# How Did We Get Here?

A
Zine About
Privacy at the
Library

In the early 20th century, when the library profession was debating privacy and its relationship to free speech, information about patrons flowed in a relatively simple manner. A patron communicated information about herself—her interests, beliefs, and values—in the process of borrowing a book. Book borrowing involved the library creating a paper record and storing it in its circulation records system.
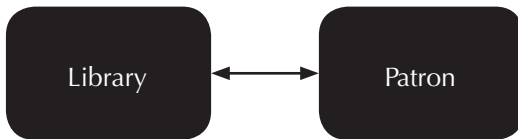
Over time, the library has evolved into a complex institution that is caught up in the flow of patron information in many different ways.
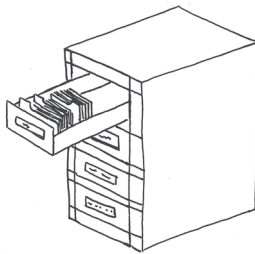
LAW

In the Sixties, libraries began experimenting with computer-based networking and automation of cataloging and circulation systems. These innovations led to further advancements in library information management systems for the purchasing, cataloging, and circulation of library holdings. Eventually, other database services would develop and become essential to institutional operations. Today, a great majority of library information management systems are commercially run, and libraries function as digital consumers reliant on third parties.
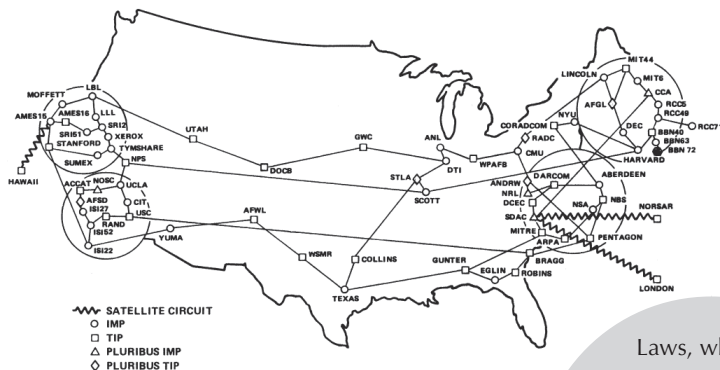
The ARPANET in 1980.

At the same time as these library modernization efforts, researchers were designing the proto-Internet. The next two decades saw the creation of protocols and standards that would lead to the creation of the Internet, email, and other networked communication tools.

By the time the commercial Web took off in the Nineties, policymakers and librarians were acutely aware of the transformative impact of the Internet and sought to eliminate the "digital divide." As a result, libraries began transforming into places that not only lent books, but also provided vital public access to the Internet.

Laws, whether at the local, state, or federal level, also shape the ways in which information about library users will be dealt with. Patrons as well as library workers can participate in regulatory debates about privacy policies that affect whether and how the library provides patron data to legal authorities. And lawmakers can institute policies that support privacy and data literacy at the library.

3

The transformation of libraries into *digital dependents* on third party services for information management and operations, on the one hand, and *digital providers* of computer and Internet services, on the other, complicates the goal of protecting patron privacy.
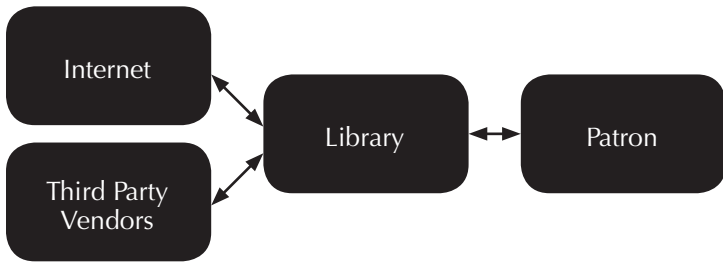

