



NAVIGATING THE CHANGING LANDSCAPE OF LIBRARY PRIVACY

Deborah Caldwell-Stone
American Library Association
Michael Robinson
University of Alaska, Anchorage

Intellectual Privacy



Why is privacy so important in libraries?



“The library, as the **unique sanctuary of the widest possible spectrum of ideas**, must protect the confidentiality of its records in order to insure its readers' right to read anything they wish, free from the fear that someone might see what they read and use this as a way to intimidate them...”

Student accused of being a terrorist for reading book on terrorism

Staffordshire University apologises after counter-terrorism student Mohammed Umar Farooq was questioned under Prevent anti-extremism initiative



📷 Mohammed Umar Farooq was enrolled in a master's course on terrorism, crime and global security. Photograph: David Sillitoe for the Guardian

A postgraduate student of counter-terrorism was falsely accused of being a terrorist after an official at [Staffordshire University](#) had spotted him reading a textbook entitled Terrorism Studies in the college library.



...Without such protection there would be a chilling effect on our library users, as inquiring minds turn away from exploring varied avenues of thought because they fear the potentiality of others knowing their reading history.

-- Supporting documentation for 1981 passage of New York State statute CPLR §4509

“We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.”

ALA Code of Ethics

“Librarians and other information workers respect personal privacy, and the protection of personal data, necessarily shared between individuals and institutions. The relationship between the library and the user is one of confidentiality and librarians and other information workers will take appropriate measures to ensure that user data is not shared beyond the original transaction.”

IFLA Code of Ethics

In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others.

Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

Privacy: An Interpretation of the Library Bill of Rights

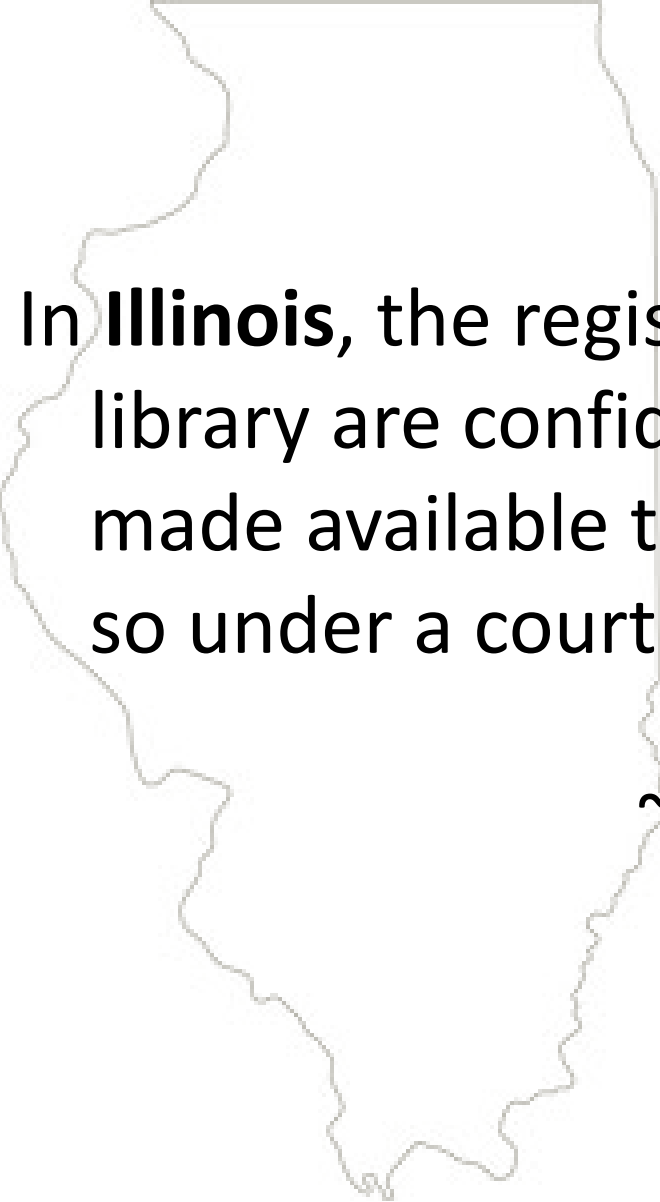
Library users should have the right to personal privacy and anonymity. Librarians and other library staff should not disclose the identity of users or the materials they use to a third party.

IFLA Statement on Libraries and Intellectual Freedom

Laws

- First Amendment
- Fourth Amendment
- Court Opinions
 - FISA/USA Freedom Act/Gov't Surveillance
 - Search warrants, subpoenas
 - State Library Confidentiality Laws
 - State Reader Privacy Laws
 - FOIA/Open Records Laws (Data Management)

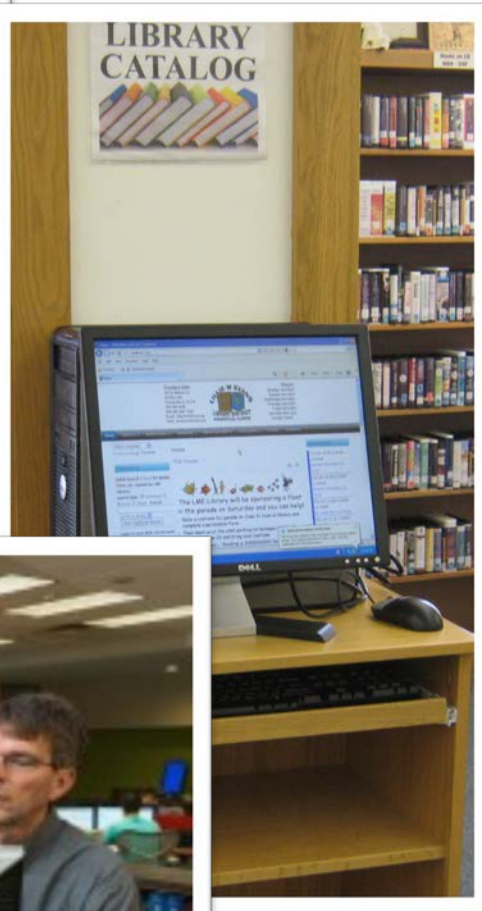
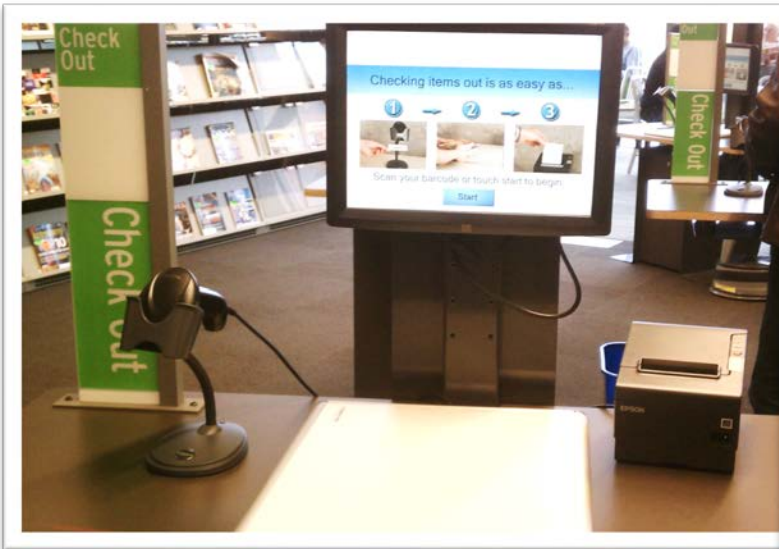
Laws



In **Illinois**, the registration and circulation records of a library are confidential information and cannot be made available to the public unless required to do so under a court order.

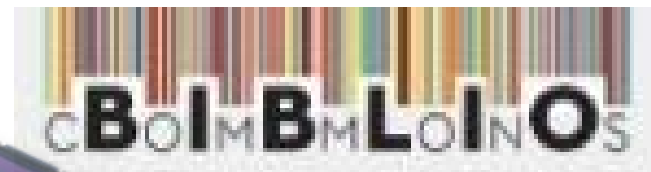
~~IL Rev. Statutes 75 ILCS 70/1 et al.





And more...





Adobe Digital Editions



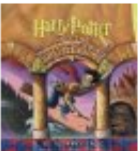








The Library as Source of Patron Data



Adobe is Spying on Users, Collecting Data on Their eBook Libraries

🕒 6 October, 2014 📁 Adobe, Privacy, Security, Security Breach, Spying 📍 adobe, collecting, data, ebook, libraries, spying, users 👤 Nate Hoffelder

3 Item(s) Checked Out

	Title	Call No.	Due	Renew	Fines	Links
	Harry Potter and the sorcerer's stone Rowling, J. K.	PZ7.R79835 Har 1999ab	05/01/2011	<input type="checkbox"/> Renew (2 of 2 renewals remaining)	No	Share  TWEET THIS 
	Picture perfect Picoult, Jodi,	PS3566.I372 P49 2002	05/01/2011	<input type="checkbox"/> Renew (2 of 2 renewals remaining)	No	Share  TWEET THIS 
	Harry Potter and the sorcerer's stone Rowling, J. K.	PZ7.R79835 Har 1998	05/01/2011	<input type="checkbox"/> Renew (2 of 2 renewals remaining)	No	Share  TWEET THIS 

Unauthorized or Inadvertent Disclosure of Patron Data

Patron Profiles

Understand your community on a household level

The Patron Profiles app available through Analytics On Demand explains who your customers are (and aren't) so you can make data-driven decisions and drive meaningful outcomes.

