CS 175 – Communications Security and Social Movements

Catalog Description: Equipping students with the theory and practice of communications security, this course explores how social movements can remain effective in the context of mass surveillance and state repression.

Credits: 4 Terms Offered: Spring (negotiable)

Prerequisites: None

Courses that require this as a prerequisite: None

Structure: On campus, two 1 hour 50 minute lectures per week

Instructors: Glencora Borradaile

Course Content:
Historic asymmetry in power between governments and large corporations on the one hand and grassroots social and political movements on the other persists in the information age. Social movements newly empowered with instantaneous mass communications and social media are simultaneously threatened with ubiquitous, suspicionless surveillance. However, privacy-enhancing technologies can shift the balance of power to individuals and social movements, especially those opposing corporate and state power to overcome structural, institutional, or ideological discrimination.

This course involves a hybrid of instruction in the technical basis and practical use of privacy-enhancing online communication tools and an exploration of their utility in the context of widespread state surveillance. In active- learning in-class exercises, we will set up and understand implementations of Pretty Good Privacy (PGP) encryption for sending private emails; Off The Record (OTR) encryption to enable secure instant messaging; and The Onion Router (TOR) to allow anonymous Internet activity. The underlying security protocols will be physically acted out.

In-class discussions will explore the role of privacy-enhancing online communication tools in empowering social movement organizing. The class will explore well-documented historic abuses of power in the state-sponsored surveillance and disruption of diverse, justice-oriented social movements such as the Black Panther Party, the American Communist Party, and the American Indian Movement. For instance, the U.S. Federal Bureau of Investigation Counter-Intelligence Program (COINTELPRO) disruption of black power and civil rights movements beginning in the 1950s will provide context for present-day abuses of power under the PATRIOT Act and PRISM- related U.S. domestic mass surveillance, and the protective role encryption technologies might play today. In these discussions, those socially-constructed categories (such as race) used to justify such state abuses will be critically examined. To provide comparative international context, we will also explore the possibilities of unchecked mass surveillance and Internet censorship in overseas authoritarian regimes. Throughout, writing assignments will provide the opportunity for reflection on surveillance-enabled abuses of state power and the potential role of secure communications in overcoming these.

Students will complete a major project featuring an in-class presentation and a written or recorded component to demonstrate and explain to their peers a privacy-enhancing online communication tool and discuss the social- movement context in which the tool could be useful.
Course materials include necessary hardware and software (Debian Live bootable USB disk), primary sources, scholarly articles, book chapters, and films.

**DPD Statement:**
CS 175: Secure Communications and Social Movements fulfills the Difference, Power, and Discrimination (DPD) requirement in the Baccalaureate Core. The DPD requirement engages students in the intellectual examination of the complexity of the structures, systems, and ideologies that sustain discrimination and the unequal distribution of power and resources in society. The unequal distribution of social, economic, and political power in the United States and in other countries is sustained through a variety of individual beliefs and institutional practices. These beliefs and practices have tended to obscure the origins and operations of social discrimination such that this unequal power distribution is often viewed as the natural order. Examination of DPD course material will enhance meaningful democratic participation in our diverse university community and our increasingly multicultural U.S. society.

**Learning Resources:**
Access to a computer is required for this course. Ideally students will have a laptop available to be booted with the Debian Live operating system from a (provided) USB disk (http://live.debian.net) and can bring to the classroom as needed. Alternate arrangements will be made in cases where this presents a barrier.

**List of Technical Resources:**
- EFF surveillance self defense tutorials [https://ssd.eff.org](https://ssd.eff.org)
- strong passwords – Micah Lee [https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess](https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess)
- OTR: encryption, authentication, deniability – https://www.youtube.com/watch?v=aV6-s9o9bVw

**List of Readings & Primary Sources:**
*Week 1*: Ta-Nehisi Coates “The Case for Reparations” *The Atlantic* June 2014
[http://www.theatlantic.com/magazine/archive/2014/06/the-case-for-reparations/361631](http://www.theatlantic.com/magazine/archive/2014/06/the-case-for-reparations/361631);
Jonathan Christiansen “Four Stages of Social Movements” (overview)


Week 4: NSA and Internet security - [http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html](http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html) (and primary documents linked)

Week 5: [student presentations]


Week 8: [student presentations]