In their roles as digital providers, libraries generate new kinds of patron data. For example, they hold patron computer reservation data, because computer reservation management systems typically require users to authenticate their identity by entering their patron ID numbers.
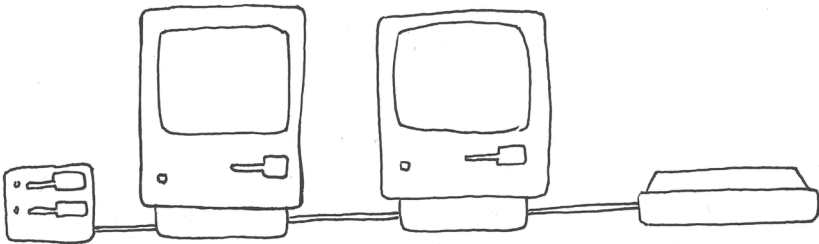
Libraries also hold Internet traffic data, collected by network management tools that are used to help administrators manage network performance and bandwidth usage, block particular types of IP addresses from using the network, or block access to certain domain names. In this context, like any institution that sets up and manages its own network, libraries today are faced with IT issues that shape conditions for patron privacy.

In their role as digital dependents, libraries contract services with third-party vendors who, in turn, generate new kinds of patron data. In this context, defending privacy also grows more complex. For example, services ranging from chat reference to periodical databases to "social" tools in the online catalog must capture patron information in order to function. This raises the possibility for security and other consumer privacy risks, such as use of patron data by third parties in ways patrons might not expect or desire.
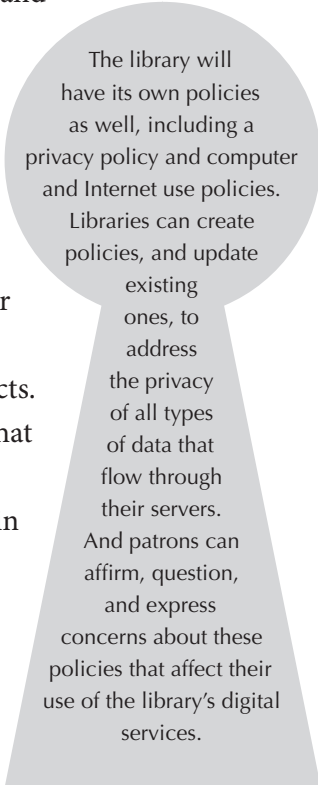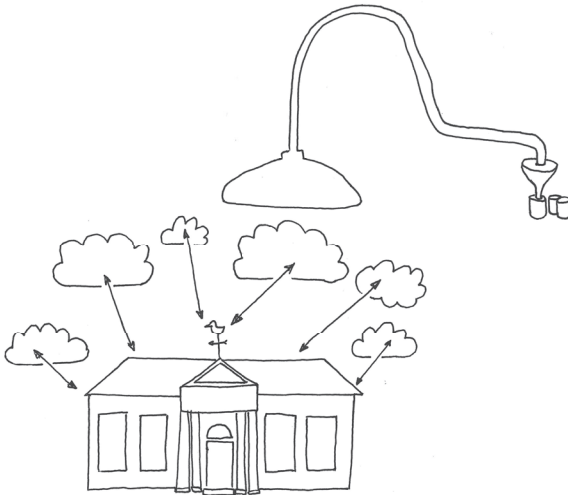
