



Privacy in Public Libraries

Lauren Abner
**Kentucky Department for
Libraries & Archives**

May 19, 2021

Presentation Contents

- [Why We're Talking Privacy](#)
- [Privacy Laws](#)
- [Privacy for Sale](#)
- [Why Privacy Matters](#)
- [Library Ethics & Privacy](#)
- [The Questionable Privacy of Digital Library Services](#)
- [Librarians Defending Privacy](#)
- [Reflection](#)
- [Wrapping Up](#)

Why we're talking privacy

- Trends in the legal landscape surround privacy issues
- Public concern over data breaches, tracking of location data and online activities, and sale of 'anonymized' data
- Libraries' reliance on third party vendors for digital services



[Return to Presentation Contents](#)



Privacy Laws

[Return to Presentation Contents](#)

KRS 61.931

- [Kentucky Revised Statutes](#) 61.931, 61.932, 61.933, and 61.934 govern Personal Information Security and Breach Investigations
 - Went into effect January 1, 2015
- Special Purpose Government Entities (SPGEs)—such as public libraries—and vendors with access to personal information must maintain, implement, and update policies & procedures to protect it.
 - See next slide for definition of ‘Personal Information’

KRS 61.931 defines 'Personal Information'

"Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- a) **An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;**
- b) **A Social Security number;**
- c) **A taxpayer identification number that incorporates a Social Security number;**
- d) **A driver's license number, state identification card number, or other individual identification number issued by any agency;**
- e) **A passport number or other identification number issued by the United States government; or**
- f) **Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;**

General Data Protection Regulation (GDPR)



- Went into effect on May 25, 2018
- Gives EU citizens unprecedented control over their personal data:
 - Right to give explicit consent for use of personal data
 - Right to access what data a company has about you and transfer that data (data portability)
 - Right to be forgotten
- Affects all companies that conduct business in the EU or that have a website that can be accessed from the EU or by EU citizens – most websites use a product or service from a company that must comply
- Companies must prove they have your consent to collect and keep your information
- Massive fines for non-compliance—up to 4% of a company’s annual turnover

Privacy Rights in California

- California Consumer Privacy Act went into effect on January 1, 2020; see <https://www.caprivacy.org/>
- Prop 24 in November 2020 created the California Privacy Rights and Enforcement Act to start 1/1/23
- Protects personal information of all California residents
 - Access data stored, ask for its deletion, data portability
- Defines ‘personal information’ broadly – covers information about households even if an individual’s name isn’t included
- Affects companies that receive information about California residents depending on certain thresholds for annual revenue, # of California residents whose personal info is received
 - Allows for fines and limited civil class action penalties

[Return to Presentation Contents](#)



Privacy for Sale

Cambridge Analytica Scandal

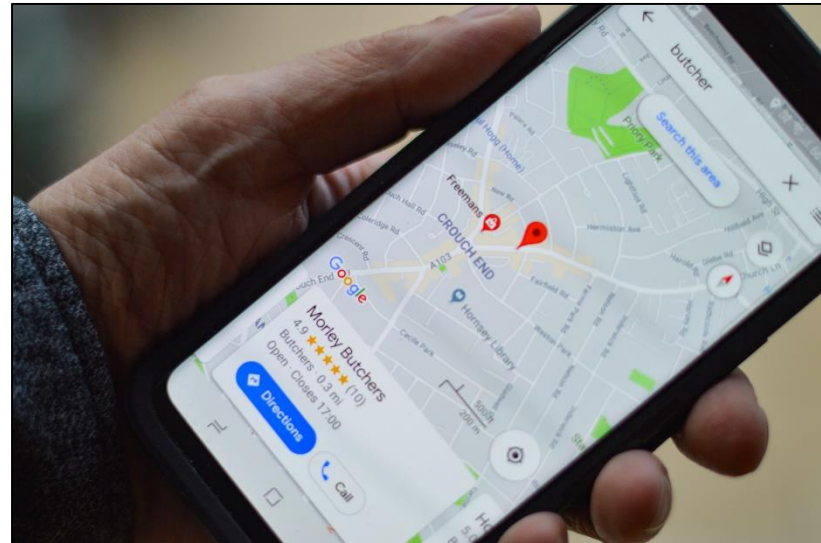


December 2015 – [*The Guardian*](#) [reported](#) that Cambridge Analytica, a British political consulting firm, is illegally harvesting Facebook profile data without consent on behalf of US political campaigns

