Introduction to data privacy literacy

Amy Swackhamer - Web Services Librarian, UMD Libraries

MD Tech Connect, December 2025

What we’ll cover

a general overview of digital privacy for individuals

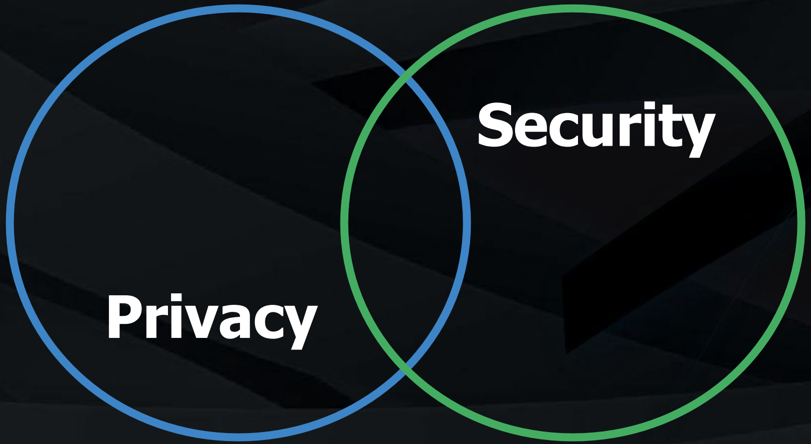
- Why you should care about data privacy
- Who collects your data and what do they do with it
- The privacy regulation landscape
- Vectors of concern and possible actions
- What libraries are doing to promote privacy
- Resources to get started and learn more

Caveats

- Specific tools and strategies vary depending on circumstances and priorities
- Privacy issues are constantly evolving

Background

Privacy and Security



Privacy is having control over who has what level of access to information about you. Security is being able to trust the systems that you use to be effective in keeping your data and you safe.

Why do we need privacy?

“The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society. One cannot exercise the right to read if the possible consequences include damage to one's reputation, ostracism from the community or workplace, or criminal penalties.”

- The American Library Association, https://www.ala.org/advocacy/privacy

Who has your data?

Big Tech

Alphabet (Google)

- Gmail
- Google Search
  Google Office
- YouTube
- FitBit
- Android
- ReCAPTCHA
- Google Analytics
- Waze
- Nest
- (more)

Meta (Facebook)

- Facebook
- Instagram
- Threads
- WhatsApp
- Oculus
- (more)

Amazon

- Amazon.com
- AWS
- Whole Foods
- Ring
- Twitch
- (more)

Apple

- Mac OS
- iPhones
- Apple watch
- Apple Music
- Apple TV⌵
- (more)

Microsoft

- Windows
- Microsoft Office
- XBox
- (more)

Just one example: A bit of Google’s data privacy track record

- **2004** - Gmail is revealed to be scanning the contents of user’s email accounts without consent.
- **2007** - Privacy International gives Google the lowest possible ranking in its 2007 Consultation Report, “Hostile to Privacy.” Google was the only company in the list to receive that ranking.
- **2010** - Germany’s data protection authority discovers that Google has been using its StreetView camera vehicles since 2007 to intercept and store payload data from unencrypted public networks, including names, credit card information, and passwords.
- **2019** - Google is the only World Wide Web Consortium (W3C) member to vote to veto the Privacy Interest Group (PING) from expanding its charter so it can require new technical specifications take data privacy into consideration.
- **2022** - Google settles with 40 US states for around $400 million over allegations that it illegally tracked user location information even when the users had turned off location tracking.

Who has your data?

Most companies you do business with

- Phone apps
- Credit card companies
- Stores with rewards/loyalty programs
- Car manufacturers
- Smart device manufacturers
- Streaming service providers
- Your internet service provider

Who has your data?

Data Brokers

You have probably never heard of most of the companies that buy, aggregate, and sell data about you with almost no oversight. These “partners” (as they are described in website privacy policies) sell things like “risk management” services to companies based on data dossiers about individuals to rate them on probability of different behaviors, and can provide lists of people with very specific attributes to advertisers.

Some library database providers are also major personal data brokers, including Thomson Reuters and RELX.

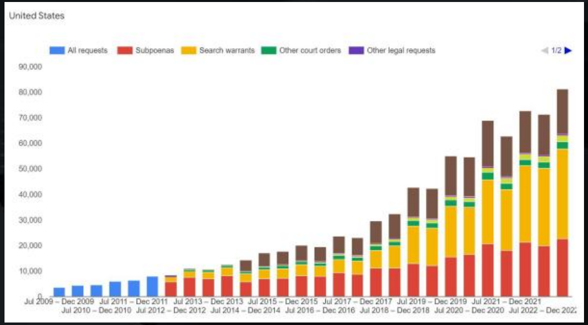
What kind of data about you may be gathered and exploited?