Improve on ROI and plan for the future

Large corporate, governmental, and non-profit organizations use "big data" to their advantage. Public libraries, big or small, can also find value in embracing a data-driven approach. You too can better understand the communities you serve and leverage analysis to help define and accomplish your library's goals.

Actionable insights from Analytics On Demand will lead to better outcomes:

- **Understanding patrons**—Embrace a human-centric approach with real household data from your community.
- **Administrative decision making**—Provide services and allocate resources to increase your library's impact on diverse user groups and populations.
- **Strategic planning**—Continuous access to usable data allows libraries to modify plans, based on discoveries throughout the process.
- **Performance measurement**—Refresh data as often as needed to understand the impact of your data-driven decisions.

Eye-opening customer insights

Patron Profiles reports include:

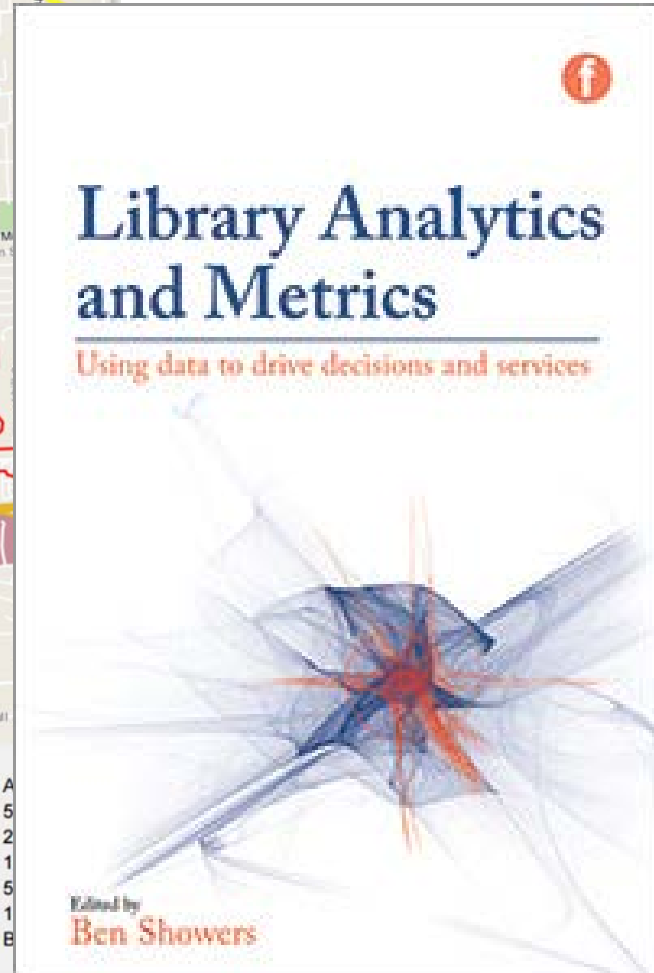
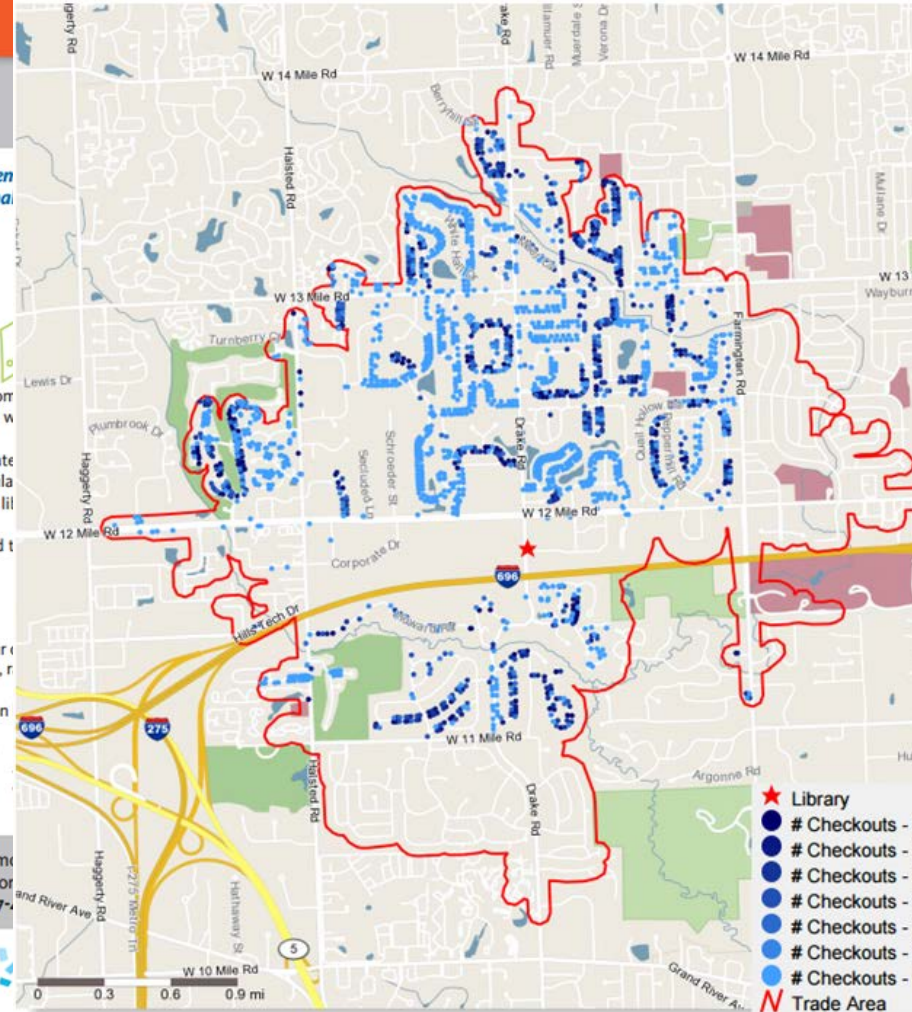
- **Demographic overview**—Change happens over time. See your library activity aligned with demographics like population, age, race, and lifestyles by household.
- **Patron analysis demographics**—View library activity based on household composition, length of residency, behaviors, and interests.
- **Mosaic profiles**—Learn who your users are and find more like them using this well-known household-based segmentation system from Experian, which classifies all U.S. households and neighborhoods in 71 unique Mosaic types and 19 groupings.



Visit www.gale.com/forpl to learn more about the pricing information and customizable options: 1-800-877-7423

An education-focused library deserves an education-focused partner.

Library Patron Households by Checkout Volume



The Library as User and Collector of Data

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin, *Privacy and Freedom* (1967)

Data Privacy/Data Breach Laws

- Video Privacy Protection Act
- Child Online Privacy Protection Act
- Student Data Privacy
- Biometric Privacy
- Broadband Privacy
- Locational Privacy
- Data Breach Reporting

Privacy in Today's Library

Confidentiality

Freedom from surveillance

+ Limits on Information Collection & Use

+ Personal choice and control

+ Robust Network and Data Security

Five Steps To Better Digital Privacy in the Library

1. Update your library's policies, practices and standards to assure patron privacy

- New standards: NISO Consensus Principles on Users' Digital Privacy
- ALA Library Privacy Guidelines / Checklists
- Privacy Audits (Storage, Use, Data Flows)
- Records Management Plan (Schedule for Retention / Destruction)

Five Steps To Better Digital Privacy in the Library

1. Update your library's policies, practices and standards to assure patron privacy
2. Employ Encryption Technologies

Five Steps To Better Digital Privacy in the Library

1. Update your library's policies, practices and standards to assure patron privacy
2. Employ Encryption Technologies
3. Require vendors to adhere to the same privacy and record retention standards used by the library.