- **March 2018** – Scandal gained worldwide recognition after whistleblower [revealed](#) that the Facebook accounts of up to 50 million Americans were compromised
- **July 2019** – The [Federal Trade Commission](#) [fined](#) Facebook a record \$5 billion for deceiving users about their privacy. The Securities and Exchange Commission also fined Facebook \$100 million for failing to notify investors about the Cambridge Analytica scandal in a timely fashion

Location Tracking

- **Summer 2018** – All 4 Major cellular network carriers including Verizon, AT&T, Sprint, and T-Mobile [agreed to stop](#) selling users' geolocation data to third-party vendors
- Companies such as Securus Technology sold real-time location data to law enforcement without confirming a valid warrant to access that information



- **April 2020** – Google and Apple release COVID-19 contact tracing framework for health apps using Bluetooth Low Energy (BLE) transmissions. September 2020 – [privacy flaws](#) exposed by researchers.

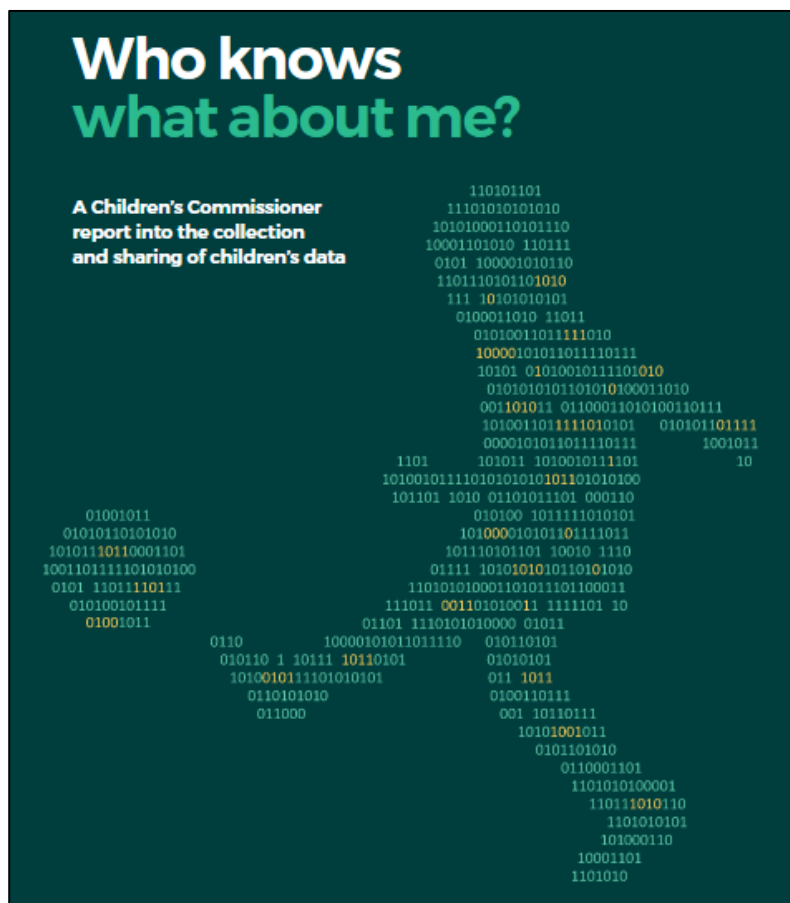
Always Listening



Tech companies have recorded users of voice assistant services without consent and allowed contractors to analyze those recordings.

- **Alexa** – [Amazon announced](#) that users can opt out of human review of voice recordings in August 2019 after the practice was exposed in April 2019. Some [users have reported](#) that unauthorized recordings have been sent to random contacts.
- **Siri** – [The Guardian reported](#) in July 2019 that Apple contractors regularly listen to sensitive user recordings
- **Google Assistant** – Dutch publication [VRT NWS reported](#) that Google hires contractors to listen to and transcribe snippets of recordings

Kids' Privacy Is a (Bad) Joke



- November 2018: UK's Children's Commissioner published [*Who knows what about me?*](#), a report encouraging parents to think about the datafication of their children's lives
- By age 13, parents will have uploaded an estimated 1,300 photos & videos of their child
- By age 18, a child is estimated to have 70,000 posts about them
- Digital footprint includes social media, online medical records, school records, etc.

