Digital Privacy for Librarians (& Others)

Howard Besser, NYU
http://besser.tsoa.nyu.edu/howard/Talks/

Digital Privacy for Librarians (& Others)-

• Background/Importance
  – Timely
  – A personal story
  – Recent News
  – Listing the basic issues
• Digital Privacy Training Project: The Library Freedom Institute
  – Aims
  – Collaboration & Funding
  – Schedule/Timeline
  – Program/Curriculum
• The larger questions
  – Privacy vs. preserving the cultural record
  – Public Policy: regulation, gov’t intervention

CyberSecurity Awareness Month

A Personal Story

My uncle’s “Smart TV”

TV warned me that I needed to accept certain services
But to accept Services, it looked like I’d have to let them track me

Try reading a Privacy Policy on a TV screen

Is Your Vizio Television Spying on You? What to Know
NY Times, 2/7/2017
• This week, Vizio, one of the biggest makers of internet-connected televisions, agreed to pay $2.2 million to settle charges that it has been collecting and selling viewing data from millions of TVs without the knowledge or consent of the sets’ owners.
• Has sold more than 11 million internet-connected TVs since 2010
• Another is from gauging the effectiveness of advertisements, including the ability to “analyze a household’s behavior across devices,” using the IP address attached to all the internet-enabled gadgets in a home. That could mean tracking whether someone visited a website on their laptop after seeing a fast food commercial, or if an online ad motivated them to watch a TV show.
• Vizio has manufactured TVs since at least February 2014 with software turned on by default that collects “information about what a consumer is watching on a second-by-second basis.” It also was said to have remotely installed the software... onto TVs sold without it.

That Game on Your Phone May Be Tracking What You’re Watching on TV
NY Times, 12/28/2017
• The apps use software from Alphonso, a start-up that collects TV-viewing data for advertisers. Using a smartphone’s microphone, Alphonso’s software can detail what people watch by identifying audio signals in TV ads and shows, sometimes even matching that information with the places people visit and the movies they see. The information can then be used to target ads more precisely and to try to analyze things like which ads prompted a person to go to a car dealership.
• Mr. Chordia said that he could not disclose the names of the roughly 1,000 games and the messaging and social apps with Alphonso software because a rival was trying to hurt its relationships with developers.

Frequent public revelations of massive privacy attacks on:
• email providers
• health care companies
• governmental agencies
• universities
• political campaigns
• election officials
• other targets (including libraries)
Types of Digital Privacy Threats to Individuals

- Identity theft
- Fraud
- Advertising
- Exploitative marketing (subprime loans)
- Human rights violations

Privacy Issues are around us all the time

- Clips from the past week’s News-

New Business Models are built around what today we consider surveillance

- “Ride-hailing platforms track a variety of personalized statistics, including ride acceptance rates, cancellation rates, hours spent logged in to the app and trips completed. … Uber uses the accelerometer in drivers’ phones along with GPS and gyroscope to give them safe driving reports, tracking their performance in granular detail.”
  - Rosenblat, Alex, “When your boss is an algorithm”, NY Times, Oct 12, 2018

The trouble, though, is that business models for these device don’t often allow for the kind of continuing security maintenance that we are used to with more traditional computing devices. Apple has an incentive to keep writing security updates to keep your iPhone secure; it does so because iPhones sell for a lot of money, and Apple’s brand depends on keeping you safe from digital terrors.

- But manufacturers of low-margin home appliances have little such expertise, and less incentive. That’s why the internet of things has so far been synonymous with terrible security — why the F.B.I. had to warn parents last year about the dangers of “smart toys,” and why Dan Coats, the director of national intelligence, has identified smart devices as a growing threat to national security.

- The Internet of Things Consortium, an industry group that represents dozens of companies, did not respond to an inquiry.
Tech Workers concerned about Privacy
Dragonfly, Project Maven

Individual wanting to protect own privacy is still implicated by those around him/her

- Messages from others to him/her are captured
- Familial DNA

Familial DNA

We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans

Scooters are back in SF, and already people are behaving badly

- SF Chronicle, Oct 15, 2018

- Skip and Scoot have said they will share information with the San Francisco Municipal Transit Agency on locals’ riding habits — including where, when and how far — while at the same time guarding riders’ privacy
- “The GPS in our scooters lets us know where every scooter is, all the time,”