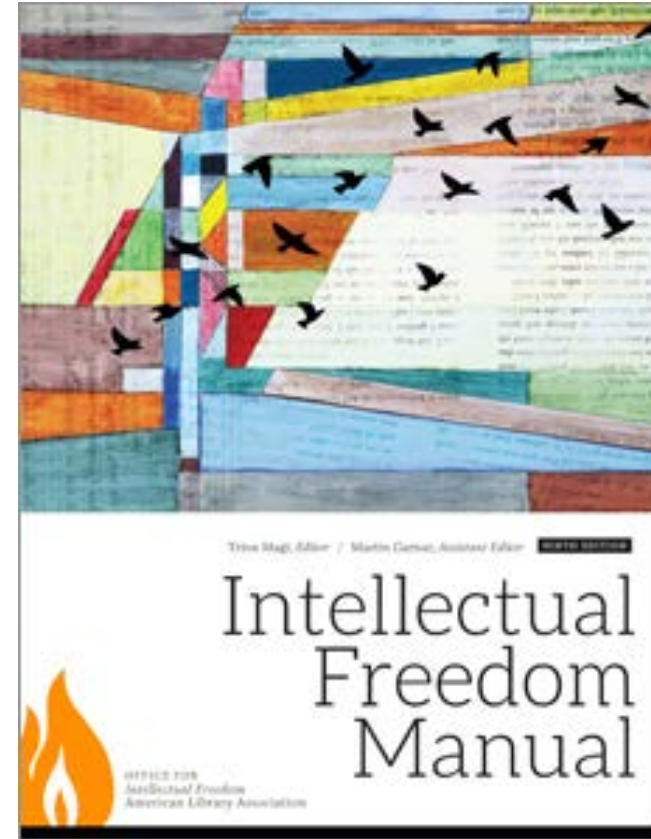
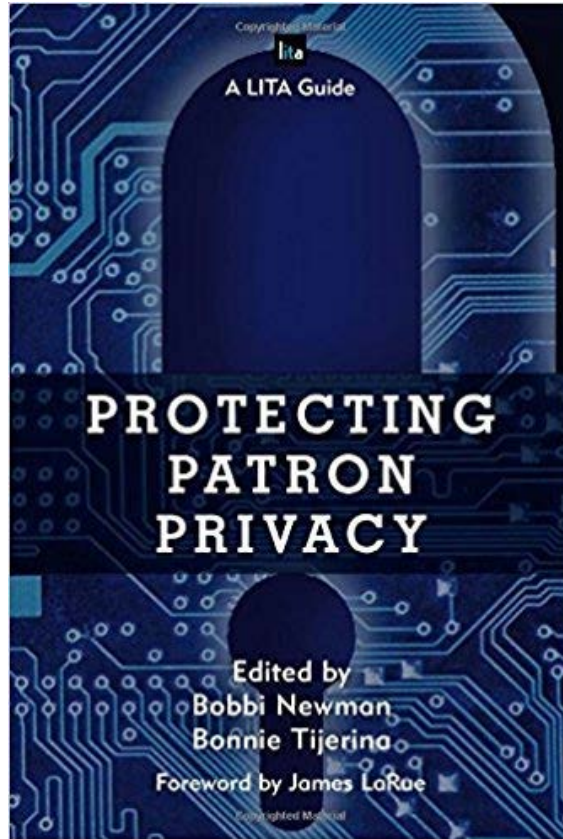
Five Steps To Better Digital Privacy in the Library

1. Update your library's policies, practices and standards to assure patron privacy
2. Employ Encryption Technologies
3. Require vendors to adhere to the same privacy and record retention standards used by the library.
4. Add Encryption and Privacy Tools to Public Computers

Five Steps To Better Digital Privacy in the Library

1. Update your library's policies, practices and standards to assure patron privacy
2. Employ Encryption Technologies
3. Require vendors to adhere to the same privacy and record retention standards used by the library.
4. Add Encryption and Privacy Tools to Public Computers
5. Train library staff and library users about privacy rights and best practices online and off that preserve the privacy and confidentiality of sensitive information

Resources on law, ethics, policy, and practice:



Questions?

Let's Get Practical

- Resources for Libraries
- Digital Content Providers
- Integrated Library System
- HTTPS & Let's Encrypt
- Tools to Protect Web Users



Library Privacy Resources



Choose Privacy Week



HOME WHY PRIVACY? **RESOURCES »** PROGRAMS » BLOG CONTACT US »

Search this site...

RESOURCES

Educate yourself on how libraries can protect the privacy of online users.

Librarians and library workers can be the privacy experts in their communities.

[Tools to Protect User Privacy](#)

Technologies and practices users can employ to protect their online privacy.

[Guidelines & Checklists for Libraries](#)

Privacy guidelines, checklists, and other resources to assist librarians, libraries, schools and vendors develop best practices for online privacy.

[Sample Policies & Documents](#)

Samples of privacy policies and other documents to give you ideas on how to get started.

[HTTPS & Let's Encrypt](#)

Resources on using HTTPS and Let's Encrypt on library websites and servers.

[Students & Minors](#)

Selected resources on students' and minors' privacy including federal laws, scholarly articles, standards and principles, news and viewpoints, and legislative outlook.

[Presentations & Webinars](#)

Recent presentations and webinars on privacy and libraries.

IN THIS SECTION

Resources

[Tools to Protect User Privacy](#)

[Guidelines & Checklists for Libraries](#)

[Sample Policies & Documents](#)

[HTTPS & Let's Encrypt](#)

[Students & Minors](#)

[Presentations & Webinars](#)

<https://chooseprivacyweek.org/resources/>

Library Privacy Guidelines

- Published by ALA Intellectual Freedom Committee
- Help libraries develop best practices
- Balance user privacy vs operational needs
- Empower user to make decisions



[f](#) [t](#) [RSS](#)

Choose Privacy Week

ALA American Library Association

HOME WHY PRIVACY? RESOURCES » PROGRAMS » BLOG CONTACT US »

Search this site...

GUIDELINES & CHECKLISTS FOR LIBRARIES

Library Privacy Guidelines

The ALA Intellectual Freedom Committee approved a set of privacy guidelines that are intended to assist librarians, libraries, schools and vendors to develop best practices for online privacy and data management and security. The guidelines currently include:

- ▶ [Guidelines for Data Exchange Between Networked Devices and Services](#)
- ▶ [Guidelines for E-book Lending and Digital Content Vendors](#)
- ▶ [Guidelines for Library Management Systems](#)
- ▶ [Guidelines for Library Websites, OPACs, and Discovery Services](#)
- ▶ [Guidelines for Public Access Computers and Networks](#)
- ▶ [Guidelines for Students in K-12 Schools](#)

These guidelines attempt to balance the need to protect reader privacy with the needs of libraries to collect user data and provide personalized services, while respecting and protecting the individual's right to make their own informed decisions in regards to how much privacy they are willing to trade for convenience or added benefits.

The ALA Intellectual Freedom Committee also approved guidelines to minimize the negative impact of content filters on intellectual freedom, including a section on privacy issues such as SSL decryption.

- ▶ [Guidelines to Minimize the Negative Effects of Internet Content Filters on Intellectual Freedom](#)

Library Privacy Checklists

The Library and Information Technology Association (LITA) partnered with the ALA Intellectual Freedom Committee to develop checklists that are intended to provide libraries of all types with practical guidance on implementing the Library Privacy Guidelines published by the Intellectual Freedom Committee. The checklists currently include:

IN THIS SECTION

Resources

Tools to Protect User Privacy

Guidelines & Checklists for Libraries

- Library Privacy Guidelines for Data Exchange Between Networked Devices and Services
- Library Privacy Guidelines for E-book Lending and Digital Content Vendors
- Library Privacy Guidelines for Library Management Systems
- Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services
- Library Privacy Guidelines for Public Access Computers and Networks
- Library Privacy Guidelines for Students in K-12 Schools
- Guidelines to Minimize the Negative Effects of Internet Content Filters on Intellectual Freedom
- Library Privacy Checklist Overview
- Library Privacy Checklist for Data Exchange Between Networked Devices and Services
- Library Privacy Checklist for E-book Lending and Digital Content Vendors

Library Privacy Guidelines

LIBRARY PRIVACY GUIDELINES FOR E-BOOK LENDING AND DIGITAL CONTENT VENDORS

Introduction

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users' right to privacy and to prevent any unauthorized use of patron data[1]. Librarians and libraries may also have a legal obligation to protect library users' data from unauthorized disclosure.

Libraries enter into licenses or agreements with commercial vendors in order to provide library users access to digital information, including e-books, journals, and databases. Access to these resources is most often provided via networks and the internet. In the course of providing these services, most e-book and digital content vendors collect and use library patron data for a variety of reasons, including digital rights management, consumer analytics, and user personalization. Libraries and vendors must work together to ensure that the contracts and licenses governing the provision and use of digital information reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide vendors with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their use of digital content.

Agreements, Ownership of User Data, and Legal Requirements

Agreements between libraries and vendors should address appropriate restrictions on the use, aggregation, retention, and dissemination of patron data, particularly information about minors. Agreements between libraries and vendors should also specify that libraries retain ownership of all data and that the vendor agrees to observe the library's privacy policies and data retention and security policies.

- E-book Lending & Digital Content Vendors
- Library Management Systems
- Library Websites, OPACs & Discovery Services
- Public Access Computers & Networks
- Data Exchange Between Networked Devices & Services
- Students in K-12 Schools

Bonus Guideline - Filtering

- Published by ALA IFC
- How to make filters less sucky
- Includes section on privacy & SSL decryption

GUIDELINES TO MINIMIZE THE NEGATIVE EFFECTS OF INTERNET CONTENT FILTERS ON INTELLECTUAL FREEDOM

Introduction

For a variety of reasons, many public libraries and schools install content filters on the Internet access they provide to their patrons and students. A library may decide to filter in response to community standards or to comply with state filtering legislation in order to receive funding. A governing authority such as a school district or local government may also require a library under its jurisdiction to filter. Libraries that receive federal E-rate funds for Internet access or in-building network enhancements must also comply with the filtering and other requirements of the Children's Internet Protection Act (CIPA).

Whatever the reasons, many libraries must deal with the well-documented negative effects of content filters on intellectual freedom. Filters often block adults and minors from access to a wide range of vital information and forms of expression that are constitutionally protected speech. CIPA requires only a narrow category of speech to be blocked: visual images that are obscene, child pornography, or visual images that are deemed "harmful to minors" under the law. Filtering technology is not sophisticated enough to make such narrow distinctions, and as a result both over filtering and under filtering occurs in the attempt to block images that meet these criteria.

