This is an electronic version (preprint) of an article published in *Behavioral and Social Sciences Librarian*. The article is available online at https://www.tandfonline.com/doi/full/10.1080/01639269.2017.1696072 (subscription required).

Full citation:
Davis, R. C. (2019). "Digital Privacy Resources for You, Your Library, and Your Library's Patrons (Internet Connection column)." *Behavioral & Social Sciences Librarian, 36*.2, 104-107. doi:10.1080/01639269.2017.1696072.

Internet Connection:
Digital privacy resources for you, your library, and your library's patrons

Robin Camille Davis
rcdavis6@ncsu.edu

###

Introduction

Digital privacy is an especially hot topic in libraries in this moment, but it's easy to get bogged down with complex technical discussions. For librarians just starting to reexamine digital privacy in this era of mass surveillance and mass hacking, a better way to begin understanding digital privacy is to make small but important changes to their personal privacy habits. The next step may be to extend the privacy mindset to their library, where infrastructural changes can help safeguard patrons' data. Finally, the privacy-oriented library may provide patrons with information about how they can control their own digital privacy. In this column, I've provided reliable privacy resources and tools for these three scenarios.

Resources for personal privacy

These tools are easy to implement and offer you more control over your personal data. This is the tip of the iceberg — you don't have to disrupt your internet routines too much to start protecting your information.

Check your passwords

Using the Secure Password Checker (password.kaspersky.com) from Kaspersky, an internet security company, you can visualize how easy a password is to hack. A short password, even if it looks like gibberish, is much easier to "brute-force" (in which a computer program tries all character combinations until it's guessed) than a longer, but more human-readable one. For instance, *3kc9E8* can be cracked in 3 hours, but *Privacy4Everyone!* would take 4 centuries. Of course, this is just one

instance of how your login could be cracked — this doesn't account for stolen passwords. So in addition to choosing a secure password, you should…

Make important accounts harder to hack

Most banks and email services now offer "two-factor authentication" (or 2FA), which, if enabled, require a password and some other security check to access your accounts. For instance, if you (or a hacker) try to log into your Google account on a computer you've never used before, Google will send a 6-digit code by text to your mobile phone. You must input this code on the login screen before proceeding. Other account-based services may offer 2FA as well. Check twofactorauth.org for lists organized by category.

Use plugins to see who's tracking you

There are a number of reliable, free browser plugins that visualize how websites track your browsing activity. These plugins simply display whether a website or an ad on the website has put a cookie (tracker) on your computer. Lightbeam (from Mozilla), Privacy Badger (from the Electronic Frontier Foundation), and Ghostery (from an ad firm that desires better internet advertising) are all reliable plugins that display tracking activity *and* give you the option to block some or all trackers. You may be surprised to see that many library databases use advertising trackers… Note: not all cookies are for advertising, and they usually don't log your personal information, just the browsing history of your computer. Still, it's a good privacy practice to clear cookies on a regular basis, if not block most outright. An added bonus: blocking trackers makes browsing faster.

Prune your mobile apps

As Gutermuth (2017) points out, apps don't always treat your personal information responsibly. For example, your location may be shared with third parties by an innocuous-seeming flashlight app. Even if you haven't opened an app in a long time, it may still be collecting data. On a regular basis, you should delete apps you don't use anymore and look at your privacy settings to see which data you've permitted each app to access.

Resources for a privacy-oriented library infrastructure

Now that you have changed some small things in your daily routine to take more control over your data privacy, perhaps it's time to look at your library or institution with new eyes. Libraries, of course, have historically prioritized patron privacy. With new technologies, however (and perhaps with decreased funding for new activities), some data privacy basics may have slipped through the cracks. The resources below provide tools and checklists that are useful for introducing librarians to data privacy in the library.

Library Freedom Project (libraryfreedomproject.org)

This energetic project team organizes privacy workshops for librarians focused on keeping libraries free of surveillance. Their website compiles many resources, from

the simple to the technologically advanced. The Library Digital Privacy Pledge is a good first step; it recommends that library websites implement HTTPS (rather than the less-secure HTTP) so that patrons can browse for materials on an encrypted site, without the worry of a third party monitoring what they search for or look at.

Data Privacy Project (dataprivacyproject.org)

This New York City-based project organizes workshops for librarians focused on data privacy and digital literacy. The workshops take a wide view of the "data flows" of the library, examining, for instance, what information is transmitted and to where when a patron downloads an ebook from a vendor. Though this IMLS-funded project is local to New York, the curriculum for their excellent module "Digital Privacy: Fundamental Concepts for Libraries" is available on their website under a Creative Commons license.

Library Privacy Checklists from ALA

The ALA's Intellectual Freedom Committee (2017) produced seven checklists focused on different library systems, from ebook vendors to OPACs. These audit-like checklists include detailed actions librarians might take to ensure that all systems are held to a high standard of patron privacy protection.

For more privacy resources for libraries, see Phetteplace (2017).

Resources for library patrons

As you reexamine your own privacy habits and those of your institution, your library's patrons may be asking questions as well. This is also a good chance to demonstrate the library's continued relevance to many aspects of patrons' interests. These resources are useful for organizing privacy workshops for patrons.

Data Privacy Project (dataprivacyproject.org)

In addition to the librarian-oriented materials highlighted in the previous section, the Data Privacy Project has also made curriculum for patron-focused workshops available on their website. The module "Digital Privacy: Hands-On Tactics and Tools for Libraries" is aimed at librarians who plan to share privacy tools with patrons.

Examples of privacy workshops offered in libraries

Cornell's Olin & Uris Libraries produced a three-part digital privacy workshop in spring 2017, splitting curriculum up into "Get Started with the Basics," "Encryption for Both Storage and Communication," and "Advanced Strategies for Greater Protection" (Kotaska 2017). Temple University Libraries organized a workshop in spring 2017 about "Protecting Your Personal Privacy in a Digital World" (Rowland 2017). New York Public Library (n.d.) routinely offers such workshops at branch libraries, including "Protecting Your Privacy Online" in English and Spanish. To see more examples, try searching the web with a query such as *library privacy workshop site:.edu*, which will display search results from academic websites, and *library privacy workshop site:.org*, which displays results from organizations.

References

Gutermuth, Lisa. 2017. "How to Understand What Info Mobile Apps Collect about You." *Slate*. February 24. http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html. Archived in the Internet Archive.

Intellectual Freedom Committee, American Library Association. 2017. "Library Privacy Checklists." *American Library Association*. http://www.ala.org/advocacy/privacyconfidentiality/library-privacy-checklists. Archived in the Internet Archive.

Kotaska, Robert. 2017. "Protecting Your Digital Privacy: A Series of Three Workshops : @ Olin & Uris Libraries." *@ Olin & Uris Libraries, Cornell University*. January 10. http://blogs.cornell.edu/olinuris/2017/01/10/protecting-your-digital-privacy-a-series-of-three-workshops/. Archived in the Internet Archive.

New York Public Library. n.d. "Classes & Workshops." *The New York Public Library*. https://www.nypl.org/events/classes/calendar.

Phetteplace, Eric. 2017. "Online Privacy in Post-Election America ACRL TechConnect Blog." *ACRL TechConnect Blog*. March 13. http://acrl.ala.org/techconnect/post/online-privacy-in-post-election-america. Archived in the Internet Archive.

Rowland, Fred. 2017. "Protecting Your Personal Privacy in a Digital World." *Human Sciences (A Temple Libraries' Blog), Temple University*. February 27. https://sites.temple.edu/humansciences/2017/02/27/protecting-your-personal-privacy-in-a-digital-world/. Archived in the Internet Archive.