Third party management of patron data also raises questions about how this data can be protected from government surveillance, since government actors could request patron data from third parties that may have more lenient rules than libraries.
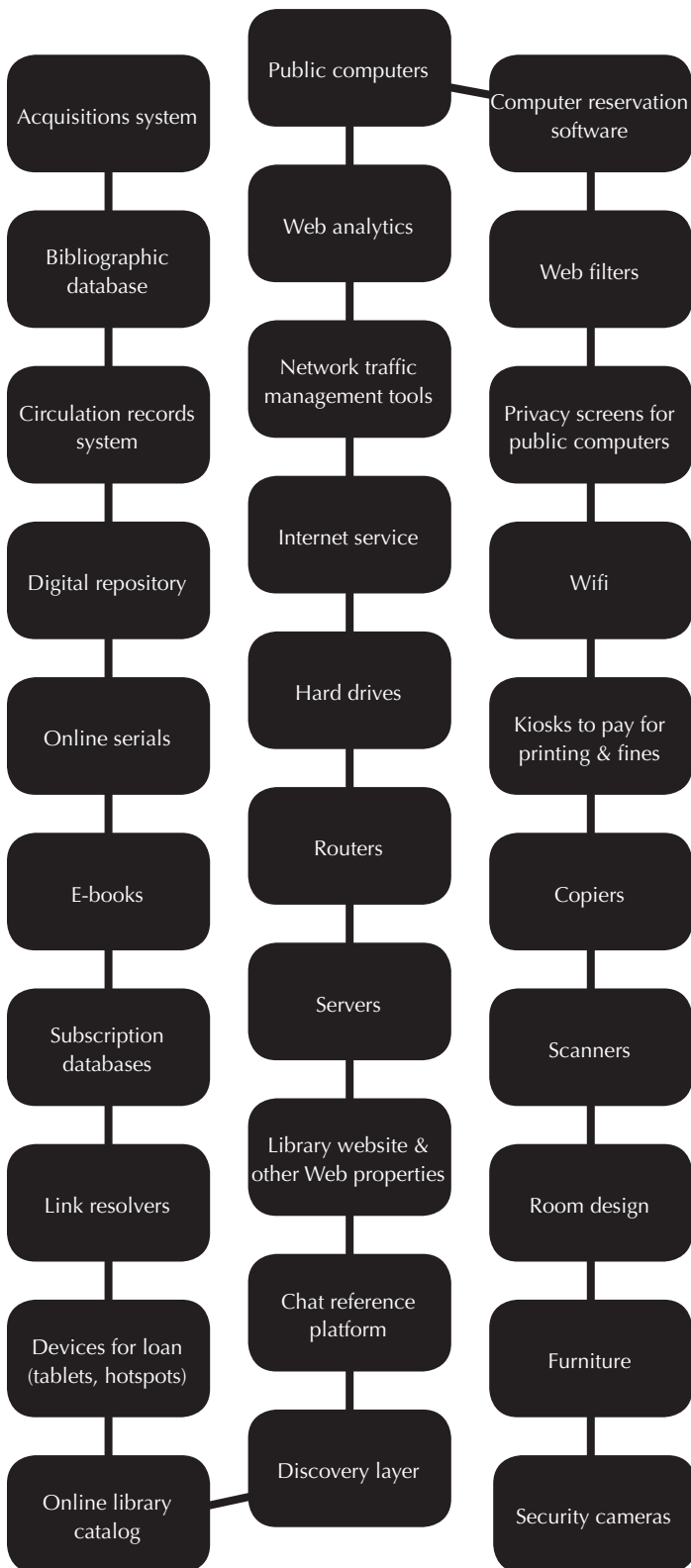
Of course, not all information about a library user is transmitted digitally. There are some physical considerations, such as the way a room is arranged, where computers are placed, and whether library staff or other patrons are able to see what a patron is doing, for example, on a computer screen. But by and large, many different pieces of a library's information architecture require *digital* information about a patron to function.

How many of these things can the library easily change and control in order to protect patron privacy? Arguably, the only items are furniture or physical objects. Public computers could be installed so that other patrons walking by can't easily see the monitors. A library might take certain measures to lock up routers and servers, so that no one could tamper with them.

The library will have its own policies as well, including a privacy policy and computer and Internet use policies. Libraries can create policies, and update existing ones, to address the privacy of all types of data that flow through their servers. And patrons can affirm, question, and express concerns about these policies that affect their use of the library's digital services.