Student Privacy in the Age of Coronavirus



Photo by [Andrew Neel](#) on [Unsplash](#)

- Apps to track movements on college campuses
- For K-12 students, devices issued by school districts may have extensive filtering and monitoring software loaded
- Videoconferencing—constant need to be online
- Zoom privacy issues – lack of encryption for all account levels, 2FA for desktop and mobile not added until September 2020



Why privacy matters

Social Consequences



Image by [Gerd Altmann](#) from [Pixabay](#)

Financial Consequences



Photo by [Maarten van den Heuvel](#) from [Pexels](#)

Political Consequences

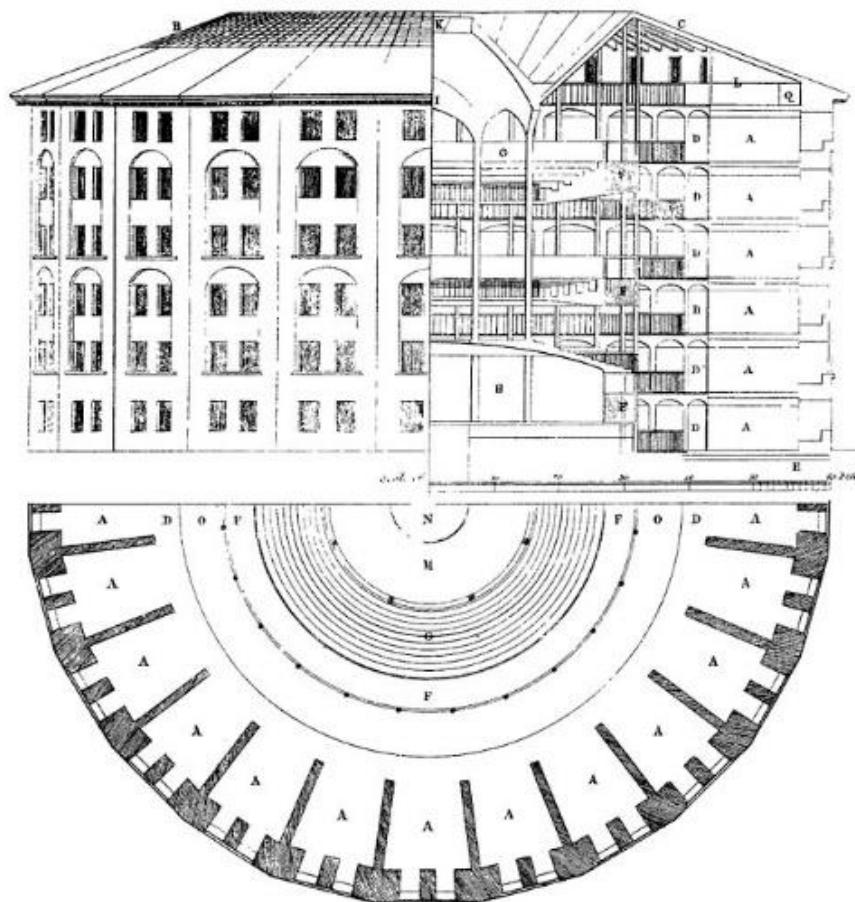


Image by [Ichigo121212](#) from [Pixabay](#)

Self-Censorship

A drawing of a panopticon prison by Willey Reveley, circa 1791, commissioned by utilitarian social reformer Jeremy Bentham. The panopticon requires only 1 guard because any prisoner can be observed at any time from the central tower, which forces prisoners to behave as though they're always being watched.

Image source: By Jeremy Bentham - The works of Jeremy Bentham vol. IV, 172-3, Public Domain, <https://commons.wikimedia.org/w/index.php?curid=3130497>



Everyone has something to hide...even if you don't realize it yet



Library Ethics & Privacy



[Return to Presentation Contents](#)

Privacy & Intellectual Freedom

- The American Library Association (ALA) has codified the rights & responsibilities of library services in the *Library Bill of Rights* and the *Code of Ethics* for librarianship. These documents express the relationship between privacy and intellectual freedom.
 - Intellectual freedom: “the rights of library users to read, seek information, and speak freely as guaranteed by the First Amendment” (see [ALA Intellectual Freedom: Issues and Resources](#)).
 - Intellectual freedom is not possible without privacy, and censorship (or lack of privacy) has a negative effect on free speech.

