Cyber Freedom & Security

Fall 2017

Facilitator:	Sean O'Brien	**Time:**	Wed. 5:30pm – 7:30pm
E-mail:	sean.obrien@yale.edu	**Place:**	Bass Library (Room L34A)

Statement: This reading group will focus on cyber freedom in law and cyber security in practice. Though often perceived as diametrically opposed, the concepts of cyber freedom and cyber security are in fact complementary, with software, hardware, and spectrum freedom as a prerequisite (but not a guarantee) for cyber security. We explore this relationship within the context of pervasive corporate and government surveillance, a reality exposed most prominently by the 2013 Edward Snowden disclosures. Snowden relied upon a mix of Free and Open-Source Software (FOSS) to communicate extremely sensitive data, despite powerful adversaries, because he simply "couldn't trust" proprietary alternatives. The contemporary lawyer and legal scholar faces a sea of complex digital choices, which may be better informed through studying the security practice of whistleblowers, activists, and journalists. Contemporary problems are further complicated by the increasing frequency and escalation of cyber attacks, massive data breaches, and the threat of global cyberwar. We will reflect upon these current events, discussing their effect on the cyber landscape.

Objectives: We try to be as comprehensive as possible, discussing a wide variety of FOSS tools/applications with accompanying real-world examples. At the end of the course, a participant should be able to:

1. Understand the significance of privacy as it applies to software-mediated communication.
2. Describe the general scope of Five Eyes government surveillance and that of corporate partners.
3. Perceive the importance of FOSS, transparent development, and open technology as security principle.
4. Evaluate emerging technology on its merit and potential for data security, privacy, and anonymity.
5. Initiate and sustain encrypted communication, often over networks that safeguard anonymity.
6. Apply simple techniques to everyday Web browsing that improve user privacy and data security.
7. Explore the digital frontiers of GNU/Linux, P2P, Tor, and the Deep Web.
8. Develop a communications plan for real-world implementation of privacy-respecting technology.

Schedule: Wednesdays 5:30pm – 7:30pm, roughly every other week (see sessions below for specific dates).

Session 1 - Why Free and Open-Source Software Matters (August 30, 2017)

Readings:

- Software Freedom Law Center, *A Legal Issues Primer for Open Source and Free Software Projects* (2008), Chapters 1 & 2: https://www.softwarefreedom.org/resources/2008/foss-primer.html
- Free Software Foundation, Inc. v. Cisco Systems, Inc., No. 8-CV-10764 (S.D.N.Y. 2008). https://www.fsf.org/licensing/complaint-2008-12-11.pdf
- Edward Snowden, "The Last Lighthouse: Free Software in Dark Times," Mar. 19, 2016: http://ioterror.com/items/show/34
- Bruce Schneier and Eben Moglen, "Snowden, the NSA, and Free Software," Dec. 12, 2013: http://ioterror.com/items/show/4

In-class Video:
Richard Stallman, "Introduction to Free Software and the Liberation of Cyberspace," Apr. 7, 2014: https://www.fsf.org/blogs/rms/20140407-geneva-tedx-talk-free-software-free-society

Hands-on with: Etherpad, Jitsi Meet, Riseup Share/Up1, Firefox Send, Wire

Session 2 - Going Dark (September 13, 2017)

Readings:

- Wikimedia Foundation, et al. v. National Security Agency, et al., No. 15-2560 (D. Md. 2015). https://www.aclu.org/files/assets/wikimedia_v2c_nsa_-_complaint.pdf
- Berkman Center for Internet & Society, *"Don't Panic" Making Progress on the "Going Dark" Debate* (2016), pp. 1-12: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf
- Asher Schechter, "Who Needs the KGB when we have Facebook? An Interview with Eben Moglen," Apr. 8, 2015: http://emoglen.law.columbia.edu/my_pubs/Who-needs-KGB-when-we-have-Facebook-Schechter.pdf
- National Security Agency, "Tor Stinks," Jun. 2012: https://www.eff.org/files/2014/04/09/20131004-guard-tor_stinks.pdf

In-class Video:
Tor Project, "Introduction to Tor," Mar. 17, 2015: https://www.youtube.com/watch?v=JWII85UlzKw

Hands-on with: Better Web browsing & search, Ad-blockers, Ad-blockers, FreedomBox, Tor Browser

Session 3 - Operating System Insecurity (September 27, 2017)

Readings:

- Tom Mendelsohn, "Secure Boot snafu: Microsoft leaks backdoor key," Aug. 11. 2016: http://arstechnica.com/security/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/
- The Associated Press, et al. v. Federal Bureau of Investigation, No. 16-CV-1850 (D.D.C. 2016). https://assets.documentcloud.org/documents/3109606/16-Cv-1850-Dkt-No-1-Complaint.pdf
- Daniel Kahn Gillmor, "Is This the FBI's 'New' Method for Unlocking the San Bernardino iPhone?," Mar. 22, 2016: https://www.aclu.org/blog/free-future/fbis-new-method-unlocking-san-bernardino-iphone
- Jacob Appelbaum, "To Protect and Infect, the Militarization of the Internet," Dec. 31, 2013: http://www.nakedcapitalism.com/2014/01/jacob-appelbaum-30c3-protect-infect-militarization-internet-transcript.html

In-class Video:
The Linux Gamer, "What Is Linux?," Sep. 22, 2015: https://www.youtube.com/watch?v=tFFNiMV27VY

Hands-on with: Tails, Quillux (Privacy Lab's GNU/Linux distro)

Session 4 - The Spy In Your Pocket (October 4, 2017)

Readings:

- Atari Games Corp. v. Nintendo of America Inc., 975 F.2d 832 (Fed. Cir. 1992). https://scholar.google.com/scholar_case?case=15866317401594691669
- Ron Amadeo, "Google's iron grip on Android: Controlling open source by any means necessary," Oct. 20, 2013: http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/4/
- E-mail from Lisa Jackson to John Podesta, *Wikileaks Podesta E-mails Archive*, Dec. 20, 2015: https://wikileaks.org/podesta-emails/emailid/30593#efmAHtANd
- Tobias Boelter, "WhatsApp vulnerability explained: by the man who discovered it," Jan. 16, 2017: https://www.theguardian.com/technology/2017/jan/16/whatsapp-vulnerability-facebook

In-class Video:
Jonas Anton Östman, "Liberating Software at the Lower Levels" (first 11 mins), Feb. 8, 2016: https://www.youtube.com/watch?v=1ZIX1zO7pAs

Hands-on with: F-Droid, Orfox, GNU Ring, Riot.im

Session 5 - Sharing On A Hostile Web (October 18, 2017)

Readings:

- Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide," Oct. 30, 2013: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
- Samuel Gibbs, "Dropbox hack leads to leaking of 68m user passwords on the internet," Aug. 31, 2016: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
- Electronic Frontier Foundation, *Encrypt The Web Report*, Nov. 4, 2014: https://www.eff.org/encrypt-the-web-report
- United States v. Lavabit, LLC, et al., No. 13-4625 (4th Cir. 2014). http://cases.justia.com/federal/appellate-courts/ca4/13-4625/13-4625-2014-04-16.pdf

In-class Video:
Code.org, "The Internet: Encryption & Public Keys," Aug. 21, 2015: https://www.youtube.com/watch?v=ZghMPWGXexs

Hands-on with: OnionShare, SparkleShare, Tahoe-LAFS

Session 6 - Plugging The E-mail Hole (November 1, 2017)

Readings:

- Microsoft Corp. v. United States, No. 14-2985 (2d Cir. 2017). http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2017-01-24.pdf
- Matthias Pfau, "Why a Private Key Should Not Be Stored on a Central Server," Jan. 25, 2016: https://tutanota.com/blog/posts/private-key
- H. Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption (Revised)* (1998), Chapters 1& 2: https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html

- Arun Vishwanath, "'Spearphishing' Roiled the Presidential Campaign," Nov. 8, 2016: https://theconversation.com/spearphishing-roiled-the-presidential-campaign-heres-how-to-protect-yourself-68274

In-class Video:
Dark Web Academy, "How PGP Works," Mar. 26, 2016: https://www.youtube.com/watch?v=CHi2RclGvIM

Hands-on with: PGP/GPG, Thunderbird, Enigmail

Session 7 - How I Learned to *Keep* Worrying (November 15, 2017)

Readings:

- Eben Moglen, "Snowden and the Future," Dec. 4, 2013, Part IV: http://www.snowdenandthefuture.info/PartIV.html
- Front Line Defenders, *Workbook on Security: Practical Steps for Human Rights Defenders at Risk* (2015), Chapter 5: https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk
- B. Schneier, K. Seidel, and S. Vijayakumar, *A Worldwide Survey of Encryption Products* (2016): https://www.schneier.com/academic/archives/2016/02/a_worldwide_survey_o.html
- United States v. Aaron Swartz, No. 11-CR-10260 (D. Mass. 2013). https://www.docketalarm.com/cases/Massachusetts_District_Court/1--11-cr-10260/USA_v._Swartz/docs/106.pdf

Last Session: Let's stay in touch with the tools we learned about!