Online Privacy in the Library
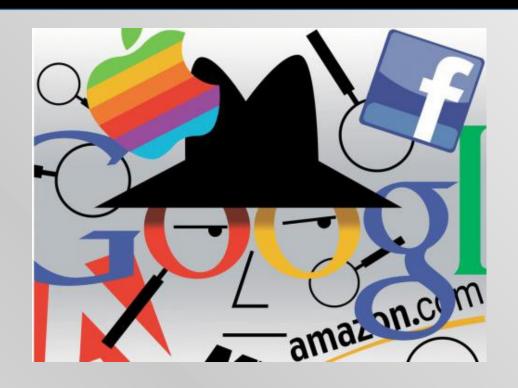
Mike Robinson

Chair, Intellectual Freedom Committee
Alaska Library Association
http://consortiumlibrary.org/blogs/mcrobinson/

Introduction

- Need for privacy
- Threats to privacy in the library
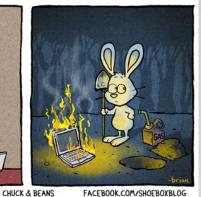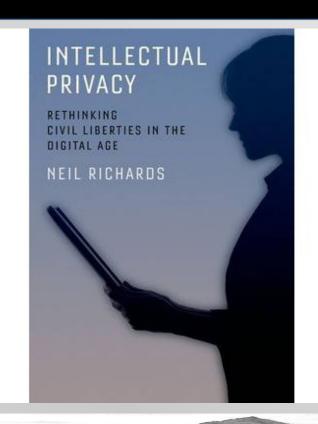- Safeguards
- Public awareness

Why Online Privacy?

- Safety & security
- Human diginity
- Intellectual freedom
- Constitutional & legal rights

Why Online Privacy?
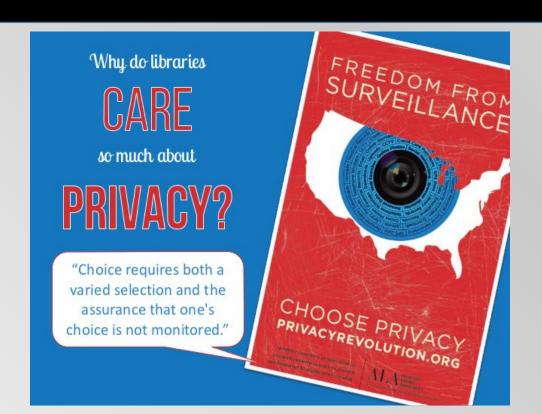
- 1st Admendment

- Free speech includes freedom to read

- Surveillence chills inquiry

INTELLECTUAL PRIVACY

RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE

NEIL RICHARDS

Why Online Privacy?

- ALA Library Bill of Rights
- Confidentiality of library records
- Opposition to Patriot Act
- Libraries as champions for privacy

Threats to Privacy

- Data sharing
- Data mining
- Data theft
- Surveillance

- Social media & the cloud
- Content personalization
- Activity tracking
- Email & http://
- Monitoring & filtering
- Wifi hotspots
- Malware & hacking
- Mobile apps & devices

Threats in the Library

- Public computers & networks

- Integrated library systems

- Library catalog & websites

- Ebooks & other econtent

Anything shared over the network is open to misinterpretation.

Your information footprint is larger than you think.

There is no anonymity on the Internet.

Sharing information over a network means you give up control over that information.

The Internet not only duplicates, it never forgets!

Over Exposed?

http://teachingprivacy.icsi.berkeley.edu

Identity is not guaranteed on the Internet.

Communication over a network, unless strongly encrypted, is never just between two parties.

Just because something can't be found today, doesn't mean it can't be found tomorrow.

You can't avoid having an information footprint by not going online.

Information about you on the Internet will be used by somebody in their interest - including against you.