Code of Ethics



The American Library Association's [Code of Ethics](#) (original 1939; amended 2008) outlines the ethical responsibilities that guide the library profession. Several of those responsibilities relate to patron privacy and intellectual freedom.

Code of Ethics, 3

“3. 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.”

Code of Ethics, 6.

“6. We do not advance private interests at the expense of library users, colleagues, or our employing institutions.”

Library **BILL *of* RIGHTS**

The American Library Association's [Library Bill of Rights](#) (original 1939; amended 2019) expands upon the importance of avoiding censorship in providing library services in several articles.

Library Bill of Rights, Article III

“III. Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.”

Library Bill of Rights, Article IV

“IV. Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas.”


Privacy: An Interpretation of the Library Bill of Rights

ALA further defined the relationship between privacy and intellectual freedom in [*Privacy: An Interpretation of the Library Bill of Rights*](#) (original 2002; amended 2019), which opens with the statement, “**Privacy is essential to the exercise of free speech, free thought, and free association.**”

TL;DR

- **Patrons should expect library services to be provided without censorship and without the violation of their privacy.**
- When libraries engage in censorship or “advance private interests at the expense of library users”, they deny their patrons the right to freedom of speech by curtailing access to information and the ability to express opinions freely.

The Questionable Privacy of Digital Library Services

A person is shown from the back, wearing large black headphones and holding a smartphone. The phone screen displays a grid of colorful icons, likely a library or music application. The person is wearing a plaid shirt and brown pants. The background is a blurred indoor setting.

[Return to Presentation Contents](#)

3rd Party Services on the Rise



Virtual Programming Tools



Adobe Digital Editions



- Early October 2014 – Security [researchers confirmed](#) that Adobe Digital Editions 4.0 is transmitting huge amounts of library patron data to Adobe’s servers in plain text, making it possible to piece together individual reader’s usage
- Late October 2014 – ADE version 4.0.1 added encryption to patron data, but a large amount of data is still transmitted to Adobe’s servers when an ebook with Digital Rights Management is activated.
- Adobe [argued](#) this data collection is within their privacy policy, but collecting information on individual users’ reading habits isn’t necessary for the service they’re providing.

Kanopy Data Breach



- March 2019 – Library video streaming platform notified users of a security incident where users' IP addresses and associated activity were exposed. Kanopy's CEO claimed that only 162 user emails and passwords were affected, of which 82 also included the library patron account number.
- According to security researcher Justin Paine, Kanopy left weblogs unprotected, possibly allowing individuals to be identified with information such as geolocation, timestamp, device type, IP address, and the URLs of accessed files. <https://www.digitaltrends.com/home-theater/kanopy-streaming-data-breach/>

Gale Analytics on Demand

- Santa Cruz Public Libraries (SCPL) supplied patron addresses to Gale Analytics on Demand (AoD) to create marketing reports; AoD uses demographic info from credit agency Experian
- June 2019 California civil grand jury found that:
 - “The use of Gale Analytics on Demand by Santa Cruz Public Libraries was inconsistent with the Library’s long-standing policy on Confidentiality of Library Records.”
 - SCPL “did not adequately inform its patrons about the Library’s use of Gale Analytics on Demand or obtain their consent for this use”



Read the full grand jury report, *Patron Privacy at Santa Cruz Public Libraries: Trust and Transparency in the Age of Data Analytics*:
http://www.co.santa-cruz.ca.us/Portals/0/County/GrandJury/GJ2019_final/SantaCruzPublicLibrariesReport.pdf

LinkedIn Learning



- **2015:** Microsoft, owner of social networking site LinkedIn, acquired online learning platform Lynda.com
- **2019:** Lynda.com announced its rebranding as LinkedIn Learning and its intention to change the authentication process for library patrons—users must create a personal profile & agree to LinkedIn Learning’s terms of service rather than using a library barcode + PIN for access
 - The American Library Association [condemned the change](#) as a violation of patrons’ right to privacy
- **2020:** Libraries win! LinkedIn Learning [won’t require](#) library users to create a LinkedIn profile to access their content

Sound off!