Digital Privacy Topics we cover in LFI

- government and law enforcement surveillance
- corporate/“third party surveillance”
- “the problem” other — intimate partners, family, classmates, school admin, employer, etc
- risk assessments/threat modeling
- right to privacy/privacy in the courts/legal matters, subpoenas
- best practices: preventing malware, passwords, data breaches, doxing
- privacy policies, vendor agreements
- Around the digital privacy/Internet freedom world
- Teaching privacy classes
- Issues unique to mobile devices, messaging
- email
- Internet of Things
- Youth Services

LIBRARY FREEDOM INSTITUTE AIMS
Privacy Declarations

• UN General Assembly’s Universal Declaration of Human Rights
• ALA’s Bill of Rights
• ALA’s Choose Privacy Week

Though ALA prioritizes privacy, libraries have problems protecting it

• “libraries are terrible at privacy,” using invasive tracking technologies like Google Analytics, and feeding sensitive patron information direct to Facebook through social media buttons — Barbara Fister, Inside Higher Ed, Feb 12, 2015
• only about 15% of academic and large public libraries have implemented even the most basic privacy protection for web queries (HTTPS) — Library Technology Reports May/June 2015

What is LFI?

Basic Aims

• Create over 80 Digital Privacy Advocates, primarily in public libraries through intensive training
  – 4-6 months of 1 or 2 webinars/week
  – Weekly readings and practical individual or group assignments
  – 5 hours/week release time
• Geographic dispersal
• Train the Trainer

Advocates will learn

Expectations of Privacy Advocates

• Undergo intensive training (6 months, 5 hours/week; or 4 months, 5 hours/week)
• Outreach to and liaison with community groups for privacy advising and instruction
• Conduct regional workshops
• Re-align own library to be highly respectful of digital privacy
• Encourage community engagement with privacy policy issues
Taught by staff and special guest trainers how to:

• Install, troubleshoot, and maintain privacy software on both patron machines and public library workstations.
• Teach own train-the-trainer workshops to other librarians in your region.
• Approach members of their community regarding privacy concerns and teach privacy-related community workshops.
• Use their new role as a Privacy Advocate to influence policy and infrastructure.

Outreach to most vulnerable groups

• Seniors
• Immigrant groups
• Muslims
• Groups with poor english skills
• Communities with lower levels of digital literacy, awareness of digital issues

COLLABORATION & FUNDING

Partners

• Library Freedom Projet (Tor)—4 previous years of running workshops
• NYU MIAP—15+ years of curriculum development & multiple instructional delivery methods

Funding

• IMLS
• $450K
• 3 years

Advisory Board

• Brewster Kahle, Founder & Director, Internet Archive
• Freddy Martinez, director, Lucy Parsons Labs (digital security in Chicago)
• Erinn Atwater, University of Waterloo Centre for Applied Cryptographic Research & advocate for digital security needs of women, queer, and transgender
• Nasima Ahmed (works at intersections of technology, policy, and community organizing)
• Laura Quilter, Copyright and Information Policy Librarian UMass Amherst, Adjunct Professor Simmons College School of Library & Information Science
• Scott Bonner, Director, Ferguson Municipal Public Library District
• Eric Hellman, founder & President, Free Ebook Foundation & prolific library privacy blogger
• T.J. Lamanna Cherry Hill Public Library in New Jersey
Outside Advisory Organizations

• ALA Intellectual Freedom Committee
• EFF
• ACLU
• Tor

LFI Website
https://libraryfreedomproject.org/lfip/

SCHEDULE/TIMELINE

Stages

• Publicity & Recruitment
• Iteratively build curriculum & delivery, evaluate curriculum & delivery, revise, and run it again

Schedule

• Publicity & Recruitment (# of applicants)
• Prepare initial curriculum & speakers
• June-Nov 2018 Run 6 mth Pilot with 13 participants
• Oct 2018-Mar 2019 Evaluate curriculum, instructors, delivery system & revise accordingly
• Apr 2019-Sep 2019 Run full 6 mth Institute for 30 participants
• Oct 2019-Jan 2020 Evaluate & prepare for shorter (4 mth) institutes
• 2020 Run two 4 mth Institutes for 20+ participants each
• Evaluate & make recommendations

Publicity & Recruitment

• Dec 2017-Feb 2018
• ALA
• Public Librarians
• Privacy groups
• Tweets from Jim Neal, Cory Doctorow
**Application Requirements**

