https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
https://www.thoughtworks.com/insights/blog/all-internet-traffic-written-postcards
Week 10

https://developers.cloudflare.com/1.1.1.1/fun-stuff/dns-over-tor/
https://blog.torproject.org/dont-let-facebook-or-any-tracker-follow-you-web

Mike perry or mike tigas for mobile week

Week 11: Vendor agreements and library policies
Overview
Librarians have been some of the staunchest supporters of privacy, at least since the ALA Core Values of Librarianship were created in 1939. But our reliance on third-party vendors who don't necessarily share our values has created a disconnect between our beliefs and our practices. This week, Sarah Houghton, aka The Librarian in Black, will talk to us about vendor policies and privacy, and how to demand that our vendors respect our fundamental values in the products they sell us.

Learning objectives
- Learn about common privacy issues with vendors, like their use of third-party tracking
- Learn how to create better vendor agreements using the ALA Library Privacy Checklists
- Learn about vendors who actually do a good job

Readings
- Some about historical vendor breaches or bad stuff, like Adobe, Overdrive, Thompson/Reuters ICE agreement
- ALA Library Privacy Checklists http://www.ala.org/advocacy/privacy/checklists
- https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1330&context=collaborativelibrarianship
- http://www.readersfirst.org/
- https://drive.google.com/open?id=1jdPwQeC5RAUbBWLAhyIYxWHa0pTdVObc SJPL audit results (all but TotalBoox got back to them and promised to make changes, but what about other vendors?)
- https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security
- https://www.eff.org/files/2018/01/08/checklist_-_how_to_assess_a_vendors_data_security.pdf
-

Guest lecturer
Sarah Houghton, The Librarian in Black http://librarianinblack.net/librarianinblack/

Discussion
- How do your vendor policies measure up?
- Find trackers on your vendors using Lightbeam or Privacy Badger

Assignment
- Create an implementation plan for 1-3 vendors using the privacy checklists.

Week 12: Everything on the internet is a scam

Overview

Well, maybe not *everything* on the internet is a scam, but it sure is hard to tell when our inboxes overflow with AI-generated phishing emails, Twitter bots try to pick fights with us about politics, and our favorite news sites are nonconsensually mining Bitcoin by stealing our CPU power. This week, Gary Price of INFODocket will talk to us about what the hell is going on with internet scams, how the lack of a regulatory environment to protect internet consumers has created a digital black market, and what we can do to protect our privacy and identify malware, phishing, bots, malvertising, fake news, and other digital scammers.

Learning objectives
- Scams and where to find them
- Strategies for mitigating an attack and cleaning up after one

Readings
https://gizmodo.com/facebook-turned-its-two-factor-security-feature-into-th-1823006334/amp?__twitter_impression=true
Something actually good:
https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/
http://www.pbs.org/wgbh/nova/labs/lab/cyber/research#/corp/chooser

https://mobile.nytimes.com/2018/06/20/business/equifax-hack-small-claims-court.html

How to find out if you've been the victim

Revisit Facebook/Cambridge Analytica stuff here?

Guest lecturer
Gary Price of INFODocket

Discussion
- Talk about how you've encountered various internet scams personally or in the library
- How would you address this issue in an outreach environment, especially with lower literacy patrons?

Assignment
- Make a library handout or small poster about staying safe from scams (either about one type in particular, eg phishing, or general advice)

Week 13: Email encryption // more on teaching privacy

Overview

This week, privacy and security trainer Yakira Dixon will give us the rundown on making email more secure with end-to-end encryption. They'll talk about the various options for email encryption and the benefits and drawbacks of each one. We'll then return to our week 5 concept of threat modeling, thinking through teaching strategies for teaching different groups in our community.

Learning objectives

Readings

FSF email encryption guide
EFF Security Education Companion stuff about email
Dell's piece about Efail
Micah's piece about Efail

Guest lecturer

Yakira Dixon of Thoughtworks

Discussion
- Discuss teaching strategies for email encryption
- Discuss the other teaching strategies we went over this week

Readings

https://gizmodo.com/new-pgp-encryption-exploits-are-being-discovered-almost-1826329086

Assignment
- Make instructional slides for teaching email encryption, or;
- Make an outline for a program plan for teaching a class aimed at one particular threat model, or;
- Make an outline for a basic privacy training for staff

Week 14: Basic security for librarians

Overview

Understand the difference between privacy and security, how they often overlap but don't always, learn basic best practices for security

In this workshop we will be navigating the best ways to make digital privacy/security education accessible to youth under the age of 18. We will work through best practices and activities to pursue at your library to engage young people.