Filters also threaten the privacy of users by monitoring and logging Internet activity. As more websites move to HTTPS to secure communications from eavesdropping, this presents a challenge for filters that employ content inspection techniques. Some filters now include the ability to decrypt HTTPS protocols and can thereby monitor and log user activities on secure websites. Implementation of these capabilities is not required under legislation like CIPA, nor is it consistent with the mission and values of libraries.

These guidelines are issued to provide public and school libraries with information about how to select, configure, manage, and assess content filters to minimize the negative effects on free inquiry and the privacy of library users.

Selection

Library staff, who have an ethical obligation to protect intellectual freedom, and information technology (IT) staff, who typically must install and support the product, should work collaboratively to select filtering software.

Library Privacy Checklists

LIBRARY PRIVACY CHECKLIST FOR E-BOOK LENDING AND DIGITAL CONTENT VENDORS

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the [Library Privacy Guidelines for E-book Lending and Digital Content Vendors](#).

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Provide links to vendor privacy policies and terms of service pages for users when appropriate, e.g. from the library's own privacy policy page or from a library web page about the vendor's product or service.
2. Work with vendors to configure services to use the opt-in method whenever possible for features that involve the collection of personal information.
3. Develop a strategy to assist patrons in managing their privacy when using vendor products and services. The strategy could include in-person reference, handouts, web guides, classes, or other programming. Topics covered could include:
 1. Settings for personal accounts on vendor websites.
 2. Vendor applications on personal devices including any privacy settings and how to remove the application and any associated stored data.
4. Notify staff and patrons of any data breaches and assist patrons in mitigating the impact (changing passwords, uninstalling applications, etc).

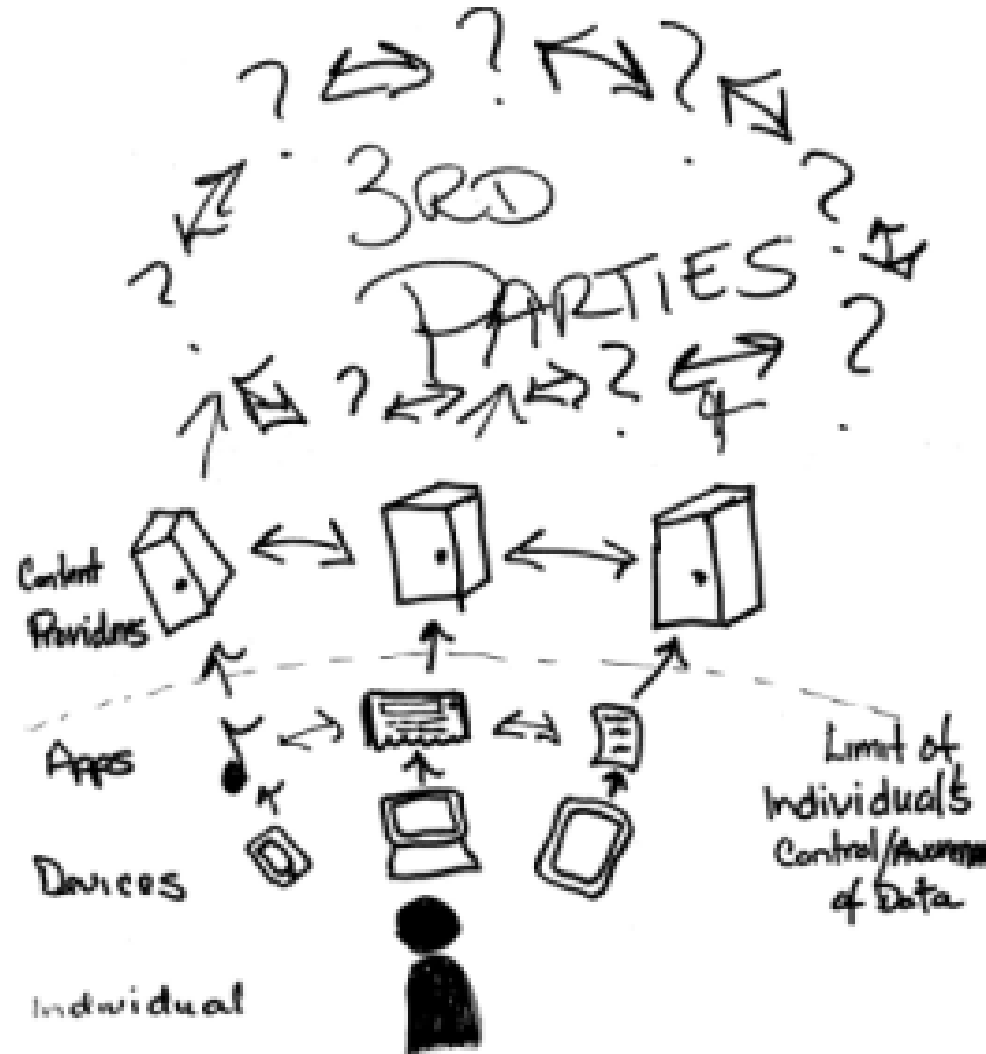
Priority 2 Actions

1. Add privacy considerations to the library's selection criteria for new purchases or the renewal of existing purchases. These considerations should include the vendor:
 1. Notifying users of their privacy policies at the point of access and restricting the collection of patron data to clearly stated operational purposes.
 2. Seeking patron consent for data collection by using the opt-in method whenever possible

- Published by ALA IFC & LITA
- Checklist for each privacy guideline
- Practical actions libraries can take
- Organized into priority 1, 2 & 3

Questions?

Content Providers Checklist



Content Providers - Priority 1

- Library should link to vendor privacy policies
- Work with providers to configure services to use opt-in method
- Help patrons manage their privacy settings
- Notify patrons of any data breaches

Content Providers – Priority 2

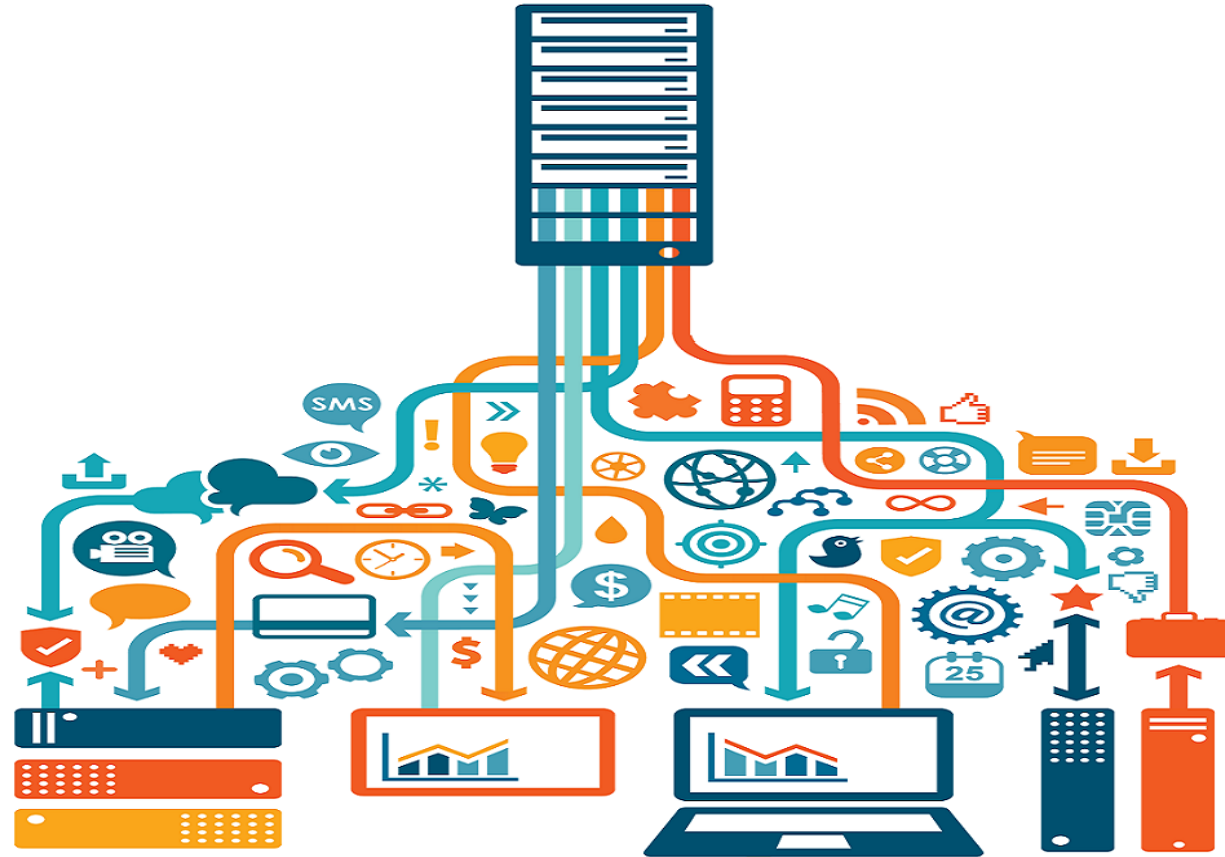
- Add Privacy Considerations to Section Criteria
 - Provider has a published privacy policy
 - Supports opt-in method
 - Users can access & review personal data
 - HTTPS / encryption for data communications
- License Agreements with New Content Providers
 - Conform to state confidentiality laws
 - Conform to library privacy policies
 - Stipulate that library retains ownership of user data
 - Include protocol for law enforcement requests
 - Include protocol for notification of data breaches

Content Providers – Priority 3

- Review Existing License Agreements
 - Work with providers to address privacy concerns
 - Consider not renewing agreements that can not address concerns
- Review vendor's data governance plan
 - If vendor has no plan, ask them to create one
- Ask vendor to conduct regular privacy audits
 - and share the results with the library

Questions?