**What are
your biggest
privacy
concerns
related to
library
services?**



Librarians on the Frontlines of Privacy

[Return to Presentation Contents](#)

Privacy Programming

DC Public Library
teaching courses
on patron privacy



Teen Programming



Boston Public Library
teaching teens to resist
facial recognition
software

Photo: Kathy Pham/American Civil Liberties Union of Massachusetts via [American Libraries](#)

Virtual Privacy Lab



San José Public Library created the Virtual Privacy Lab (<https://www.sjpl.org/privacy>) where users can generate a custom privacy toolkit by selecting from the topics that interest them. Also note that SJPL has a section for its complete [privacy policy](#) and links to the [vendor privacy policies](#) of the third-party services it uses.

CryptoParty



Some public libraries have hosted CryptoParty events. From <https://www.cryptoparty.in/> : “CryptoParty is a decentralized movement with events happening all over the world. **The goal is to pass on knowledge about protecting yourself in the digital space.** This can include encrypted communication, preventing being tracked while browsing the web, and general security advice regarding computers and smartphones.

Tor Browser in Libraries



Background image of Tor 'onion' routing: [The Hacker News](#); foreground image of Kilton Library in Lebanon, NH: Library Freedom Project 44

Choose Privacy Week



The American Library Association observes Choose Privacy Week during the first week of May. Resources related to library privacy are available at <https://chooseprivacyeveryday.org/>

Projects & Research



University of Maryland
College of Information –
Safe Data, Safe Families
project funded by IMLS:
<http://safedata.umd.edu/>



New York University partnered with the Library Freedom Project to create the Library Freedom Institute, funded by IMLS, to train Privacy Advocates. <https://libraryfreedom.org/>



Data Privacy Project

Privacy training modules created for New York Public Library staff with IMLS funding:
<https://dataprivacyproject.org/>

Reflection

A black and white photograph of a person's face, partially obscured by their hand, symbolizing reflection or self-examination. The person's eye is visible, looking directly at the camera. The hand is raised, with fingers spread, partially covering the face. The background is bright and out of focus.

[Return to Presentation Contents](#)

What privacy steps can you take?



- In the next 6 months, what step(s) can you take to:
 - Improve patron privacy at your library?
 - Improve your own privacy practices at work or in your personal life?

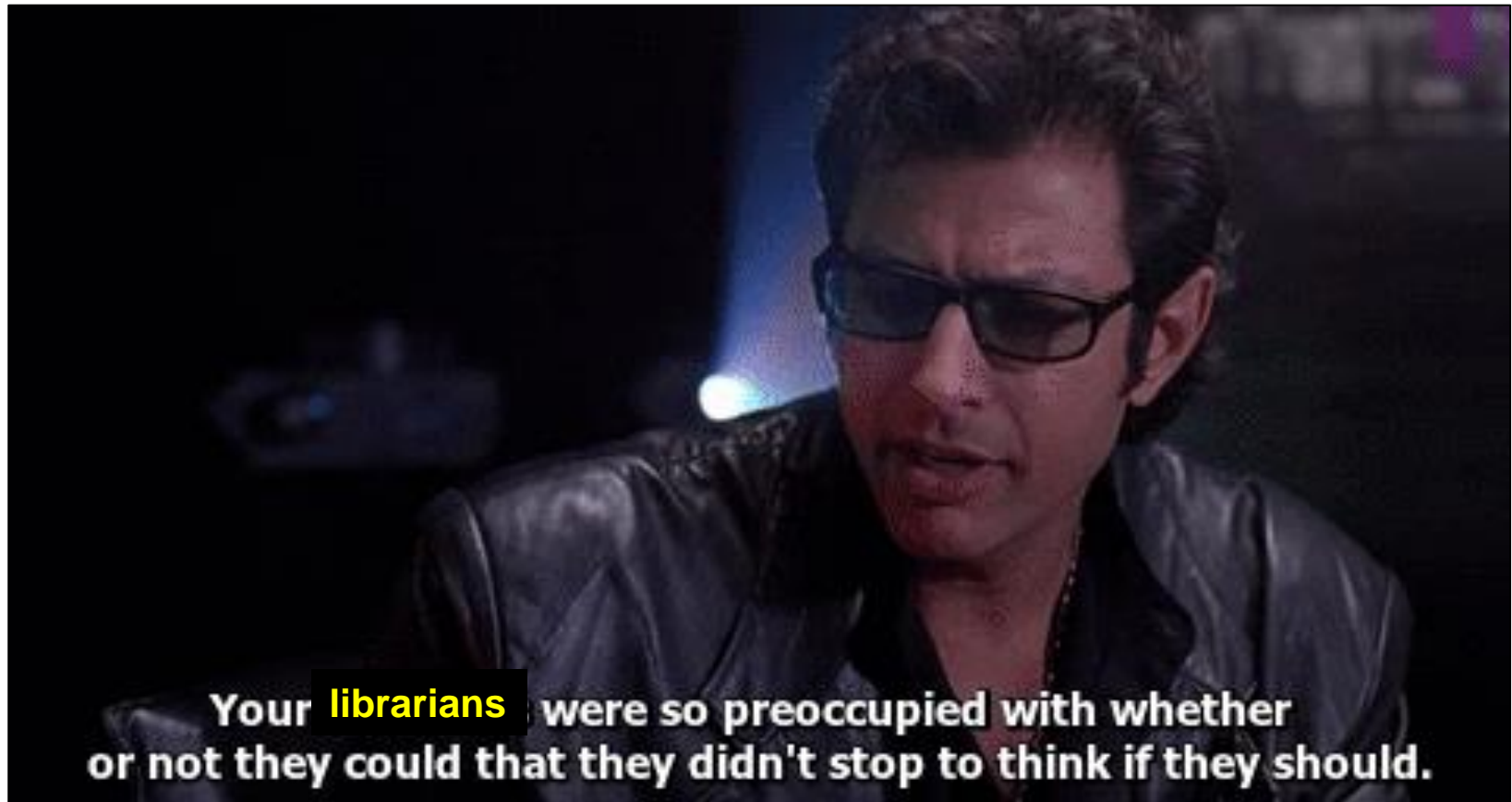
Wrapping Up...