### Schedule of Topics

<table>
<thead>
<tr>
<th>Block</th>
<th>Technical Concepts</th>
<th>Social Context</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Black Power, Message Integrity &amp; Authenticity</strong> <em>(Weeks 1-5)</em></td>
<td>How the Internet works: email, messaging, &amp; the world wide web</td>
<td>Intro to State Power: COINTELPRO to PATRIOT Act</td>
</tr>
<tr>
<td></td>
<td>Operating system security</td>
<td>NSA revelations: crackers &amp; cracking</td>
</tr>
<tr>
<td></td>
<td>Online threat modeling</td>
<td>#blacklivesmatter &amp; social media tracking</td>
</tr>
<tr>
<td></td>
<td>How encryption works</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public key cryptography &amp; PGP authentication</td>
<td></td>
</tr>
<tr>
<td><strong>End of Block 1: Wrap-up, Student Projects &amp; Presentations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Red Scare, Message Privacy &amp; Secrecy</strong> <em>(Weeks 6-8)</em></td>
<td>PGP encryption</td>
<td>Introduction to security culture</td>
</tr>
<tr>
<td></td>
<td>OTR</td>
<td>The Red Scare: intersectionality &amp; state repression</td>
</tr>
<tr>
<td></td>
<td>Cryptocat</td>
<td></td>
</tr>
<tr>
<td><strong>End of Block 2: Wrap-up, Student Projects &amp; Presentations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Censorship, State Violence &amp; Online Anonymity</strong> <em>(Weeks 9-10)</em></td>
<td>TOR/Tails</td>
<td>Keeping journalists safe in totalitarian states</td>
</tr>
<tr>
<td></td>
<td>SSL, HTTPS</td>
<td>Jumping the Great Firewall of China</td>
</tr>
<tr>
<td></td>
<td>VPN</td>
<td>Tahrir Square: overcoming network disruption</td>
</tr>
<tr>
<td><strong>End of Block 3: Wrap-up and Course Review</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Measurable Student Learning Outcomes:
This course fulfills OSU Baccalaureate Core’s **Difference, Power, and Discrimination** category. DPD learning outcomes:

1. **Explain** how difference is socially constructed;
2. Using historical and contemporary examples, **describe** how perceived differences, combined with unequal distribution of power across economic, social, and political institutions, result in discrimination.
3. **Analyze** ways in which the interactions of social categories, such as race, ethnicity, social class, gender, religion, sexual orientation, disability, and age, are related to difference, power, and discrimination in the United States.

Students who successfully complete the course will also be able to:

1. **Understand** concepts of communication security and basic encryption.
2. **Effectively use** and **explain** to others secure online communication tools.
3. **Describe** and **contextualize** uses of surveillance to suppress social movements both historically and currently.
4. **Identify** existing and potential uses of secure online communication tools to enhance the effectiveness of social movements.

Evaluation of Student Learning:

30% **Quizzes and short assignments**
These will assess student understanding of technical concepts and their ability to use privacy-enhancing online communication tools.

25% **Written responses to readings and primary sources**
Students will select readings and primary sources and provide short written responses that:
- illustrate historical use of surveillance and infiltration in the disruption of social movements engaged in countering discrimination and lack of access to power
- comment on the potential for suppression of dissent enabled by contemporary mass surveillance. 

An effective response will be 250-750 words in length, and will demonstrate an understanding of how state surveillance was or can be used to maintain unequal distribution of power across economic, social, and political institutions by undermining the social movements that seek to address inequity. In order to receive credit, a response must be submitted prior to the class session for which the material will be discussed. Responses should be in complete sentences and paragraphs, observing proper grammatical, spelling, and punctuation conventions.

5% **Peer critiques**
Students will provide constructive and evaluative critiques of project presentations by their peers. Critiques should address the following: Were you able to understand how the tool works? Could you use the tool as described? Was the social movement context meaningful and clearly described?

40% **Projects**
Students will choose a privacy-enhancing technology not covered in lecture (e.g. mesh networking, mobile device security, file and whole-disk encryption, secure collaborative documents, steganography). Students will:
- explain how the technology works conceptually;
- explain what surveillance threat the technology prevents against;
- demonstrate correct setup and use of the technology; and,
- describe a social-movement context in which the tool was or could be deployed.

In-class presentations (10% of final grade) will provide a first look at student projects. Students will prepare a final project submission in any easily shared format (e.g. a wiki, zine, video) that meets the above requirements. The final submission (30% of final grade) should take into account peer critiques and
instructor feedback based on the first-look presentation. Students will work in groups of 2 or 3; each group shall have at least one member who has technical familiarity at the onset of the course. The technology of choice and final submission format will be approved by the instructor.

**Course communication** will occur verbally during class and in writing via the course website and email list. It is your responsibility to keep up with class news, as occasionally schedules of reading assignments and due dates may change; if you miss class, please ask a classmate to fill you in on any important notifications you may have missed, and be sure to check your OSU e-mail account regularly.

**Students with Disabilities:**
Accommodations are collaborative efforts between students, faculty and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at 541-737-4098.

**Link to Statement of Expectations for Student Conduct,** i.e., cheating policies http://oregonstate.edu/studentconduct/offenses-0
Please make yourself familiar with the **Student Conduct Code**, which can be accessed at http://studentlife.oregonstate.edu/studentconduct/. Please pay particular attention to the section on Academic Dishonesty, which OSU defines as “an intentional act of deception in which a student seeks to claim credit for the work or effort of another person or uses unauthorized materials or fabricated information in any academic work." For some guidelines on plagiarism, see http://www.wpacouncil.org/node/9, and don’t hesitate to talk to me if you are uncertain about how to properly utilize or cite material.

Revised: Winter 2016