- Letter from Supervisor agreeing to 5 hours/week release time for 6 consecutive months
- Cite any prior experience with
  - Training (particularly technical)
  - Outreach (particularly to “at risk” communities)
  - Involvement with regional cultural heritage groups
  - Policy
  - Implementing new programs within their library

**Assessment & Curriculum Revisions**

- Nov 2018-Feb 2019
- Interviews and questionnaires with participants, instructors/lecturers, Advisory Board
- RA for assistance

**Pedagogy (1/2)**

- Continual mix of concepts with practical exercises/experience
- Cohort Model
  - Collaboration btwn participants
  - Group projects
  - Bring them all together for intensive weekend about 1 month into project
- Exercises focus on projects that can be re-used and re-purposed
- Frequent illustrations using their own environment (personal impact)

**Pedagogy (2/2)**

- Weekly subjects
- Webinars (with expert speakers)
- Readings
- Exercises
- Threaded discussions
- Cohort Model
- Group Activities
- Intensive in-person weekend

**Themes**

- Your Digital Footprint
- Risk Assessment & Threat Modeling
- Balancing privacy protection against effort required (& every person will reach a different balance)
- Privacy Strategy & Tools
- Privacy expectation levels for different tasks (from town hall to private room)
- Doxing/Outing and other harassment usually happens within commercial products (needs to be mitigated or litigated)
Weekly Curriculum (1/2)

Weekly Curriculum (2/2)

Weekly live Webinar lectures (posted on Vimeo)

Weekly live Webinar lectures (posted on Vimeo)

Lecture on facilitating Whistle-Blowing

Post-Webinar Chat Discussions
https://libraryfreedom.chat/t/week-17-discussion/183
Discussion around Topical News Items

https://libraryfreedomchat.org/in-the-news

Tools, Protocols, etc.

- Tor, Tails
- Onionshare
- https, Encryption
- VPN
- Privacy Badger

Value of Cohort Model

- Emphasis on collaboration
- Learning from each other
- Creates long-term support network

Almost Each Week/Topic has

- Guest lecture
- Learning Objectives
- Readings
- Discussion Topics
- Assignment (with alternatives for participants lacking time that week, or for those whose patrons might not fit the profile)

Sample Discussion & Assignment (Youth)

- **Discussion**
  - How are young people uniquely affected by the loss of privacy?
  - What about the idea that young people don’t care about their privacy?
  - What did you learn about engaging youth in privacy discussions and workshops?
- **Assignment**
  - Come up with an outreach or programming idea aimed at youth, or;
  - Write a one-page handout about some of the privacy and security issues with EdTech;
  - aimed at youth librarians, school librarians, teachers, or parents, or;
  - If you don’t work with youth at all, continue developing one of your assignments from a previous week or start work on your final assignment

Sample Assignment (Personal info collected)

- [https://myactivity.google.com/myactivity](https://myactivity.google.com/myactivity)
Sample Assignment (Doxing)

Look for your personal info on data broker websites and try to remove it. Talk about what you learned. Here are some data broker opt-out links:

• http://www.spokeo.com/opt_out/new
• http://www.peekyou.com/about/contact/optout/index.php
• equest.html
• https://www.intelius.com/optout.php
• http://www.beenverified.com/opt-out-instructions
• Did you find your data on other sites? What was the opt-out process like?

Sample Assignment (3rd Party Tracking)

• Download one of the third-party tracker blockers. Here is a list of some of them:
  
  – ○ Privacy Badger: https://www.eff.org/privacybadger
  – ○ Lightbeam for Firefox (not actually a blocker, just identifies trackers):
  – ○ 1Blocker ad-blocker for iOS devices: https://backstage.1blocker.com/say-hello-to-1blocker-x8b55efe1ae3

• Then, write a comparison of two different tracker-blockers/ad-blockers, or incorporate one into privacy class curricula (either as part of a slide deck or curriculum you’re already working on, or alone).

• If this doesn’t fit into what you’re doing for your final assignment, incorporate this week’s information into that final assignment in your own way.