but don't
stop here



[Return to Presentation Contents](#)

The Take-Away

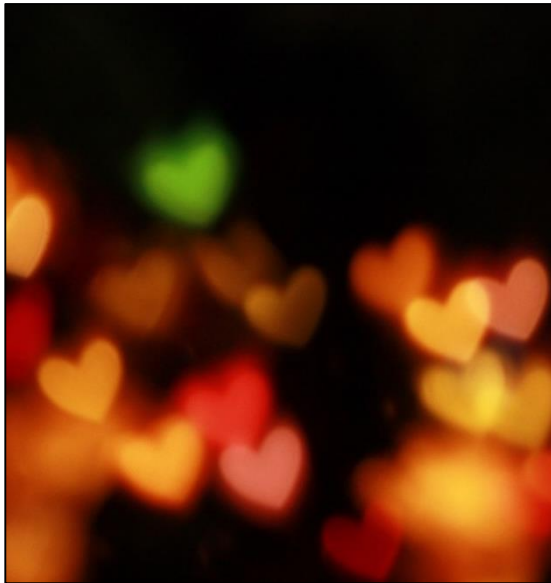


Your **librarians** were so preoccupied with whether or not they could that they didn't stop to think if they should.

Privacy Resources

- **American Library Association Privacy Tool Kit** – <http://www.ala.org/advocacy/privacy/toolkit>. ALA provides information on library values, privacy policies, privacy procedures, and advocacy talking points.
- **Choose Privacy Every Day** – <https://chooseprivacyeveryday.org/> - ALA clearinghouse for library privacy resources
- **Virtual Privacy Lab** – <https://www.sjpl.org/privacy>. Privacy toolkit from San Jose Public Library in English, Spanish, and Vietnamese.
- **Data Privacy Project** – <https://dataprivacyproject.org/>. Patron privacy training used by New York Public Library staff.
- **Electronic Frontier Foundation** – <https://www.eff.org/>. The Tools section includes guides for safer online communications, the Privacy Badger browser extension, and Panopticlick, a tool for analyzing how well your browser settings prevent online tracking

Thanks for your time & attention!



Lauren Abner
Technology Consultant
lauren.abner@ky.gov
(502) 564-1728

KDLA survey link:
<https://www.surveymonkey.com/r/PrivacyPubLibs>

[Return to Presentation Contents](#)