ILS Checklist



ILS – Priority 1

- Develop a privacy policy & publish it on library website
- Only collect & store patron information needed for library operations
- Aggregate or anonymize reports to remove personally identifiable information
- Configure ILS by default to remove transactional data when item is returned
 - Allow patrons to opt-in to check history if available
- Develop library procedures for handling government & law enforcement requests for patron information

ILS – Priority 2

- Restrict access to patron records to staff members with a demonstrated need
- Configure library notices to send minimal personal information
- Develop policies & procedures regarding the extraction & sharing of patron data
 - Restrict access to extracts to appropriate parties
 - Policy should include disposal/deletion of extracts
- Encrypt offline data backups
- Keep ILS application & server software up-to-date

ILS – Priority 3

- Store all passwords (patron and staff) in a secure fashion using proper cryptograph
- Encrypt all traffic between ILS server & any client connections outside a secure LAN
- Conduct security audits of ILS server & network
- Create procedures to handle data breaches & mitigate their impact on patrons

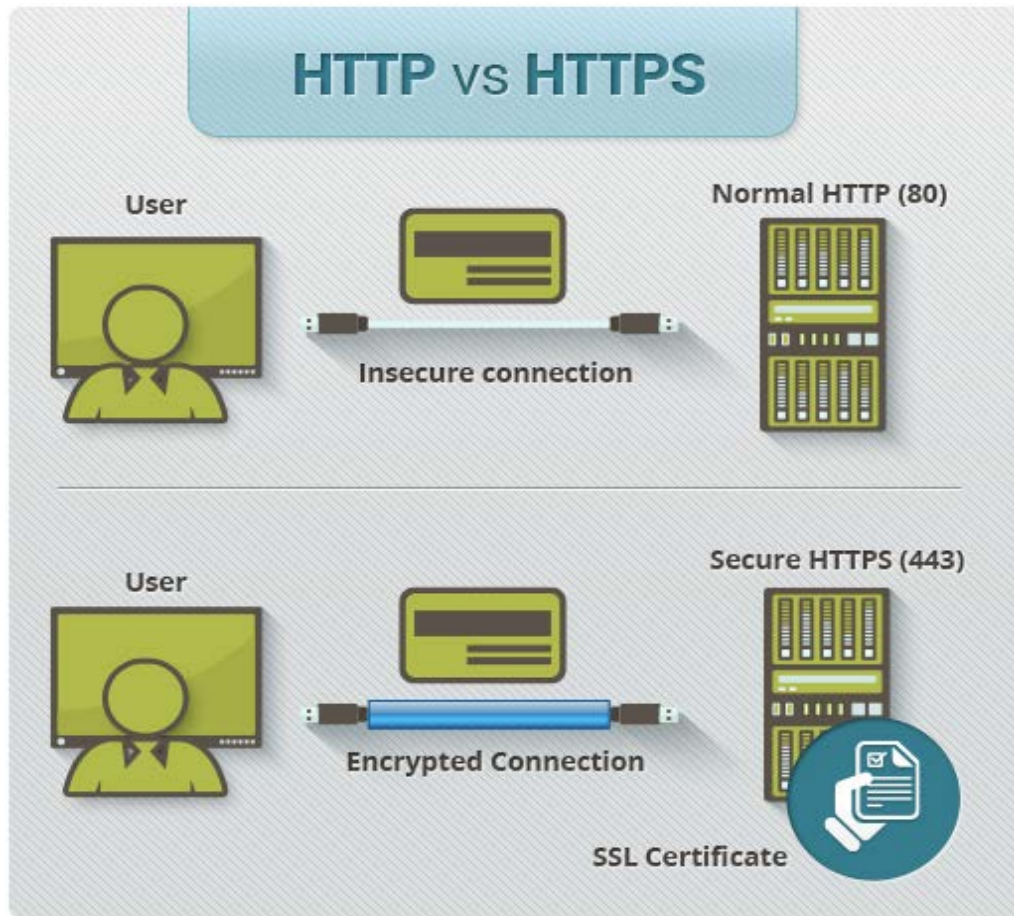
Questions?

HTTPS & Let's Encrypt

- Why HTTPS?
- Encrypt the Web Movement
- Free & Easy HTTPS with Let's Encrypt



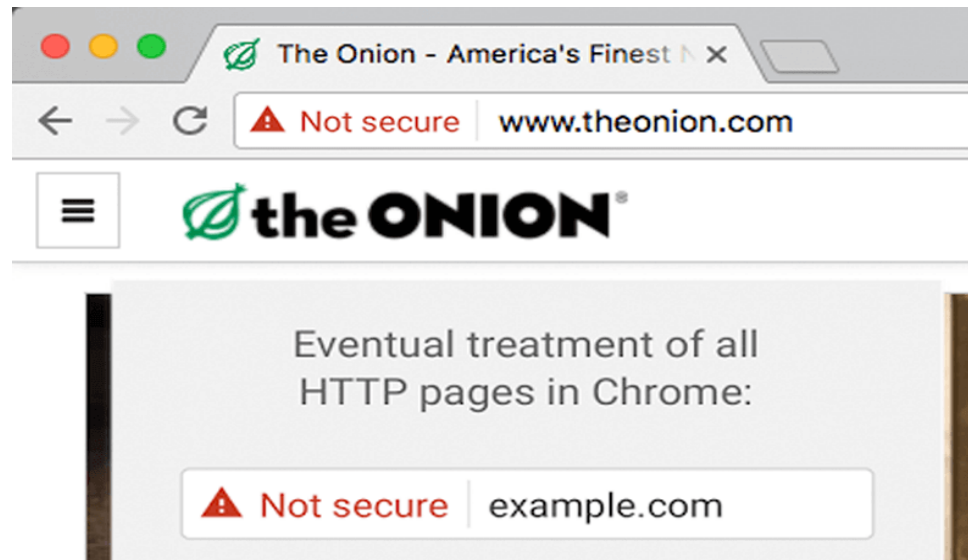
Why HTTPS?



- HTTP transmits content in the clear allowing potential eavesdropping
- HTTPS transmits content in encrypted tunnel that prevents eavesdropping
 - Thus helping protect reader privacy

Encrypt the Web Movement

- Electronic Frontier Foundation launches [Encrypting the Web](#)
- Federal government sites are required to be HTTPS
- Google boosts ranking of HTTPS sites in search results
- Firefox & Chrome begin to warn that HTTP sites are insecure
- [Secure the News](#) project to move news sites to HTTPS
- [Library Digital Privacy Pledge](#) encourages libraries & content providers to adopt HTTPS



Free & Easy HTTPS



- Let's Encrypt certificate authority
- Free certificates
- Tools for easy installation & renewal
- Free + easy = no excuses

Let's Encrypt - Sponsors

Platinum



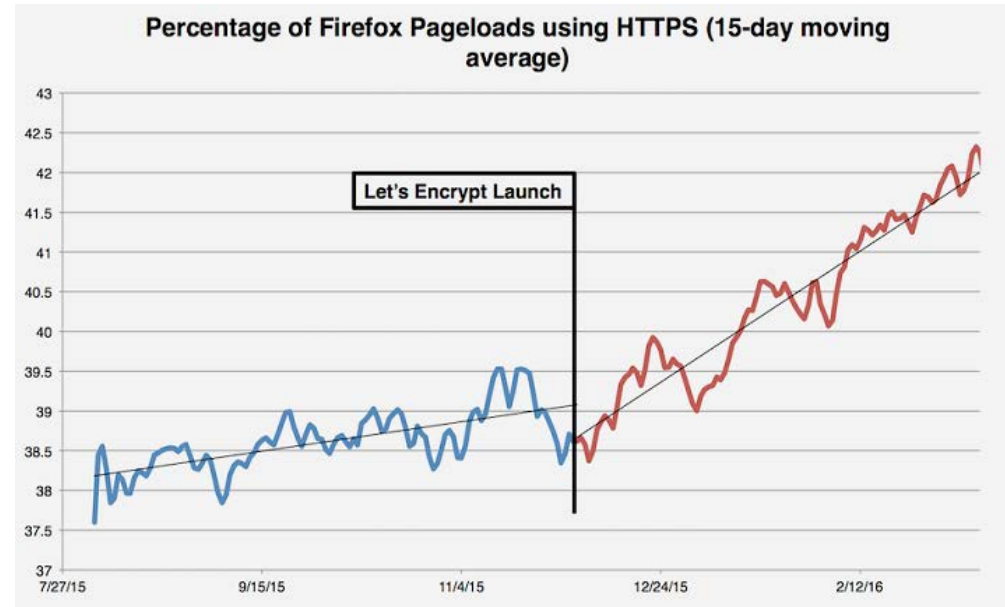
Gold



Silver



Let's Encrypt - Adoption



- **Rapid adoption** since debut in Nov 2015
- Jan 2016 248,000 certificates
- Jan 2017 28 million certificates
- 50% of web is now HTTPS

Let's Encrypt - Tools

System administrators can usually install certificates by using the [Certbot](#) client in a matter of minutes on web servers running up-to-date operating systems. In addition, Let's Encrypt has been integrated into over a hundred [web hosting platforms](#) so that



certificates can be installed by customers from their control panel with just the click of a button.