Threats - Public Computer

- Access control software

- Display screens

- Web browsing

- Digital fingerprints

- Malware
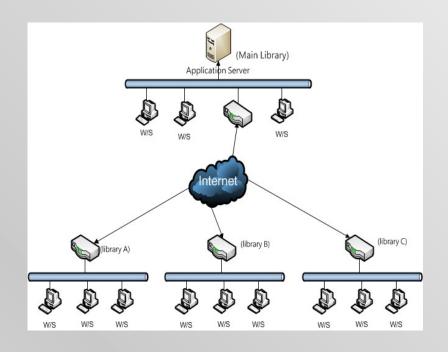
Threats - Networks

- Monitoring

- Content filters esp. those that break https

- Packet sniffers esp. wifi

- Weak wifi encryption

- Rogue wifi hotspots

Threats - ILS

- Over retention of user data

- Unencrypted data transmissions

- Notifications & reports

- Personally identifiable information & PINs

- Unencrypted backups

Threats - Catalog & Websites

- Lack of https

- Web analytics & logfiles

- Personalization

- Social - comments, ratings, recommendations, etc

- Embedded content & scripts

Threats - Ebooks & Econtent

- Lack of https

- Identity managment & DRM

- Vendor policies & practices about user data

- Sharing with 3rd parties

Safeguards for Privacy

July 2, 2001
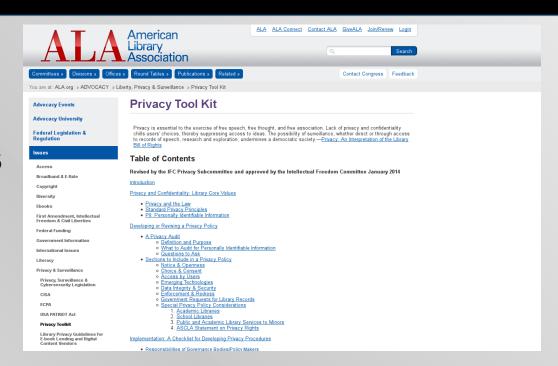
- Privacy audit

- Privacy policies

- Public computer & network

- Integrated library system

- Library catalog & website

- Vendor agreements & licenses

Safeguards – Privacy Audit

- Survey all technologies provided by the library

- Describe current practices

- Evaluate existing policies

- Make recommendations

http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy

Safeguards – Privacy Policies

- Guidance ALA, FIPP, state law
- Create privacy-specific polices
- Add privacy to existing policies
- Ways to inform users

FTC Fair Information Practice Principles (FIPP), May 2000
https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

Safeguards - Public Computer
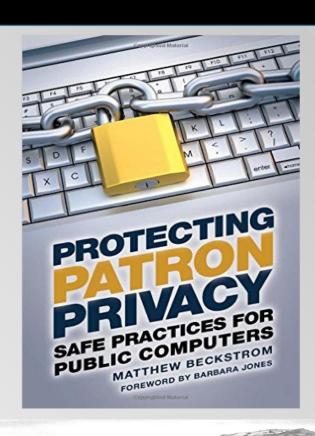
- Purge records of logins

- Anonymous access

- Privacy filters on screens

- Check out laptops, tablets

- Up-to-date software

- Erasure software

Safeguards - Public Computer
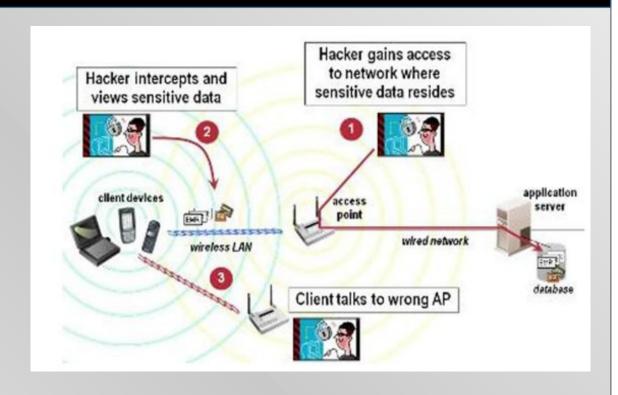
- Clear cache, cookies, history on browser exit