- Web search history
- Web pages visited
- Demographic information (age, gender, race, income, etc.)
- Location data (including your patterns of movement and real-time location)
- Fitness tracker data (heart rate, weight, exercise habits and performance, etc.)
- Driving habits (speed, braking, mileage, etc.)
- Purchase history
- Financial information (investments, debts, etc.)
- Genetic data
- Health information (conditions, prescriptions, test results, etc.)
- Photos of you for facial recognition systems
- Relationships (family members, social media connections or follows)
- **Most anything that happens online**, is posted online, or is processed through a connected device

Who might want access to your data?

- Advertisers
- Political influence campaigns
- Law enforcement*
- US government agencies
- Foreign governments
- Car insurance companies
- Medical insurance companies
- Current/potential landlords
- Current/potential employers
- Stalkers
- Any kind of adversaries or malicious actors (identity thieves, ransomware creators, etc.)

* Law enforcement and government agencies purchasing data about people is criticized by privacy advocates as subverting the 4th Amendment's ban on unreasonable search and seizures. Law enforcement also issues warrants for data. Here's a chart of requests received by Google 2009 - 2022.



Laws protecting digital privacy

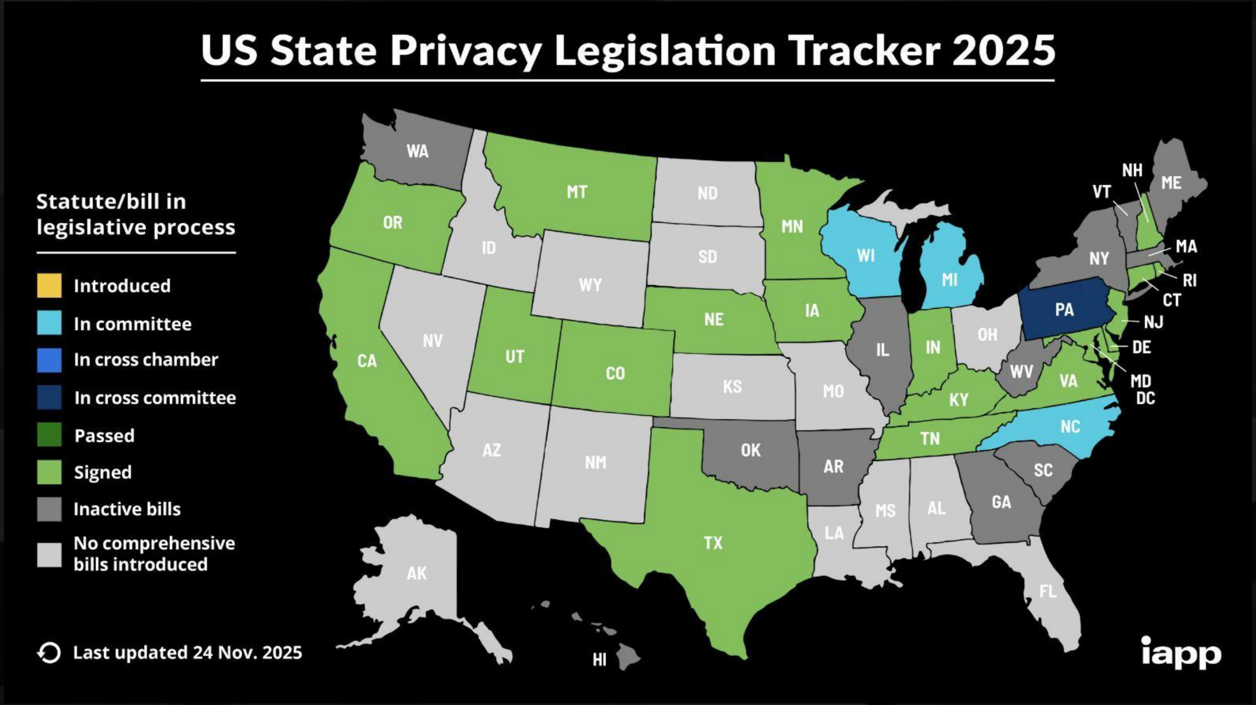
The European Union’s GDPR

The world’s most influential privacy law, which doesn’t apply to us

The European Union’s **General Data Protection Regulation (GDPR)** went into effect in 2018 to strengthen individual rights over personal data using 7 principles:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

The US lacks nationwide data privacy regulations



Find the International Association of Privacy Professionals's State Privacy Legislation Tracker at https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Good news for us

Maryland Online Data Privacy Act of 2024 (MODPA)

- Limits companies or a certain size or data sale volume to collecting what is reasonably necessary for the product or service they provide
- Prohibits processing personal data for secondary reasons without the consumer's prior consent
- Prohibits the sale of sensitive data (e.g. race, religious beliefs, sex life or orientation, genetic or biometric data, Consumer Health Data, or precise (within 1,750 feet) geolocation)
- Bans the sale of data about people under the age of 18
- Took effect October 1, 2025 but will not "have any effect on or application to any personal data processing activities before April 1, 2026."

