

# Privacy Technology

Tools for Protecting Your Patrons and Yourself  
on Public and Personal Computers.

---

Law Librarian, Davis Wright Tremaine

**Sue Mecklem**

---

# Tools for Privacy Protection



**Sue Mecklem**

Reference Librarian/Competitive Intelligence Analyst

Davis Wright Tremaine LLP

# Overview

- Tools for Protecting Your and Your Patrons' Privacy
  - Social Media privacy settings
  - Mobile Phone privacy settings
  - Data breach monitoring

# I wear two hats

Law librarian  
researcher



Private citizen



# How I Find Your Info



## Select your Permissible Use and GLBA/DPPA Purpose



### 1 Permissible Use ⓘ

You must select a Permissible Use from the drop down menu below to proceed. For more information please [click here](#).

(13). Locate beneficiaries and heirs ▼

### 2 GLBA (Gramm-Leach-Bliley Act) ⓘ

- (3)(B)  To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability.
- (3)(D)  Use by persons holding a legal or beneficial interest relating to the consumer.
- (3)(E)  Use by persons acting in a fiduciary or representative capacity on behalf of, and with the implied or express consent of, the consumer.
- (8)  To comply with Federal, State, or local laws, rules and other applicable legal requirements.
  - No use permitted by GLBA.

### 3 DPPA (Driver's Privacy Act) ⓘ

- (3)  Use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and, if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- (4)  Use in connection with any civil, criminal, administrative, or arbitral proceeding, in any federal, state, or local court or agency, or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court.
  - No use permitted by DPPA.

### 4 Terms and Conditions ⓘ

- I represent and warrant that use of the data obtained hereunder will not be used in whole or in part, as a factor in establishing an individual's creditworthiness or eligibility for (i) credit or insurance, or (ii) employment, nor for any other purpose under the FCRA. ⓘ Further, I understand and agree to the [Terms and Conditions](#) under penalty of perjury. I understand that the misuse of this system may cause immediate termination of my account as well as full prosecution provided by law.

TLOxp contains data governed by the GLBA and DPPA Laws and must be used in accordance therewith.

Continue to TLOxp >

# Questions to Think About

- How findable do you want to be? How private are you?
  - Do you want to be found via search engines?
  - How much can strangers see about you?
  - Photos of yourself and your children?
  - Date of Birth?
  - Where you live, work, commute, visit? Where your children or grandchildren go to school?
  - Medical conditions?



*Collage of Digital (Social) Networks* by Tanja Cappell via Flickr/Creative Commons

# Privacy Rights Clearinghouse Social Networking Privacy fact sheet



**Privacy Rights Clearinghouse**  
Empowering Consumers. Protecting Privacy.

[Sign In](#) to Your Complaint Center

[Home](#) [About Us](#) [Fact Sheets](#) [Latest Issues](#) [Public Policy & Reports](#)  [SEARCH](#)

**Browse Privacy Topics**

- Privacy Basics
- Background Checks & Workplace
- Banking & Finance
- Credit & Credit Reports
- Debt Collection
- Education
- Harassment & Stalking
- Identity Theft & Data Breaches
- Insurance
- Junk Mail/Faxes/Email
- Medical Privacy
- Online Privacy & Technology
- Privacy When You Shop
- Public Records & Info Brokers

## Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social

 [Send to Printer](#)

Copyright © 2010-2015  
Privacy Rights Clearinghouse  
Posted June 01, 2010  
Revised February 01, 2015

1. [Introduction](#)
2. [Types of Social Networks](#)
3. [What Information is Public?](#)
  - a. [Information a User Shares](#)
  - b. [Information Gathered Through Electronic Tracking](#)
4. [Who Can Access Information?](#)
  - a. [Behavioral Advertising](#)
  - b. [Third-Party Applications on Social Networks](#)
  - c. [Government and Law Enforcement Use of Social Networking Sites](#)
  - d. [Creditors May Use Social Networking Sites](#)
5. [Social Networking and Job Searches: Pros and Cons](#)
  - a. [How Social Networks May Assist Job Seekers](#)
  - b. [How Social Networks May Hinder Job Seekers](#)
  - c. [How Social Networks Can Get You Fired](#)
6. [Anonymity on Social Networks](#)

[Complaints](#)  
file a privacy complaint

[Alerts](#)  
latest issues in privacy

[Data Breaches](#)  
timeline since 2005

[Stay Informed](#)  
join our mailing list

 [California Medical Privacy](#)

[Donate](#)



 [Send to Printer](#)  
PDF version

**Follow Us!**

 [Like us on](#)


# Information Leakage on Social Media

- Information users share knowingly
  - Biographical information
  - Location
  - Habits
- Information Gathered Through Electronic Tracking
  - Cookies

# Advertiser Tracking

Facebook interface showing a sponsored post for Warby Parker and a sponsored advertisement for Consumer Reports.