- Install extensions like Privacy Badger, Https Everywhere

- Set search to to Duck Duck Go, Start Page

- Tor Browser or TAILS OS for anonymous access

Safeguards - Networks

- Purge network access logs

- Don't break https with content filters

- Limit access to ethernet ports

- Zone network traffic for staff PCs, public PCs, wifi, etc

- Deploy wifi with proper encryption

- Monitor for rogue wifi hotspots

Safeguards - ILS

- Purge user data logs, encryt backups, purge old backups

- Use with SSL with staff clients, SIP, APIs, RFID when possible or use VPN

- Avoid sending sensitive information like book titles in clear-text email notifications

- Aggregate or anonmize personal user data in reports, control access to reports

- Avoid collecting unnecessary personal information like SSN

- If possible restrict acess to PIN and other sensitive information in staff client

- Train staff in handling sensitive information

Safeguards- Catalog/Websites

Let's Encrypt
Free SSL For All
🔒 https://www.yourdomain.com

https://letsencrypt.org/
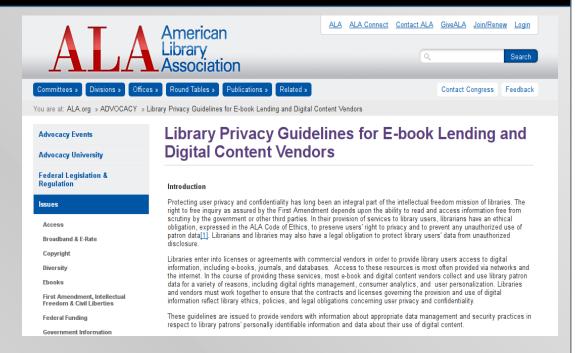
- Encrypt websites & catalogs

- Piwik alternative to Google Analytics

- Default to opt-in for personalization with ability to later opt-out

- Anonymous or authenticated users for social features?

- Vet embedded content & scripts, they often share data with 3rd parties

Safeguards – Ebooks/Econtent

- Libraries should make privacy a criteria when purchasing content

- Vendors should disclose their policies & practices around user data

- License agreements & contracts should address privacy issues

- Libraries should inform users of privacy implications when accessing online content

http://www.ala.org/advocacy/library-privacy-guidelines-e-book-lending-and-digital-content-vendors

Public Awareness

- Transparency
- Digital literacy
- Library programming

Awareness – Transparency

Sketch by Aimee Fifarek

- Online world full of threats to privacy

- Tradeoff between privacy and convenience

- Users should be able to make informed decisions

Awareness – Literacy

- People often feel powerless to protect their privacy

- Privacy should be part of any digital literacy training

- Librarians should become the privacy experts in their community

https://libraryfreedomproject.org/

Awareness – Programming

Choose Privacy Week #chooseprivacy

ALA American Library Association

HOME | OUR STORY » | RESOURCES » | MEDIA ROOM | BLOG | CONTACT US

Search this site…

Choose Privacy

Someone is watching your every move. Financial transactions, communications records, media consumption, social networking, and GPS locations are all tracked. But we can't often tell by whom.

Information should go both ways, or not at all.

Googled "Chapter 11" nine times in last year

Estimated life expectancy: 68

Has four different dating site profiles

29% of workday spent on Internet

Spends 1.5 hours on Facebook daily

Reading *Fifty Shades of Grey*

Owes $21,350 in credit card debt

Annual rent: $14,400

Insurance policy expires soon

https://chooseprivacyweek.org/

- People are concerned about online privacy
- Great topic for civic engagement
- Libraries can provide leadership

Online Privacy in the Library

Mike Robinson

Chair, Intellectual Freedom Committee
Alaska Library Association
http://consortiumlibrary.org/blogs/mcrobinson/