Optional: Fair Information Practice Principles Optional: Robert Gellman, Fair Information Practices: A Basic History (pp. 1 - 12) **Assignment: Insecure server challenge**
08/30	Citizen privacy I Speaker: Laura Brandimarte	Laura Brandimarte, ‘Does Government Surveillance Give Twitter the Chills?’ **Assignment: Write up, Discussion Questions**
09/04	Citizen privacy II	*Invasion of Privacy: A Reference Handbook.* (excerpt) Bruce, ‘In the Line of Sight.’ In *The Firm : The Inside Story of the Stasi*. Optional: Smith, R.E. ‘Introduction’, and Chapter 1: ‘Watchfulness’. In *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*.
09/06	Citizen privacy III	*The United States of Secrets*, Frontline Documentary. Parts 1 and 2. Glenn Greenwald, The Harm of Surveillance. In *No Place To Hide*. Optional: Ladar Levison v. USA
09/11	Ethics and Privacy I	Julia Annas, The Virtues. In *The Morality of Happiness*. **Assignment: Insecure server challenge 2**
09/13	Ethics and Privacy II Speaker: Julia Annas	Applying virtue to ethics, in *Journal of Applied Philosophy* **Assignment: Write-up, discussion questions**
09/18	Ethics and Privacy III	Rosalind Hursthouse. *Environmental virtue ethics*. (excerpt)

Trust and Privacy

	Topic	Reading
09/20	Threat Modeling	Adam Shostack, Chapter 2: Strategies for threat modeling. In Threat Modeling: Designing for security. NSA Aqua Book and RFC 2196, Sect. 2.1.1 Computer Science and Telecommunications Board, 'Trust in cyberspace' (Introduction and Part 2: Public Telephone Network and Internet Trustworthiness, Section: 'Attacks on the Internet') Joanna Rutkowska, 'Security through Distrusting.'
09/25	The Web of Trust	PGP Manual: How it Works, The Gnu Privacy Handbook - GnuPG (up to PGP Quick Reference)
09/27		
10/02	Interpersonal trust	Friedman et al., 'Trust online.' Ken Thompson, 'Reflections on Trusting Trust' Optional: Diverse double-compiling **Assignment: Threat model**

Computer privacy technologies: overview

	Topic	Readings
10/04	Background I	Daniel Le Métayer, 'Whom to trust? Using technology to enforce privacy' in *Enforcing Privacy* Rawat et al., Data Protection. Journal of

		Craptology. (!)
10/09	Background II	Claudia Diaz and Seda Gürses, 'Understanding the landscape of privacy technologies.' Optional: Cypherpunk's manifesto
10/11	Obfuscation	Helen Nissenbaum and Lowe. Obfuscation: A User's Guide. 'Why is obfuscation necessary?'
10/16	Obfuscation II	Nissenbaum and Lowe. Obfuscation: A User's Guide. 'Core Cases.'
10/18	~~Obfuscation III: Cryptographic obfuscation (cancelled)~~	~~Narayanan and Shmatikov, 'Uncircumventable Enforcement of Privacy Policies via Cryptographic Obfuscation', in *Privacy Technologies*~~

Anonymous Communication and Traffic Analysis

	Topic	Reading
10/23	Background I	'TCP/IP overview,' in *TCP/IP Network Administration* 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) **Assignment: Certificate challenge (due 22 October 2018, by 2:00 PM MST)**
10/25	Mix nets, Onion Routing (Tor)	Tor Overview Chaum, Mix nets Optional: Danezis and Clulow, 'Compulsion

		resistent anonymous communications.'
10/30	Traffic Analysis	How To: Use mitmproxy to read and modify HTTPS traffic **Assignment: Accessing tor in a program with stem; running an onion service**

Communications Privacy Systems

	Topic	Reading
11/01	Introduction	Whitfield Diffie et al., Privacy on the Line, 'Introduction' and 'Cryptography'
11/06	Paradigms of Cryptography	Whitfield Diffie and Martin Hellman. New Directions in Cryptography. Optional: RSA Patent.
11/08	Paradigms of Cryptography	Dan Boneh et al., Functional Encryption. **Assignment: Breaking weak cryptography**
11/13	TLS and Certificate Transparency	Martin Schmiedecker, 'Everything you always wanted to know about Certificate Transparency but were afraid to ask'

Layer 8+ Privacy

	Topic	Reading
11/15	Introduction	PGP Manual: How it Works, The Gnu Privacy Handbook - GnuPG. 'Beware of Snakeoil.'
11/20	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
11/22	Analog Hole	Arvind Narayanan and Vitaly Shmatikov, 'A Scanner Darkly: Protecting User Privacy from Perceptual Applications' Ryan Calo. Robots and Privacy.
11/27	Analog Keyhole	Sidi and Brandimarte. Infrastructural Solutions to the Analog Keyhole Problem. **Assignment. Face recognition countermeasures with OpenCV.**
11/29, 12/04		**Student presentations**

Database Privacy (Honors)

	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' **Assignment: Privacy theater and DB privacy**
	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.
- You must bring a laptop to every class session.

ASSIGNMENTS

- Assignments will be turned in via d2L. Be sure to turn in files exactly as described in the assignment: file names, formatting, etc. matters.
- There will be five “challenges” to break some privacy property on the course server. (4% each)
- There will be two programming assignments, building and working with existing privacy technologies. (20%)
- There will be five write-ups. (20%)
- There will be one final project on an approved topic of your choosing. The final project will be done in a group of three, in lieu of a final exam. (30%)
- There will also be participation (10%)

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: See assignments, where the scale is represented next to the assignment description.

- (*) 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. If we have enough interest (and I know about it early enough), we may form an honors section.

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.