**Warby Parker: Spring 2015**  
Get started with our free Home Try-On program where you can test 5 pairs of glasses, for 5 days!  
WARBYPARKER.COM [Shop Now](#)

**Consumer Reports**  
Consumer Reports  
web.consumerreports.org  
No one tests products like we do! Access unbiased product ratings and reviews.  
  
**Up to 70% off Today!**  
Shop Joss & Main for this and other glamorous finds at up to 70% off!  
599,828 people like this

English (US) · Privacy · Terms · Cookies · More  
Facebook © 2015

# AboutAds.info

• Use the "Choose All Companies" feature to opt out from all currently participating companies in one step. [GO](#)

**All Participating Companies (120)**

**Companies Customizing Ads For Your Browser (41)** SHOW

**Existing Opt Outs (0)** SHOW

**These 120 companies participate in the DAA's consumer choice page.**

Click the company name to find out more about a participating company. To opt out from one or more companies, check the box(es) in the "Select" column next to the company name(s), and then hit the "Submit your choices" button. You can also click the "Select all shown" box to pre-check all the listed companies before you hit the "Submit" button. An [-] symbol in the check box indicates that you have already set an opt out for this company.

[Need help?](#)

COMPANY NAME	SELECT ALL SHOWN <input type="checkbox"/>
<a href="#">Acxiom</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">AOL Advertising</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">eBay Enterprise (formerly FetchBack)</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">Ezakup</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">MediaMath, Inc.</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">Tapad, Inc.</a>	<i>status currently unavailable</i> <input type="checkbox"/>
<a href="#">33Across</a>	<input type="checkbox"/>
<a href="#">Accuen</a>	<input type="checkbox"/>
<a href="#">Adara Media, Inc.</a>	<input type="checkbox"/>
<a href="#">Adblade Premium Ad Network</a>	<input type="checkbox"/>
<a href="#">AddThis (including XGraph)</a>	<input type="checkbox"/>

9:18 PM

# Opting out of FB Ads

The image shows a browser window with several tabs open: 'Stop Facebook from tracki...', 'Home - Digital Advertising Alli...', 'Opt Out From Online Beha...', and 'Facebook'. The address bar shows 'https://www.facebook.com'. The Facebook interface is visible, including a search bar, user profile 'Susan', and navigation links 'Home' and 'Find Friends'. A pop-up window titled 'Facebook Ads' is centered on the screen. It contains the following text:

**Facebook Ads**

**Why am I seeing this ad?**

You're seeing this ad because **Warby Parker** wants to reach women aged 18 to 54 who are in the United States. This is based on things like your Facebook profile information and your internet connection.

**Ad Preferences**

Your ad preferences help Facebook decide which ads to show you. You can edit them to see more relevant ads.

[Manage Your Ad Preferences](#)

Your ad preferences are only visible to you. [Learn more.](#)

**About This Advertiser**

Warby Parker Product/Service

The background of the browser window shows a Facebook profile page with a green sofa advertisement for 'JOYBIRD' and a 'DAVID' advertisement. The Windows taskbar at the bottom shows the time as 9:16 PM.