Maryland Kids Code

- Unanimously passed the MD General Assembly in April 2024
- Applies to companies that create online products "that kids are likely use"
- Bans companies from profiling children under 18 to serve personalized ads
- Prohibits companies from tracking children's locations in real-time except when necessary
- Modeled on the 2022 California Age-Appropriate Design Code Act
- Faces vigorous tech industry opposition

Options to improve data privacy

Web Browsers

Risks

Browsers process and can store private information like your browsing history, usernames, passwords, and autofill information, such as your name, address, etc.

They can reveal identifying information about your location, system settings, hardware, and more to third parties.

Browser fingerprinting allows for tracking you through your machine's browser based on a pattern of details like timezone, language, privacy settings, device specs, and cookies.

What you can do

Use a secure browser for both computers and phones.

Set up HTTPS by default on your browser to encrypt your data.

Use one browser for logging into "Big Tech" accounts (Google, youTube, Facebook, X, Instagram, TikTok, etc.) and a different one for normal web searching and browsing.

Be cautious with browser extensions and only install ones you actually use from reputable providers.

Some possible tools

- Firefox
- Ungoogled Chromium
- Brave
- DuckDuckGo (mobile)
- Vivaldi
- Tor
- Mullvad

Ad/Tracker Blockers

Risks

Many online ads contain trackers that record details of your online activities and information you reveal about yourself to build profiles of you for targeted advertising, or to sell for use by advertisers.

Ads can also contain malware that infects your computer when the ad loads ("malvertising").

What you can do

Use tracker blocking tools like browser extensions, mobile apps, a VPN with ad blocking, or router-based blockers

Some possible tools

- uBlock Origin
- Privacy Badger (EFF)
- Threat Protection (Nord Security)
- AdBlock Plus plugin
- Ghostery

VPNs (Virtual Private Networks)

Risks

Internet service providers (of both your home network and wifi networks you use) are tracking your online behavior.

Other Considerations

Some services block known VPNs. VPNs can also trigger additional security checks on websites.

They will not stop browsers or sites from tracking your behavior.

What you can do

A VPN anonymizes your internet connection and stops your ISP from tracking who you contact online or what websites you visit. It blocks websites from tracking your IP address and location data.

Use a **reputable** VPN for both computers and mobile devices, particularly on public networks.

Some possible tools

- NordVPN
- ExpressVPN
- Surfshark
- Proton VPN

Search Engines

The risk

Search engines track your IP address, location, unique identifier ID, and search queries you enter. This data can be aggregated into digital profiles of you that could contain personally identifying information.

What you can do

Use a search engine that doesn't track you. Some of these are "metasearch" engines that pull results from other common search engines while preventing those engines from tracking you.

Some possible tools

- DuckDuckGo
- Brave Search
- SearX (Google sometimes blocks)
- MetaGer
- Qwant
- Kagi (not free)

Passwords

Risks

Someone who can access your accounts can find or change any information stored in them, and some accounts (e.g. email) may be used to gain access to many other accounts. This poses great privacy, financial, and reputational risks, and secure password management for key accounts is extremely important.

Many password managers can save, encrypt, and fill in webform data (like your name, address, etc.) in addition to passwords.

What you can do

- Obviously, follow password best practices (long, hard-to-guess strings including special characters, numbers, etc.)
- Use 2-Factor Authentication
- **Use a Password Manager (highly recommended)**
- Use Passkey identification where available
- Log out when you aren't using an account

Some possible tools

- Bitwarden
- NordPass
- 1Password
- Proton Pass

Email

Risks

Popular email services may allow scanning of email accounts by advertisers and developers, which is often not carefully monitored.

Remember that privacy of what you send in email is only as secure as the least secure recipient in an email thread.

What you can do

- Switch to use a privacy-focused, encrypted email service. These may have a subscription fee.

Some possible tools

- Proton Mail
- Tuta
- Mailfence
- Mailbox.org
- Posteo

Social Media

Risks

There are many privacy-related risks from social media like stalking, location disclosure, personal data collection by third parties, government monitoring without warrants, or impersonation / identity theft.