Acquisitions system

Bibliographic database

Circulation records system

Digital repository

Online serials

E-books

Subscription databases

Link resolvers

Devices for loan (tablets, hotspots)

Online library catalog

Public computers

Web analytics

Network traffic management tools

Internet service

Hard drives

Routers

Servers

Library website & other Web properties

Chat reference platform

Discovery layer

Computer reservation software

Web filters

Privacy screens for public computers

Wifi

Kiosks to pay for printing & fines

Copiers

Scanners

Room design

Furniture

Security cameras

How many of these things can the library easily change and control in order to protect patron privacy?

Overall, the dual role of libraries as digital dependents and digital providers points to the complexity of protecting patron privacy. Privacy matters lie at the intersection of library policies; third party policies; local, state, and federal laws; social norms, values, and practices of library workers and patrons; and the technology itself.

As public conversation about privacy, data, and libraries evolves, the complexity of protecting patron privacy may subside. For now, we can identify both opportunities and challenges of patron data flows as they've changed over time.

A complex set of factors determines how information flows about patrons. As we have seen, much of the library's information architecture is run by parties other than the library.

Third parties could do something with patron data that a patron would not expect or desire, or the government might try to obtain this information from third parties. To mitigate these risks, the library can pressure third parties about their terms of service or introduce technology that lets patrons obscure personal information as it travels through the library's network.

CODE

Third party providers can adopt secure solutions that make data leakage of patron information less likely.

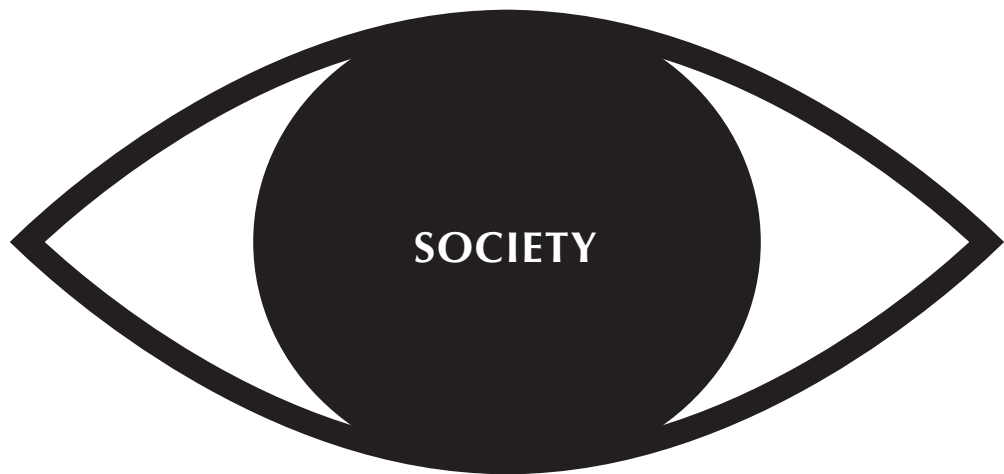Certainly, code—or the type of technology that a library implements—plays a role in privacy protection. For example, certain kinds of software encrypt or anonymize patron data to the extent that it's difficult to determine what a particular patron is doing on the Internet. Technologists can create privacy-protecting software that is effective and easy to use by people in the library—or in any setting.

Laws, whether at the local, state, or federal level, also shape the ways in which information about library users will be dealt with. For example, some state laws—like New York's Civil Practice Law and Rules section 4509—dictate that library records must be kept confidential.

A federal law, the Children's Internet Protection Act (CIPA), influences network management at many libraries. If the library receives funding through a federal subsidy program called E-rate, it must install filtering software on its network that (ostensibly) prevents minors from accessing harmful or obscene content on the Web.