# Privacy Policies

The screenshot shows a web browser window displaying the Facebook Help Center. The address bar shows the URL <https://www.facebook.com/help/405183566203254>. The page header includes the Facebook logo, the text "Help Center", and a "Log In" button. Below the header is a search bar with the text "How can we help?". The main content area is titled "Desktop Help > Privacy" and "English (US)". A left-hand navigation menu lists several topics: Basics, Controlling Who Can Find You, Troubleshoot Privacy Issues, **Accessing Your Facebook Data** (highlighted), Minors & Privacy, Safety, Questions About Our Privacy Policy, Explore Your Activity Log, and Back. The main content area is titled "Accessing Your Facebook Data" and contains the question "Where can I find my Facebook data?". Below this question is a list of three items:

- **Your Facebook Account:** Most of your data is available to you simply by logging into your account. For example, your Timeline contains posts you have shared on Facebook, along with comments and other interactions from people. Additionally, you can find your message and chat conversations by going to your inbox, or photos and videos you have added or been tagged in by going to those sections of your Timeline.
- **Activity Log:** Within your account, your activity log is a history of your activity on Facebook, from posts you have commented on or liked, to apps you have used, to anything you have searched for. [Learn more.](#)
- **Download Your Info:** This includes a lot of the same information available to you in your account and activity log, including your Timeline info, posts you have shared, messages, photos and more. Additionally, it includes information that is not available simply by logging into your account, like the ads you have clicked on, data like the IP addresses that are logged when you log into or out of Facebook, and more. To download your information, go to your [Settings](#) and click **Download a copy of your Facebook data**. [Learn more.](#)

The Windows taskbar at the bottom shows the system tray with the time 3:35 PM and date 4/11/2015, along with several application icons.

# Mobile Phones



smartphone era by stefanie maria/Creative Commons

# Mobile Phone Settings

---

- Location Services
- Password
- Photo Sharing

# The Problem with Mobile Phones by the EFF



A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

SEARCH

LANGUAGE

MENU



**The Problem with Mobile Phones**

# The Electronic Frontier Foundation says:

- “The deepest privacy threat from mobile phones — yet one that is often completely invisible—is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast.” - *The Problem with Mobile Phones*, EFF webpage

# Location Tracking Threats

- Mobile signal tracking — towers
- Mobile signal tracking — IMSI catcher
- Wi-Fi and Bluetooth tracking
- Location information leaks from apps and web browsing

*The Problem with Mobile Pones, EFF.*

# Mobile Phone Privacy Fixes

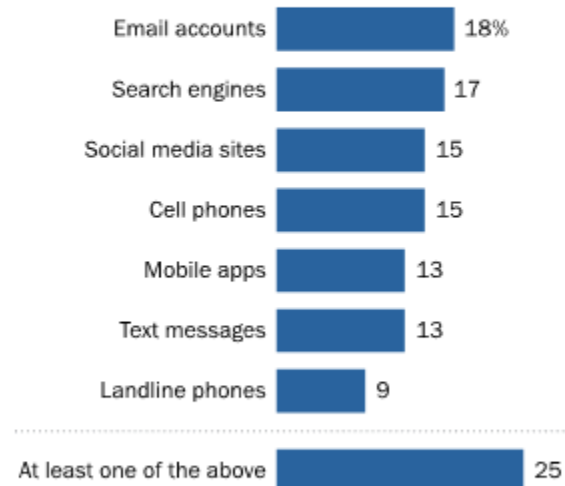
- Basic settings
  - Screen lock
  - Location sharing
- Advanced Tools
  - anonymity software (Tor)
  - privacy-enhancing browser plug-ins (Blur)
  - email encryption programs such as Pretty Good Privacy (PGP)

# Pew Research Center's Americans' Privacy Strategies Post-Snowden

---

## Surveillance Programs Prompt Some to Change the Way They Use Technology

*Among the 87% of U.S. adults who have heard of the government surveillance programs, the percentage who have changed their use of ... "a great deal" or "somewhat"*



Source: Survey of 475 adults on GfK panel November 26, 2014-January 3, 2015.

PEW RESEARCH CENTER

---

# Data Breaches



Locked, by Scott Oakley via Creative Commons/Flickr

# If your data has been breached...

- Monitor your accounts for unauthorized charges or debits
- Report a suspicious charge or debit ASAP; follow up with a letter
- Change your PIN
- If you are unhappy with bank's response, submit a complaint to the Consumer Financial Protection Bureau

# EPIC Online Guide to Practical Privacy Tools



[About EPIC](#)   [Policy Issues](#)   [Press](#)   [Events](#)