Metadata in photos you upload can reveal the location and time where something happened. Photos can also be run through facial recognition tools to identify people.

What you can do

- Set all your social media profiles to private rather than public display. Review privacy settings.
- Avoid sharing sensitive personal information on social media
- Close accounts you don’t use

Cloud Storage

Risks

Cloud storage services are a popular hacking target, and if you are backing up the contents of your computer hard drive, anything in there could be obtained.

What you can do

Use cloud storage encrypted with keys that you control. This will likely cost something.

Some possible tools

- Proton Drive
- NordLocker
- Tresorit
- Sync.com

Smartphones

Risks

Mobile apps often store logins that access personal information. Mobile apps also frequently gather excessive data to monetize.

Location data is one of the most personal types of information acquired through smartphones, since many people carry them at all times. This can show where you went, how long you were there, and who you were with.

What you can do

- Keep your phone securely locked
- Remove apps you don’t use
- Look at app permissions and remove unnecessary access to things like location, contact list, photos
- Opt out of ad personalization (i.e. tracking your detailed for targeted ads)

Some possible tools

- iVerify App
- Stolen Device Protection (iOS)

If you get very interested in smartphone privacy, there are privacy-focused phone operating systems like Graphene, Murena, And Calyx.

AI/LLM Agents

Risks

AI tools track your conversations and searches, creating a profile of what you are using them for. That data could potentially be sold or hacked.

What you can do

- When researching potentially sensitive information, use a VPN, don’t log into the AI tool, and don’t use the web browser you’re using for other online activities.

“Internet of Things” (IOT)

The risk

Your smart speakers, smart TV, smart watch, doorbell camera, and many other devices on your home network may be recording and transmitting what you do or say or monitoring network activity.

Read “smart device” as “surveillance device.”

What you can do

Research privacy for networked products you are considering purchasing, for instance on Mozilla’s “Privacy Not Included*”

Put your IOT devices on a guest network at your home, not the primary network with your computer and phone.

*unfortunately, Mozilla disbanded this group in the fall of 2024, so they won’t be helpful far into the future.

Vehicles

The risk

Privacy policies for newer cars generally allow the manufacturer to capture any data you generate through driving or transmit with your phone while connected to the car.

Car manufacturers have been selling information on driving habits, location, and more to data brokers. increased insurance rates for some people when insurance companies purchase the data.

What you can do

Unfortunately, not a lot at this point aside from buying old cars and following news developments in this area. Extremely invasive privacy policies seem to be an industry standard.

Another thing: Ubiquitous license plate readers (like Flock) used by law enforcement are tracking your car’s location and the time it was logged. This data can be tracked across states in the US.

Other things you may want to try

Data removal services

- Incogni
- DeleteMe
- Optery
- PrivacyBee
- Many others

(These are not free.)

Private messaging

- Signal
- WhatsApp (this is owned by Meta)

Current developments creating more privacy concerns

- Wearable devices with audio/video recording of people besides the owner (e.g. Meta glasses that are $250 and look like normal glasses)
- Facial recognition technology becoming common
- AI enabling easy voice cloning and deep fake videos
- Microsoft Recall (automated AI-powered searchable screenshots of everything a user does on a Windows PC)
- Palantir combined government data dossiers on US citizens
- Age verification requirements for websites leading to user identification

Where to start? A personal security plan

a.k.a. “threat modeling”

- What data do you most want to protect?
- Who do you want to protect it from?
- How severe are the repercussions of your data being uncovered?
- How much inconvenience are you willing to accept to try to prevent potential consequences?

NOTES:
Consumer Reports offers a security planner to help you get started - see audience resources.

For tools that are not free, you can often find discount codes online if you look around on privacy/security websites, podcasts, etc.

Further actions for individuals

- When possible, use products and support organizations that best align with your privacy values
- Continue to learn about privacy topics and help friends and family learn to protect their privacy (see the resource list linked at the end of this presentation)
- Contact your legislators to voice support for privacy regulations
- Support independent technology journalism

What are libraries doing to promote privacy?

- Minimizing data they collect about users
- Collaborating to monitor vendor data collection and work towards improved policies and contract terms
- Holding educational sessions on key aspects of digital privacy
- Sharing information about privacy through user guides
- Setting public access computers to purge session data and install security and ad-blocking software

See the audience resource list for places to learn more.

Questions?

aswack@umd.edu

Annotated Resource List

https://go.umd.edu/25lw

This list links to privacy guides, sources for tool recommendations, advocacy organizations, and more.