Let's Encrypt Cookbook for Library Servers

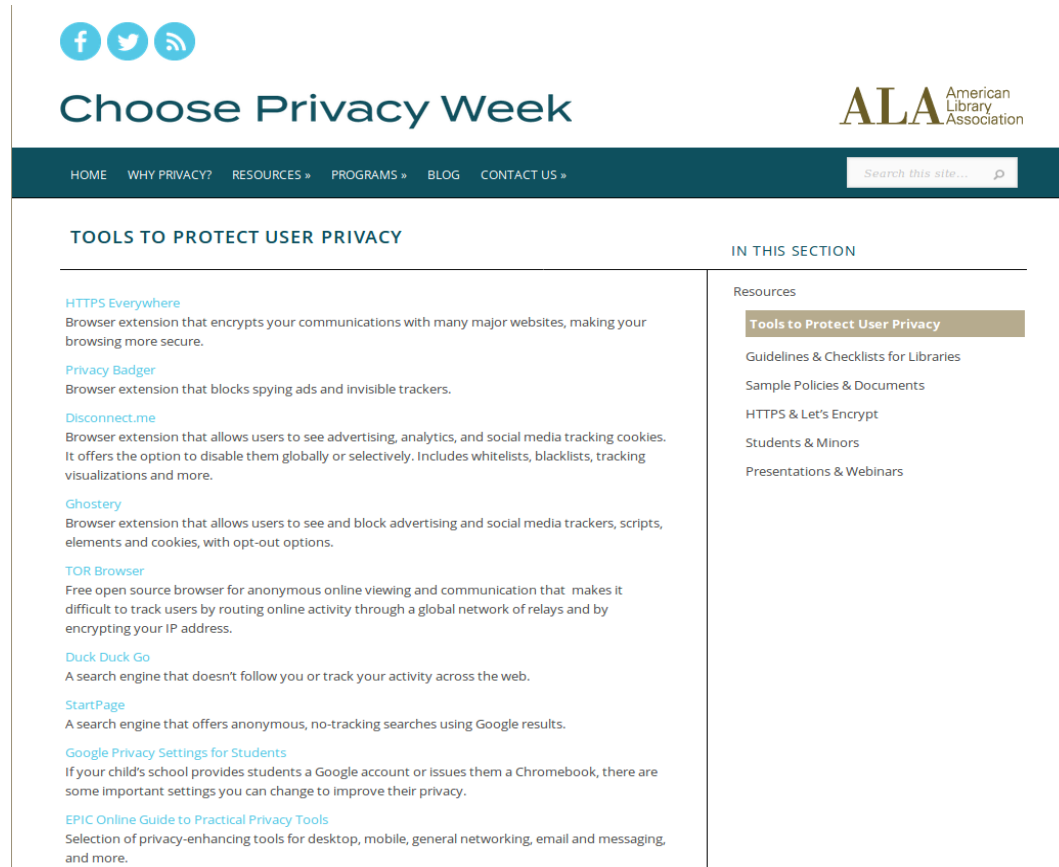
Here is a series of recipes for using Let's Encrypt to install certificates on a variety of library servers.

- ▶ [Apache Web Server on CentOS 6](#)
- ▶ [IIS Web Server on Windows 2008](#)
- ▶ [Standalone EZproxy Server on CentOS 6](#)
- ▶ [Library OPAC Server - SirsiDynix Enterprise on Tomcat CentOS 5](#)
- ▶ [API Server - SirsiDynix Web Services on Tomcat CentOS 6](#)

<https://chooseprivacyweek.org/resources/https-lets-encrypt/>

Questions?

Tools to Protect User Privacy



The screenshot shows the 'Tools to Protect User Privacy' page on the Choose Privacy Week website. The page features a dark teal header with navigation links and a search bar. The main content is divided into two columns: 'TOOLS TO PROTECT USER PRIVACY' and 'IN THIS SECTION'. The left column lists various tools with brief descriptions, while the right column lists related resources.

[f](#) [t](#) [r](#)

Choose Privacy Week

ALA American Library Association

HOME WHY PRIVACY? RESOURCES » PROGRAMS » BLOG CONTACT US »

Search this site...

TOOLS TO PROTECT USER PRIVACY

[HTTPS Everywhere](#)
Browser extension that encrypts your communications with many major websites, making your browsing more secure.

[Privacy Badger](#)
Browser extension that blocks spying ads and invisible trackers.

[Disconnect.me](#)
Browser extension that allows users to see advertising, analytics, and social media tracking cookies. It offers the option to disable them globally or selectively. Includes whitelists, blacklists, tracking visualizations and more.

[Ghostery](#)
Browser extension that allows users to see and block advertising and social media trackers, scripts, elements and cookies, with opt-out options.

[TOR Browser](#)
Free open source browser for anonymous online viewing and communication that makes it difficult to track users by routing online activity through a global network of relays and by encrypting your IP address.

[Duck Duck Go](#)
A search engine that doesn't follow you or track your activity across the web.

[StartPage](#)
A search engine that offers anonymous, no-tracking searches using Google results.

[Google Privacy Settings for Students](#)
If your child's school provides students a Google account or issues them a Chromebook, there are some important settings you can change to improve their privacy.

[EPIC Online Guide to Practical Privacy Tools](#)
Selection of privacy-enhancing tools for desktop, mobile, general networking, email and messaging, and more.

IN THIS SECTION

Resources

[Tools to Protect User Privacy](#)

[Guidelines & Checklists for Libraries](#)

[Sample Policies & Documents](#)

[HTTPS & Let's Encrypt](#)

[Students & Minors](#)

[Presentations & Webinars](#)

<https://chooseprivacyweek.org/resources/tools-to-protect-user-privacy/>

Privacy in Web Browsing

- Threats to privacy
- Browser best practices
- Browser extensions
- VPNs
- Tor browser