Introduction to Information Security for Librarians
- Overview of the Information Security industry
- Basic industry vocabulary words to help with creating alerts or comprehending industry news
- Lists of recommended industry resources
- A slightly deeper dive into the following areas: password management, social engineering, data management, physical security, end user security awareness/training

Learning objectives

Readings
Guest lecturer
Tracy Maleeff of Sherpa Intelligence

Discussion
How privacy and security often overlap, sometimes differ

Assignment
Make a security audit checklist for your library. Find out who is responsible for each thing and get to know them.

Week 15: EdTech and youth privacy
Overview
Unique issues facing young people including the technology we give them, plus strategies for teaching them

Learning objectives

Readings
https://www.huffingtonpost.com/entry/virginia-commonwealth-iris-scanner_us_55bbd29ae4b0b23e3ce2d000
https://www.edsurge.com/news/2017-02-08-want-social-emotional-learning-to-work-the-careful-balance-of-tech-and-relationships?utm_content=buffer0bf63&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
http://www.baltimoresun.com/news/maryland/education/bs-md-college-analytics-20160611-story.html

https://www.eff.org/deeplinks/2017/02/school-librarian-caught-middle-student-privacy-extremes
http://youthandmedia.org/
https://www.computerworld.com/article/2521075/windows-pcs/pennsylvania-schools-spying-on-students-using-laptop-webcams--claims-lawsuit.html
https://www.eff.org/issues/student-privacy
https://www.eff.org/deeplinks/2017/02/school-librarian-caught-middle-student-privacy-extremes
>
>
>
<https://www.eff.org/deeplinks/2017/02/school-librarian-caught-middle-student-privacy-extremes
>

Guest lecturer
Jessy Irwin
Nasma Ahmed, Digital Justice Lab

Discussion

Assignment
Something to do with outreach

Week 16: Artificial Intelligence
Overview

- basics of what AI is
- what people mean when they say it's a "black box"
- examples of its use, examples of the datasets that build it
- and then I think it's totally fine to focus on ethics rather than
directly about privacy. One thing I might assign as a reading is one of
Virginia Eubanks' essays on the digital poorhouse (excerpted from her
book). Or maybe something from Safiya Noble. You get the idea.
Essentially I want the LFI participants to understand what AI is, how
it's used (especially the implications for poor/marginalized people,
like Eubanks studies), major criticisms of that, and how it could be
used ethically. I can fill in the privacy connections with the readings
if you want to focus on ethics more broadly. How does all this sound?
Learning objectives

Learning objectives

Readings

Virginia eubanks -- the digital poorhouse [pdf]
How the machine thinks [pdf]

Guest lecturer
Caroline Sinders (speak on the 18th)

Discussion

Assignment
Begin final assignment this week

Week 17: Mobile devices and messaging
Overview
Mobile devices are not only ubiquitous, they've become the primary way of accessing the internet and communicating for the majority of internet users worldwide. However, they pose unique threats to privacy due to their fundamental design. This week, Harlo Holmes joins us to talk about mobile device privacy, why it's hard to achieve, and what apps exist to help protect privacy on mobile. We'll also discuss the landscape of messaging apps and how they each deliver on privacy promises.

Learning objectives
- Understand unique threats and challenges posed by mobile devices
- Learn about mobile apps to help protect privacy
- Learn the difference between popular messaging apps and how they protect privacy

Readings
https://www.engadget.com/2017/12/29/mobile-games-listening-children-watch/
eff.org/sms
Additionally, this set of resources from Tactical Tech could be useful, for those who want to explore the workings of a smartphone (they have printable cards for explaining the workings of a phone—I haven't used this in teaching myself, so I'm not sure about them as a teaching resource, however, they seem useful): https://myshadow.org/train

Guest lecturer
Harlo Holmes of The Guardian Project and Freedom of the Press Foundation

Discussion
- What are some of the unique ways that mobile devices threaten privacy?
- What are five steps someone could take for better privacy on her mobile device?
- Discuss the differences between Signal, Whatsapp, and iMessage

Assignment
- Create an instructional flyer about using messaging apps for better privacy; or
- Make five instructional slides about mobile device privacy

Week 18: off (Alison at Tor Meeting)
Optional readings and discussion

Assignment: continue work on final assignment

Week 19: Third party tracking
Overview
(expanding on Facebook/Google week to cover more of the landscape) how do things work? eg how is google tracking us to provide the ads that we're seeing. give people an understanding of how that's happening in advance of them installing privacy badger or whatever. could do some interesting exercises to help them understand. if i enter search terms on my firefox browser on my laptop, those things come up on my telephone immediately as suggestions or whatever

Learning objectives

Readings
https://www.reuters.com/article/us-usa-television-technology/fcc-approves-tv-technology-that-gives-better-pictures-but-less-privacy-idUSKBN1DG2XF
https://theintercept.com/2017/11/24/staggering-variety-of-clandestine-trackers-found-in-popular-android-apps/
https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#5135a6656668
https://twitter.com/existentialpink/status/948282677391712256
https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829
http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html
https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html?mtrref=www.google.com
https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/
https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/#568af4713141
https://addons.mozilla.org/en-US/firefox/addon/lightbeam/
https://backstage.1blocker.com/say-hello-to-1blocker-x-8b55efe1ae36