Intensive in-person meeting

• Focus both on technical (installations) and interpersonal (role-playing)

Library Freedom Institute

• Just at the early stages
• Much will change over time
• Interested in comments and other contributions

TENSION BTWN PRIVACY AND MAINTAINING THE CULTURAL RECORD

• Some specific issues
• Tools that partially address these issues
• The larger questions
EC’s Right to be Forgotten

As we know with Personal Digital Collections

- Personal documents, Social Media, email, personal photos are rich collections both documenting a person’s life, but in aggregate they document events as well as daily life in eras of time
- Phone camera automatically capturing metadata for date, time, geolocation, owner, etc. can offer useful information identifying the photo
  — For Discovery, Descriptive Metadata, Research, Contextualization
- But that same information can be used to harass or convict the photographer or people pictured in a photograph

Metadata from single phone photo [1/2]

Metadata from single phone photo [2/2]

FLICKR images

Images off my hard disk (Brazil election demonstrations)
I like this photo, but don’t have a clue about where/when it was taken

As we know with Personal Digital Collections

• Social Media, email, personal photos are rich collections both documenting a person’s life, but in aggregate they document events as well as daily life in eras of time
• Phone camera automatically capturing metadata for date, time, geolocation, owner, etc. can offer useful information identifying the photo
  – For Discovery, Descriptive Metadata, Research, Contextualization
• But that same information can be used to harass or convict the photographer or people pictured in a photograph

Identifying where you were, when, who you communicated with (1/2)

Twitter hands over records in NY Occupy case

Identifying where you were, when, who you communicated with (2/2)

• (CBS/AP) NEW YORK – “Twitter on Friday agreed to hand over about three months’ worth of tweets to a judge overseeing the criminal trial of an Occupy Wall Street protester, a case that has become a closely watched fight over how much access law enforcement agencies should have to material posted on social networks.”
  • “Harris had argued that seeking the accompanying user information violated his privacy and free association rights. The data could give prosecutors a picture of his followers, their interactions and his location at various points, Stolar said.”

Digital Archives contain sensitive Info

Personal records also contain PID which can be used for scams or to harass

• Social Security numbers on mundane records
• Credit card numbers on hotel reservations
• Addresses and phone numbers of 3rd parties
Some newer redaction tools

Tools for masking photos: ObscuraCam (1/2)

ObscuraCam (2/2)

Tools for Masking addresses/numbers (Bitcurator)
Finding Potentially Sensitive Data using bulk_extractor

Redacting SS#s (Bitcurator)

PUBLIC POLICY: REGULATION, GOV’T INTERVENTION
Public Policy, Regulation, Government Intervention

- Peter did such a good job on this last week — CDA Section 230
- GDPR, European Community, “Right to be Forgotten”
- Are the big advertising/tech companies “neutral”?
- FTC & “Information Injuries”

Are Tech Companies Responsible?

- “You can’t go about telling your advertisers that you can target users down to the tiniest pixel, but then throw your hands up in front of the politicians and say your machines can’t figure out if bad actors are using your platform.”
- Former Google PR Head Jessica Powell

FTC “Informational Injury” (1/2)

- medical identity theft
- doxing
- disclosure of private information
- erosion of trust
- risk of injury must be balanced with the benefits that can come from information collection

Right to Remove (Paolo Cirio, CTSP, Nov 15)

https://right2remove.us/about/

FTC “Informational Injury” (2/2)

Introduction

On December 12, 2017, the FTC hosted a workshop in Washington, DC to discuss “informational injuries,” which are injuries—both market-based and non-market—that consumers may suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data. There were two main reasons the FTC convened this workshop. First, as then Acting Chairman Norman Kotchman noted, “in making policy determinations, injury matters...we need to understand consumer injury to weigh effectively the benefits of (government) intervention against its inevitable costs.” Second, in order to take law enforcement actions against “bad” acts or practices under the FTC Act, the FTC must demonstrate that the acts or practices “cause or are likely to cause substantial injury.” The workshop asked participants to discuss and develop novel frameworks to help guide future application of the “substantial injury” prong in cases involving informational injury.

Digital Privacy for Librarians (& Others)

- http://besser.tsoa.nyu.edu/howard/Talks/
- https://vimeo.com/libraryfreedominstitute
- https://libraryfreedomproject.org/lth/
- http://www.nyu.edu/tisch/preservation/research/privacy_in_libraries/abstract_narrative_2017.06.08.pdf
- https://chooseprivacyweek.org/
Topics for group discussion

- Library Freedom Institute (topics/content, pedagogy, speakers, delivery, ...)
- Tension-between preservation and privacy
- General digital privacy questions
- Policy issues