## EPIC Online Guide to Practical Privacy Tools

---

[CD/USB Based Operating Systems](#) |  
[Internet Anonymizers, Virtual Private Networks \(VPNs\) and Proxy Servers](#) |  
[Web Browser Ad-ons](#) | [Search Engines](#) | [Email Encryption](#) | [Alternative Email Accounts](#) |  
[Anonymous Remailers](#) | [Disk/File Encryption](#) | [Secure Instant Messaging](#) |  
[Disk/File Erasing Programs](#) | [Password Vaults](#) | [Firewalls](#) | [Antivirus](#) |  
[Cookie/Cache/Internet History Cleaners](#) | [Mobile Privacy](#) | [VoIP/Video Messaging](#) |  
[Social Networking](#) | [Meshnet](#) | [Alternative Currencies](#) | [Publishing](#) |  
[Temporary Mobile Phones](#) | [Heartbleed](#) | [Additional Resources](#) |

Director of Information Technology, Warner  
Pacific College

**Linda Rudawitz**

---

# Threat Environment Changing

- Major threats from professional hackers:
  - Organized Crime:
    - Cyber Mafia: Eastern Europe and others
  - Foreign Governments
- Type of threat:
  - Social Engineering to obtain credentials
- Effects:
  - Compromise of personal information/identity theft
  - Extortion: Ransomware

# No Data is Completely Safe

- Defense in depth – what one layer misses, another may catch
- Layers:
  - User training – largest risk
  - Firewalls and web filtering
  - Anti-malware software
  - Minimize administrative privileges on devices
  - Network separation – public vs. administrative

# Cloud Computing

- Made possible by virtualization and high-speed internet connections
- Highly attractive from viewpoint of operational cost
- Less control
  - Relying upon someone else to provide security
  - Larger targets for hackers
  - No way to isolate data from Internet access
- May want to keep critical data in-house

# Encryption

- Applying a mathematical algorithm to transform data to prevent reading without the “key”
- Internet:
  - HTTPS to prevent interception of data “in transit”
  - Buy certificates from trusted authorities for servers: Verisign, GoDaddy, ...
- Desktop:
  - Encrypt entire hard disk/flash drive to prevent access to data in case of equipment theft/compromise
  - Local software: Symantec PGP
- Ransomware:
  - Bad guys encrypt your files and charge you to obtain the decryption key

# VPN – Virtual Private Networks

- A secure way to permit remote users to access network resources
  - Effectively places remote device “on-site”
  - Important to implement controls
- Security controls
  - UserId, 2-factor authentication
  - Computer Hardware Identity
  - Check for Anti-virus and update status
- Many different solutions
  - Many are difficult to support or conflict with other software
  - Sometimes used to circumvent security standards
  - Example of one that is easy to use and support: Pulse

# Pulse Secure VPN

The screenshot shows a web browser window with the URL <https://vpn.warner...>. The page features a navigation bar with the 'wp' logo and links for Home, Meetings, Preferences, Session (07:59:08), Help, and Sign Out. A search bar with a 'Browse' button is also present.

A welcome message states: "Welcome to the Warner Pacific VPN Service, adminlr. You last signed in on Tue, 14-Apr-2015 06:18:58 PDT. Welcome to the revamped Warner Pacific SSL-VPN access. Over the next few weeks we will be updating some settings to better serve your experience with the VPN service. Have feedback? E-mail us at: [servicedesk@warnerpacific.edu](mailto:servicedesk@warnerpacific.edu) - IT Team".

The interface includes several sections:

- Web Bookmarks:** A list of links including [mywp.warnerpacific.edu](http://mywp.warnerpacific.edu), [blogs.warnerpacific.edu](http://blogs.warnerpacific.edu), and [webmail.warnerpacific.edu](http://webmail.warnerpacific.edu).
- Files:** A section indicating "You don't have any files bookmarked."
- Terminal Sessions:** A section with a "Launch" button and a text input field containing "test.device.net or 192.168.2.3". Below this are links for "Warner Pacific Remote Desktop TS", "Netmon", "Veeam", and "Linda-VM".
- Client Application Sessions:** A section with a "Start" button and a link for "Pulse Secure".

# Wi-Fi/Mobile Access

- Public Wi-Fi
  - Do you know who's behind your access point and what, if anything, they do to protect you?
  - Assume its dangerous!
- Cellular
  - Somewhat safer than Wi-fi
  - Can be used for credit card transactions (SQUARE)
- Payment Card Industry (PCI)
  - Compliance with strong security standards is required (PCI DSS)
  - Requires compliant networks – usually not possible for a network with public access.
  - Both companies and vendors tend to misunderstand requirements

# Watch Out!

- Be Aware
  - Social Engineering is the biggest threat
  - Over 90% of email is SPAM
  - Firewalls and filters can't stop everything
- Be Suspicious
  - Avoid clicking links in emails
  - If a link from an email asks for a login, don't give it
- IT Departments should never ask you to follow a link to update your account.