Guest lecturer
Eric Hellman

Discussion
Review Lightbeam and list your trackers
Go through a checklist of sites and see what trackers they use
Explore alternative funding models for websites (eg Brave browser)

Assignment
Download Privacy Badger, complete checklist
Incorporate third-party tracking info, Privacy Badger into privacy class curricula

Week 20: Operating systems
Overview
Issues with major operating systems, introduce more secure alternatives and how they can be
incorporated into library use/instruction

Learning objectives

Readings

Guest lecturer
Micah Lee of The Intercept

Discussion

Assignment

Week 21: The Internet of Things
Overview
privacy implications, consent implications, some technical background on the types of
information that end up being collected and what are the technical reasons why they are
collected in the first place. using technical in certain ways creates unexpected outcomes

- what is the Internet of Things
- privacy, consent, and security implications for IOT
- some examples of IOT ridiculousness out in the wild
- what can be done

Let me know if there are particular areas you want to cover or elaborate
on and then I'll write up a description. Also, if you have readings to
suggest that would be great. I'll send you the description plus the
discussion questions and assignment that I'll give the cohort that week.
Also, please let me know what affiliations you'd like me to list for you.

Learning objectives

Readings
Amazon Echo stuff
https://www.themarshallproject.org/2018/05/24/your-home-is-your-snitch?utm_medium=social&utm_campaign=sprout&utm_source=twitter

https://www.wired.com/story/congress-privacy-groups-question-amazons-echo-dot-for-kids/amp

Guest lecturer
Matthew Garrett

Discussion
Is IoT coming to your library?

Assignment

Week 22: Around the digital privacy/internet freedom world
Overview
Introduce FOSS, things to know eg conferences, blogs, people, organizations, history. How to contribute to open source. Maybe basics about git and command line.

Learning objectives

Readings
Free software principles
Connections between free software and privacy (pre and post Snowden)
Some readings from major free software blogs, conference materials, etc
Basics of Git and some Unix command line stuff

Guest lecturer
Someone from Free Software Foundation ideally Georgia Young (TBC)

Discussion
Talk about the value of free software in libraries, contributing to free software, incorporating it into library instruction

Assignment
Learn about another open source privacy project, contribute a ticket (bug report or feature request), log on to IRC (maybe), contribute to Git

Week 23: Metadata resistance
Overview
Understand the power of metadata when it comes to privacy, how much metadata is transmitted when we use the web, and what to do

Learning objectives

Readings
We Kill people based on metadata (https://www.youtube.com/watch?v=UdQiz0Vavmc)

Guest lecturer
Sarah Jamie Lewis

Discussion
Immersion MIT exercise?

Assignment
Tools: Briar, Ricochet
Practice teaching a class this week? Bring back experiences

Description: Even when data is encrypted, it is still often possible to discover and infer a lot of information about the communication from the metadata around it e.g. Do you really need to decrypt a phone call to know the context of a call to a crisis hotline at 3 in the morning?

Communications metadata is known to be exploited by various adversaries to undermine the security of systems, to track victims and to conduct large scale social network analysis to feed mass surveillance.

In this lecture we will cover what metadata is, the different kinds of metadata that can be recovered from web browsing, common messaging applications (as well as phone calls and texting), and embedded in documents. We will also discuss mitigation strategies for protecting yourself and others against metadata analysis.

Topics Covered: Metadata Collection, Networking Protocols, Pattern of Life Analysis
Tools Covered: Ricochet, Briar, Cwtch

Suggested Readings: I'm currently at the start of writing an introductory primer for Cwtch which covers a lot of metadata resistant topics. I'll link that to your once it is done.

The First Contact Problem - Getting to SecureDrop:
https://mascherari.press/the-first-contact-problem-getting-to-securedrop/ - How metadata in
network traffic can deanonymize a source.

Assignment Ideas:

By November I would hope Open Privacy has gotten to the point where we have an App based
on Cwtch (https://cwtch.im) that people can install.

Installing, Setting up and using Ricochet & Briar.

Week 24: Library privacy success stories
Overview
Librarians across the country have already had success incorporating privacy into their libraries
-- hear their stories and learn about how they did it, challenges they had, successes, advice etc

Learning objectives

Readings
[include outreach component in this week]

Guest lecturer
Chuck McAndrew, Melissa Morrone, METRO people, Data Privacy Project, other work to
showcase (not necessarily speakers, maybe readings and discussion)

Discussion

Assignment

Week 25: off for Thanksgiving
Optional readings and discussion
More of the Security Education Companion

Assignment: continue work on final assignment

Week 26: Final week
Overview
Wrap up final assignment

Reflections on the course
Make sure all material is up on Gitlab