Certainly, code—or the type of technology that a library implements—plays a role in privacy protection. For example, certain kinds of software encrypt or anonymize patron data to the extent that it's difficult to determine what a particular patron is doing on the Internet. Technologists can create privacy-protecting software that is effective and easy to use by people in the library—or in any setting.
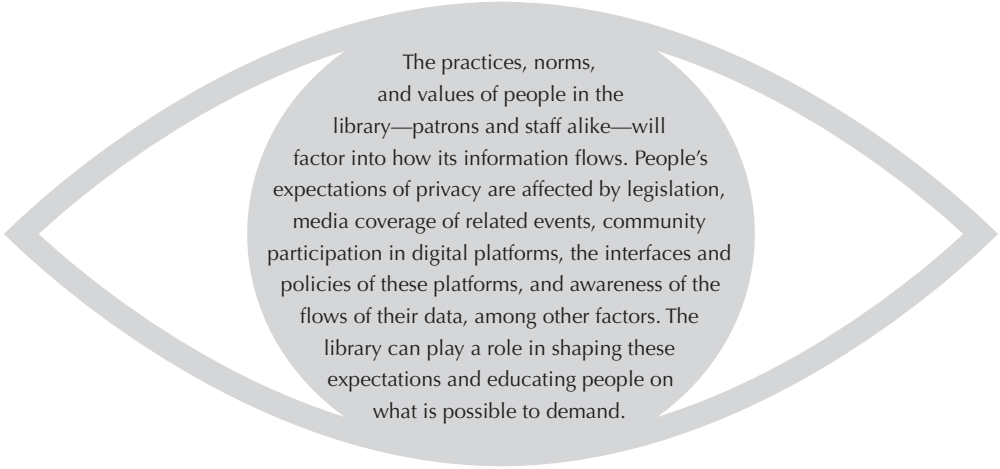
SOCIETY

Patrons as well as library workers can participate in regulatory debates about privacy policies that affect whether and how the library provides patron data to legal authorities. And lawmakers can institute policies that support privacy and data literacy at the library.

The library will have its own policies as well, including a privacy policy and computer and Internet use policies. Libraries can create policies, and update existing ones, to address the privacy of all types of data that flow through their servers. And patrons can affirm, question, and express concerns about these policies that affect their use of the library's digital services.

The practices, norms, and values of people in the library—patrons and staff alike—will factor into how its information flows. People's expectations of privacy are affected by legislation, media coverage of related events, community participation in digital platforms, the interfaces and policies of these platforms, and awareness of the flows of their data, among other factors. The library can play a role in shaping these expectations and educating people on what is possible to demand.

Finally, it's worth mentioning that the practices, norms, and values of people in the library—patrons and staff alike—will factor into how its information flows. For example, a library may provide open access to an unsecured wifi network so that patrons aren't hindered by a sign-in. Libraries may offer people the option of a guest pass for public computer access, which means they don't have to affiliate their identity with a specific member ID number.

People's expectations of privacy are affected by legislation, media coverage of related events, community participation in digital platforms, the interfaces and policies of these platforms, and awareness of the flows of their data, among other factors. The library can play a role in shaping these expectations and educating people on what is possible to demand.

This zine is based on the work of the Data Privacy Project and on the article "Library Privacy in Practice: System Change and Challenges" by Seeta Peña Gangadharan (*I/S* 13:1, 2017). For a deeper dive into this history—and present—with references, go to **moritzlaw.osu.edu/students/groups/is/files/2017/08/Gangadharan.pdf** and **zotero.org/dataprivacyproject/items**.

Seeta Peña Gangadharan, Melissa Morrone, Bonnie Tijerina, Davis Erin Anderson, and others are the people behind the Data Privacy Project. Inspiration for the project began in 2012.

Research done in part with collaboration from Brooklyn Public Library found that frontline library staff required training and support to better respond to patron needs regarding digital privacy issues. The Data Privacy Project was a two-part workshop series developed by Research Action Design (RAD) for NYC library staff in 2015-16 that covered how information travels and is shared online, what risks users commonly encounter online, and how libraries can better protect patron privacy. Funded by the Institute of Museum and Library Services, the project was led by a team of library professionals, researchers, tech experts, and community activists interested in the impact of technological advances on everyone, especially the most vulnerable populations in the U.S.

For more information about the project, plus online learning modules and full workshop materials, go to **dataprivacyproject.org**.

Zine design by Abigail Miller.

January 2018