Library Director, Hood River County Library  
District

**Buzzy Nielsen**

---

# A primary goal

- The library should be a welcoming and safe space for everyone, no matter how they're accessing it or what service they're using.

# Impediments to that goal

- Public networks are open and, by definition, insecure.
- Public computers are in open public spaces.
- There are scary people on the Internet.
- There are scary people in your library.

# Sensitive topics

- Bank accounts
- E-commerce
- Medical information
- Proprietary business data
- Social Security Numbers
- Taxes

# Policy solutions

## **Policies where privacy should be addressed:**

- Privacy Policy (natch)
- Technology/Computer/Internet Use Policy
- Code of Conduct
- Organizational Values
- Personnel Policies
- Public Records Policy (where relevant)
- Volunteer Policy

# Policy solutions

Brevity. Use plain language.

## **Things to address:**

- What you store and for how long.
- You can't guarantee privacy.
- Your networks are open.
- When you might have to share data with outside sources.
- People shouldn't be cyber creeps, data miners, or peeping Uncle Sams on your computers.

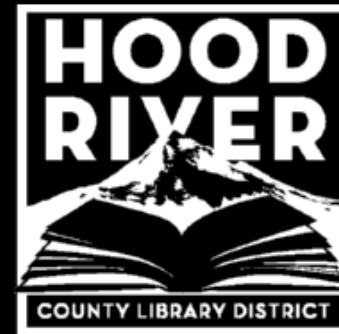
# Signage/notification

## Internet & Computer Use Notice

Because our computers are located in a public space shared by people of all ages, patrons are reminded that:

- Patrons should use discretion when choosing what to view.
- The library cannot guarantee confidentiality.
- Other patrons should respect the privacy of computer users.

Please don't hesitate to contact library staff if you have any questions, concerns, or comments.



# Signage/notification



## Internet and Computer Use Agreement

ssion, Hood River County Library District is pleased to offer publicly-accessible computers and networks. Because these etworks are open to the public and are available in public areas of the our facilities, the Library District cannot guarantee ata you transmit while using our services.

come the following rules:

ly guarantee usage of library-provided computers for one hour.

nce with our [Internet and Computer Use Policy](#), the following is prohibited:

ing pornography.

ling material that is obscene, libelous, threatening, or harassing.

ting intellectual property laws.

aging equipment or systems or using them to create malicious software.

/ with these rules may result in loss of library privileges, exclusion from District libraries, and/or prosecution.

itate to contact us if you have any questions, concerns, or comments.

# Public computer weaknesses

- Internet history
- Office application history
- Sessions left open
- Documents left on desktop

# Privacy in the browser



Firefox Preferences

General Tabs Search Content Applications Privacy Security Sync Advanced

**Tracking**

Tell sites that I do not want to be tracked  
[Learn More](#)

**History**

Firefox will: Use custom settings for history ▼

Always use private browsing mode

Remember browsing and download history

Remember search and form history

Accept cookies from sites [Exceptions...](#)

Accept third-party cookies: Always ▼

Keep until: I close Firefox ▼ [Show Cookies...](#)

Clear history when Firefox closes [Settings...](#)

**Location Bar**

When using the location bar, suggest:

History

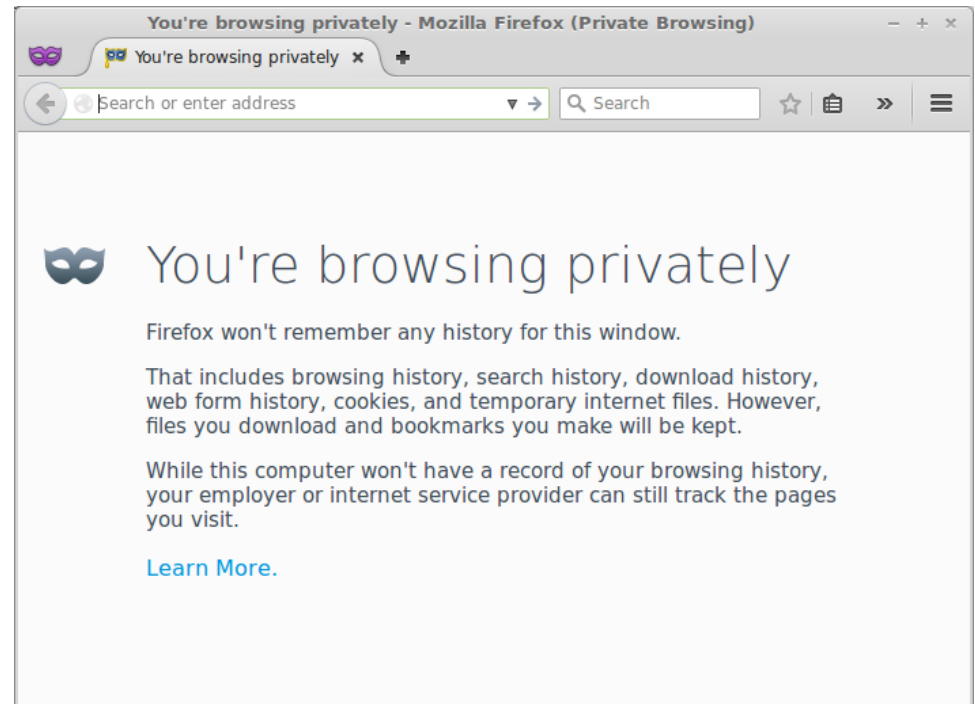
Bookmarks

Open tabs

[Help](#) [Close](#)

# Privacy in the browser

- Does saving history for a session provide a value to patrons that outweighs privacy concerns?



# Privacy in the browser

## Recommended settings

- Tell sites you don't want to be tracked
- Accept cookies: Yes
- Accept third-party cookies: Yes  
(begrudgingly)
- Keep cookies until: You close the browser
- Clear history upon exit
- Remember passwords: Oh hell no

# Privacy on the workstation

- Session timeouts (Time management software)
- Empty trash bin
- Empty temp and downloads folders
- Turn off history on all applications (office applications, image editors, etc.)
- Wipe computer upon session end
- Automatic security updates
- Don't forget selfchecks and catalogs

# Privacy on networks

- Disallow visibility on public networks
- Use firewalls to filter and block ports
- Regularly update network hardware
- Change default logins



# Privacy on networks

## DHCP Clients List

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Julie-s-iPhone	[REDACTED]	192.168 [REDACTED]	02:25:59
2	android-35ec752f3398040d	[REDACTED]	192.168 [REDACTED]	02:11:52
3	iPad	[REDACTED]	192.168 [REDACTED]	02:09:06
4	cl-internet-02	[REDACTED]	192.168 [REDACTED]	02:06:08
5	cl-internet-03	[REDACTED]	192.168 [REDACTED]	02:06:07
6	director	[REDACTED]	192.168 [REDACTED]	02:01:56
7	cl-staff-01	[REDACTED]	192.168 [REDACTED]	02:01:11
8	cl-internet-04	[REDACTED]	192.168 [REDACTED]	02:01:11
9	cl-internet-01	[REDACTED]	192.168 [REDACTED]	02:01:09
10	cl-internet-05	[REDACTED]	192.168 [REDACTED]	02:01:09
11	none	[REDACTED]	192.168 [REDACTED]	02:01:08

# Privacy in meatspace

## Concerns in the physical world

- Visibility of screens
- Documents left on printers, scanners, copiers, and desks
- Accessibility of networking hardware
- Personal devices left on tables

# Privacy in meatspace

- Use privacy screens or carrels
- Use print management software or have staff-mediated printer access
- Regularly sweep and check for sensitive documents
- Keep networking hardware in staff-only areas
- Remind patrons to keep close watch on their devices
- Shred everything!

# Privacy with staff workstations

- Assess whether looser privacy settings are preferable for staff workstations (e.g. history, cookies)
- Set strong privacy controls on workstations used by multiple staff
- Educate staff about privacy
- Educate staff about ethical and public record implications of accessing personal data on work-owned devices

So...

**Questions?**

---

Visit the Oregon Library Association's  
**Intellectual Freedom Committee**  
website for more resources.

---