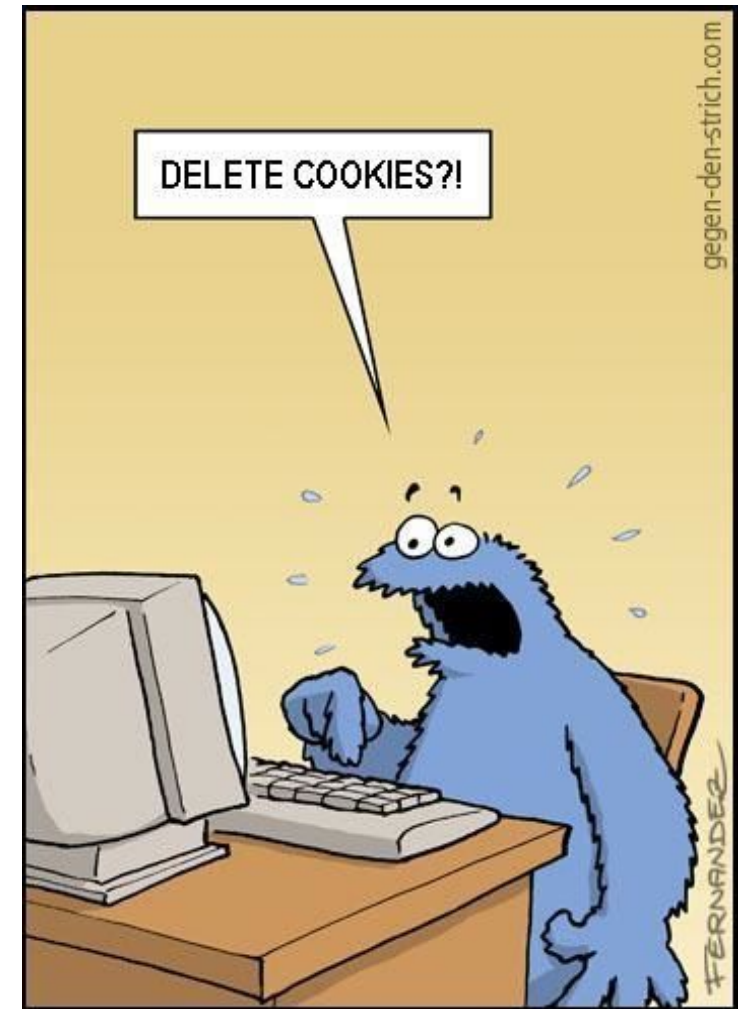
Threats to Browsing Privacy



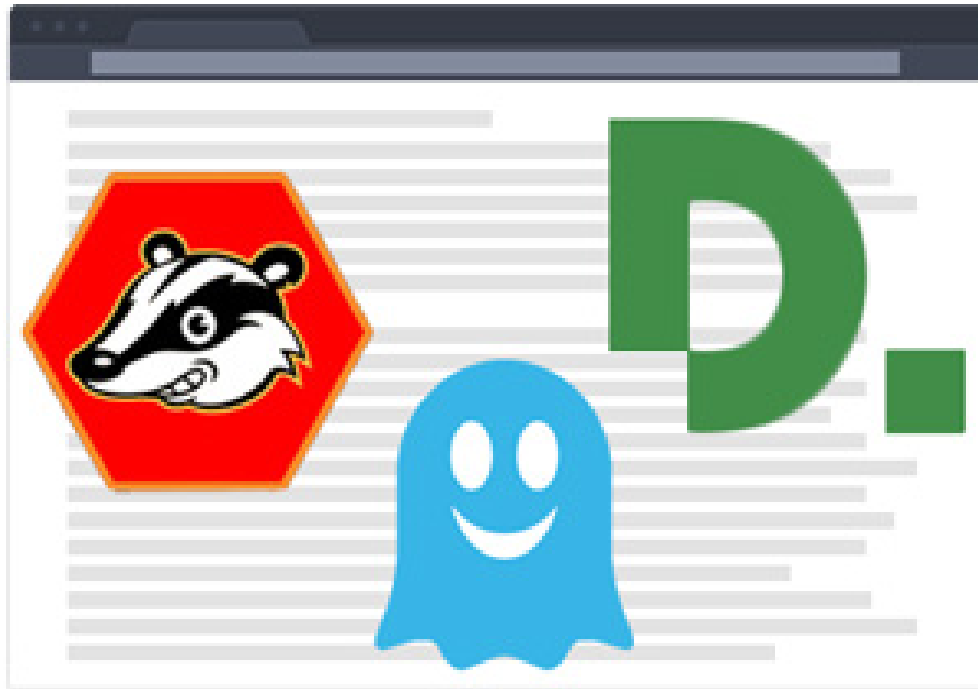
- Websites
 - Activity tracking
 - Fingerprinting
 - Cross-site scripting
- Network Monitoring
 - Work
 - School
 - ISP
- Open Wi-Fi

Browser Best Practices

- Use current browsers
- Use privacy mode
- Frequently delete cache, cookies, etc.
- Alternative Search Engines
 - [DuckDuckGo](#)
 - [StartPage](#)
- Use multiple browsers
 - one for anonymous surfing
 - 2nd for personalized/login
 - 3rd for banking/financial



Browser Extensions



- [HTTPS Everywhere](#)
 - Encrypts communications with many major websites
- [Privacy Badger](#)
 - Blocks spying ads & invisible trackers
- [Disconnect.me](#) / [Ghostery](#)
 - Visualize & block advertising, analytics & social media trackers.

VPNs

How a VPN Protects Your Data



All traffic is visible by your ISP



Which makes them happy.



Without a VPN

- ✗ DATA THAT IS NOT SENT VIA HTTPS IS NOT SECURE
- ✗ YOUR IP ADDRESS IS VISIBLE TO ALL WEBSITES YOU VISIT
- ✗ DATA IS NOT ENCRYPTED AND IS LOGGED BY YOUR ISP

KEY

- 😊 Happy ISP Capturing Your Data
- 😞 Sad ISP That Cannot Capture Your Data
- 🌐 The world wide web
- 💻 Your beautiful computer
- 🗄️ A mighty fine VPN server



All traffic is routed through your VPN



Which makes you happy!

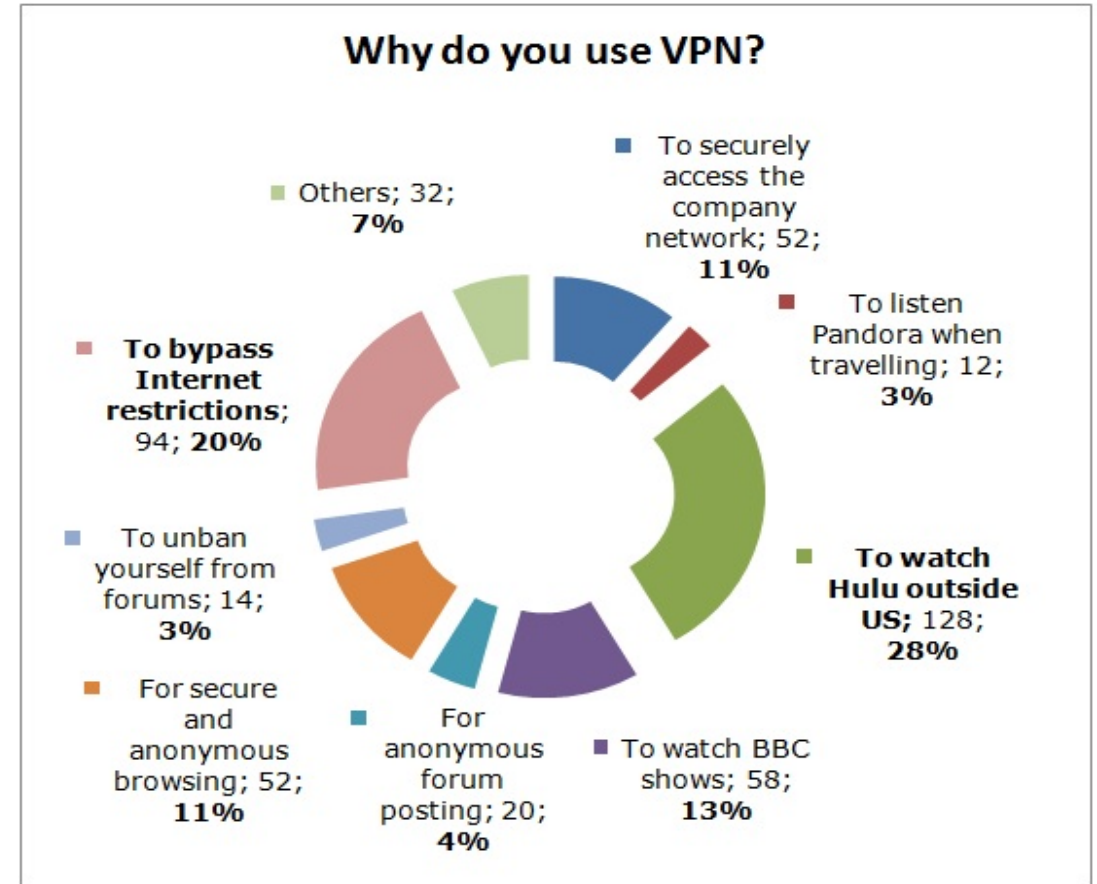


With a VPN

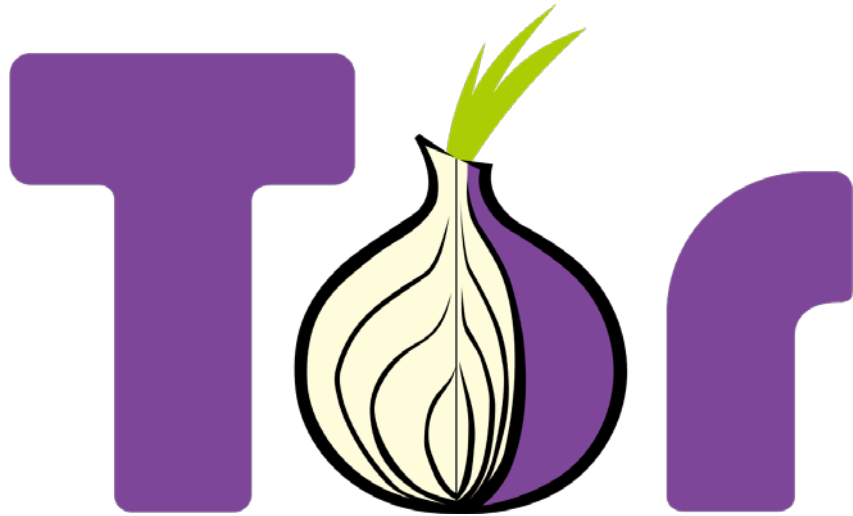
- ✓ DATA IS ENCRYPTED TO THE VPN SERVER
- ✓ YOUR IP CHANGES TO THE ONE GIVEN BY YOUR VPN
- ✓ ALL DATA IS ENCRYPTED AND CANNOT BE LOGGED

VPNs

- Protects from network monitoring by ISP, work, school
- Provides some browsing anonymity
- Not just browser, covers other apps
- Not all VPNs created equal, be selective



