Week 20: Data security for researchers, reporters, and the like

October 17, 8:30 am Pacific/11:30 am Eastern

Overview

Strong investigative journalism and fearless research are both more important than ever in an environment of “alternative facts” and constant attacks on the free press. This week, Micah Lee of *The Intercept* will talk to us about the unique threat model of researchers and reporters, and how they manage security in the newsroom. He’ll talk about things like the difference between anonymous communication and encrypted communication, browser fingerprinting, protecting the privacy of people named in leaked documents, airgapped computers, and doing research with Tor and Tor-powered tools like OnionShare and SecureDrop.

Learning objectives

- Understand the researcher and journalist threat models
- Learn about tools used at *The Intercept* for data and communications security

Readings

- The Intercept Welcomes Whistleblowers
- How We Prepared NSA’s Sensitive Internal Reports for Release
- Cybersecurity for the People: How to Keep Your Chats Truly Private With Signal
- Chatting in Secret While We’re All Being Watched

Guest lecturer

Micah Lee of *The Intercept*

Discussion

- What’s unique about this threat model? How does it overlap with other threat models we’ve discussed?
- How would you use these strategies and tools in your own communities?

Assignment

Continue work on final assignments.