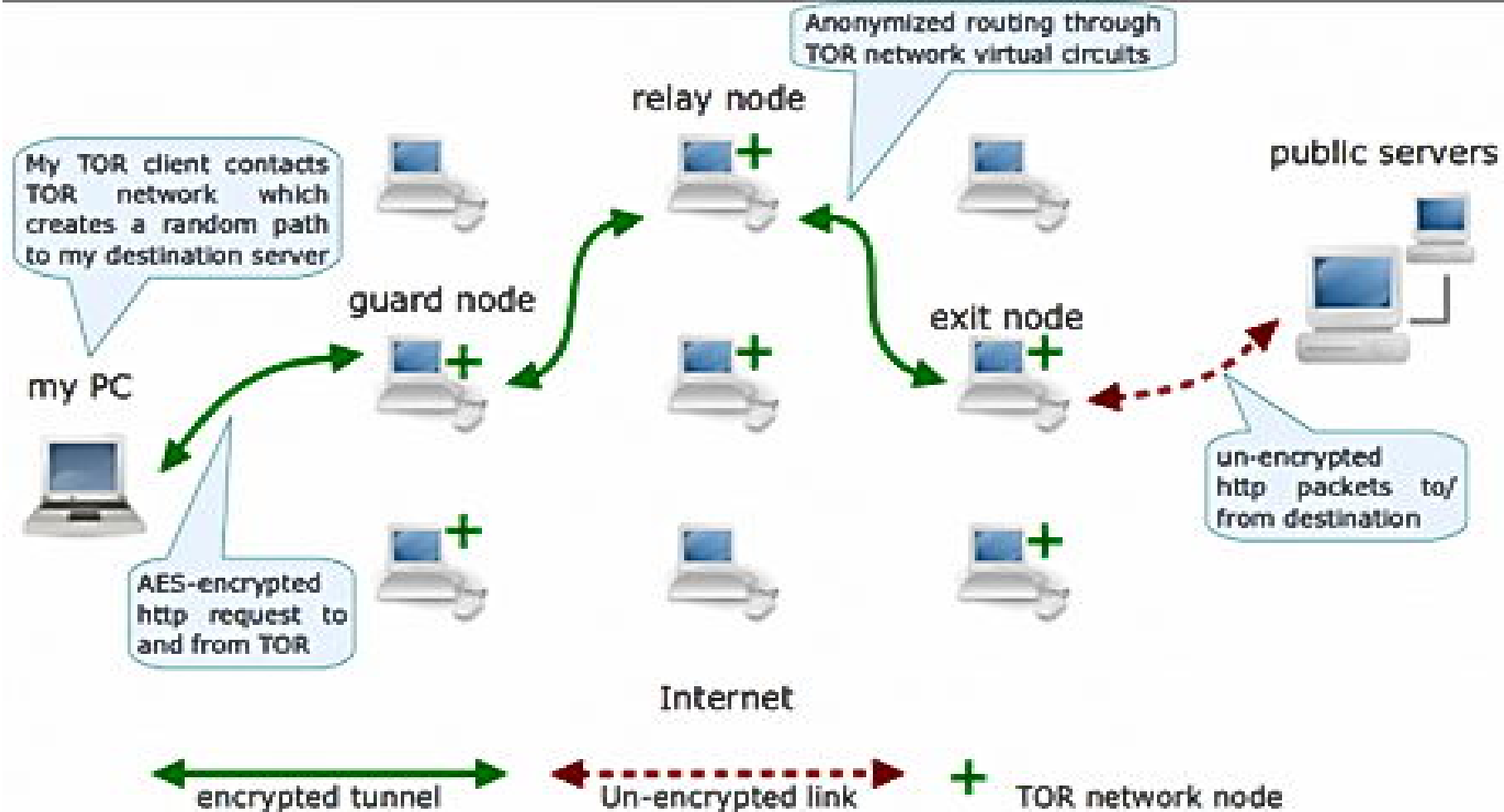
Tor Browser



<https://www.torproject.org/>

- Free browser based on Firefox
- Uses Tor Network
- Obscures IP address
- Keeps no history
- Blocks ads
- Blocks fingerprinting
- Prevents cross-site scripting

Tor Network

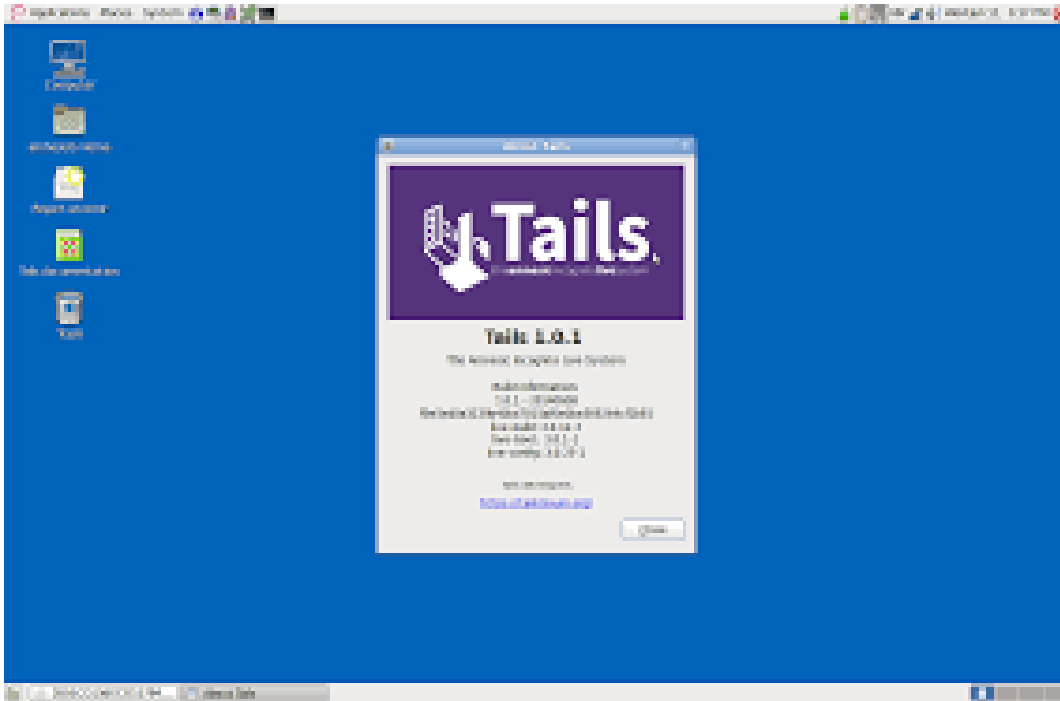


Tor Browser Usability

- Should not add Flash & other extensions
- Some scripts do not work, e.g. Captcha
- Can be slow
- Only protects browser not other apps
- Darknet association



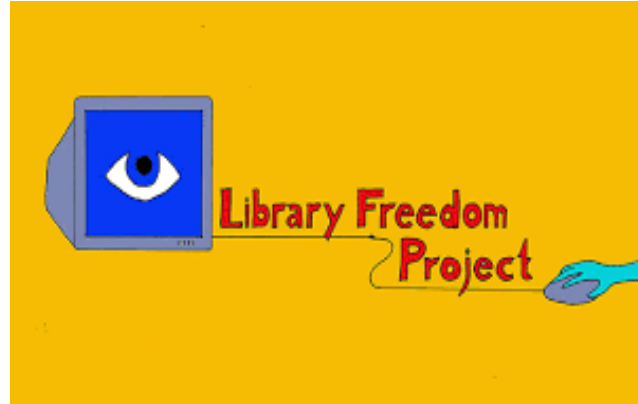
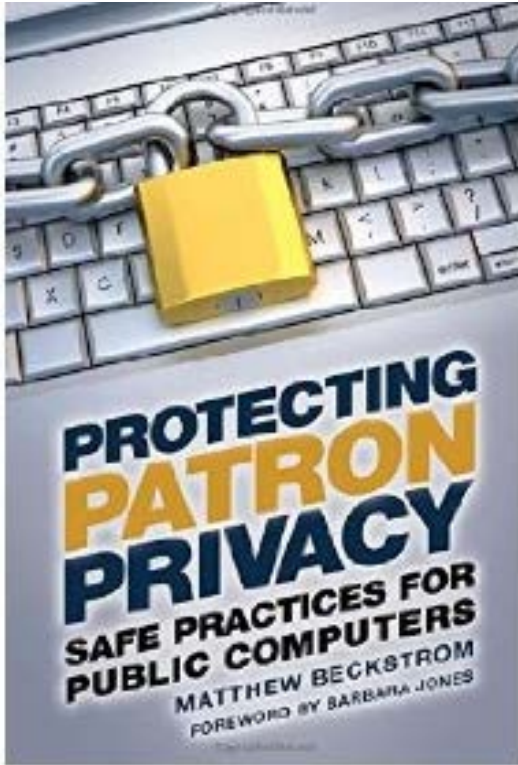
Tails – Tor’s B@d@ss Cousin



- OS for privacy & anonymity
- Based on Debian
- Boot & run from USB or CD ROM
- Leaves no trace on PC
- Uses Tor network
- Robust suite of apps

<https://tails.boum.org>

Privacy Browsing Resources



Library Freedom Project



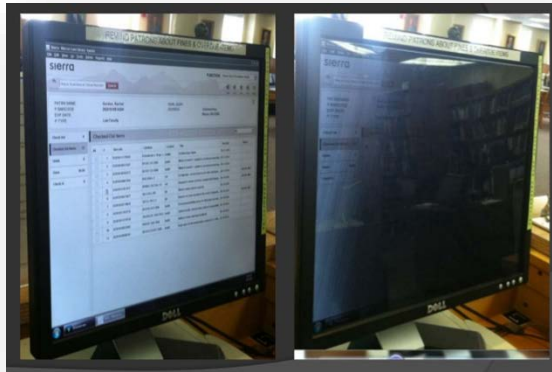
SJPL Virtual Privacy Lab



<https://libraryfreedomproject.org>

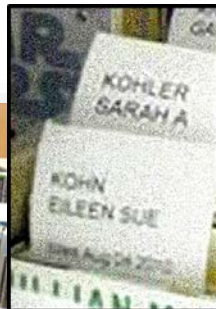
<https://www.sjpl.org/privacy>

Don't forget non-digital privacy...



Privacy Screens

Sensitive Data Displays



Self-Serve Holds

Reference Desks



Questions?

Deborah Caldwell-Stone
ALA Office for Intellectual Freedom
dstone@ala.org
[@privacyala](mailto:dstone@privacyala.org)

Michael Robinson
Consortium Library, University of Alaska Anchorage
Past Chair and Member, ALA Intellectual Freedom Privacy Subcommittee
mcrobinson@alaska.edu