FAQ: Privacy, Security, and Data Protection at Libraries

This FAQ was developed out of workshops and meetings connected to the Digital Privacy and Data Literacy Project (DPDL) and Brooklyn Public Library's past work on privacy and digital inclusion.

It provides basic information for librarians interested in: 1) general consumer privacy issues, 2) privacy issues specific to libraries' network and data management practices, and 3) privacy issues that relate to third party vendors commonly used by libraries.

Because this FAQ was created for and by librarians, we sincerely hope you will use it in your everyday work. Whether to learn something new or to advise patrons who come to you with questions, this FAQ can provide you with easy answers.

We also invite you to add to the FAQ by submitting your own questions and answers.

GENERAL CONSUMER PRIVACY QUESTIONS

Web Privacy, Security

- If I close a window, does that log me out of a website?

    No. Whenever you enter a username and password on a website, it means that you are logged in. To close out your business on that site, you need to log out. Look for parts of the website that say "Sign out" or "Log out," which might be in one of the upper corners of your screen. Google and some other programs hide this function behind a dropdown menu.

- Why do I see the same advertisements when I'm at home on my laptop and when I'm at the library on a library computer?

    A cookie can record information such as a user name and track a user who logs in across different devices. A cookie is a file that a website saves to your computer after you visit the site and allows it to understand your browsing activities on that site—such as what personal data you entered onto a site, what you put in your online shopping cart, which links on a website you clicked on, or what you searched for. Cookies create a profile of your online activities and help a site "remember" what you did so that when you go back to it, it can present you relevant content and advertising, even if you log in on a different device.

- How do I know if a website is real or fake?

    Many websites contain inaccurate and potentially harmful information. Essentially, a website that is not likely to be unsafe to you or to your finances is one that isn't trying to hide what it really is. There should be a section of the website itself called "About" or "About Us" that explains who is

behind the site. If a website makes it hard to figure out who created it and why, you should think twice before believing anything it says.

- What is a strong password?

To create a secure password, aim for something long and complex. For example, come up with a sentence that is easy for you to remember. Then eliminate the spaces between the words, change the spelling of the words or use only the first letter of each word, add numbers and symbols to make it longer. Try to use a different password for different email or other online accounts—or at least use a couple different passwords. Write down passwords on a piece of paper and store in a place under lock and key that can't be accessed by others—like a safety deposit box.

- What kinds of information count as personal or sensitive?

The address where you live. Usernames. Account numbers. Passwords and personal identification numbers (PINs). Social Security numbers. Birth dates. Your mother's maiden name and similar verification information.

- What are privacy settings?

Privacy policies are part of a site's terms and conditions. They tell you what information the site collects about you, how your information will be used, and who else may be able to access your information. Default privacy settings represent the basic level of privacy that a website has automatically set for new users. Each website has different privacy policies and settings, so it's a good idea to check them out before you start using a site.

- How do websites know where I am?

Websites can see your IP (Internet Protocol) address, a numerical label assigned to your device, and guess your physical location based on this. Location information is data taken from the GPS (Global Positioning System) on your smartphone, laptop, or digital camera that identifies where in the world you are when you post something or take a picture.

- When I'm on the welfare office's website, why does it ask me so many questions about me?

Government agencies collect information in order to determine whether applicants meet the right criteria for acceptance into a program like unemployment, food stamps, or housing benefits.

- If someone got ahold of my email password, would they be able to steal my identity?

If you use the same password for several different accounts, a sophisticated hacker may be able to steal your identity.

- How do I know if a website is secure?

Look for the address to begin with "https" or a lock symbol. That means the page of that website is encrypted.

- How do I know what information I am supposed to provide online when filling out forms? How much is too much information?

Sometimes we don't really have a choice about putting our personal information online. Many government functions, such as applying for benefits, are conducted over the Internet now. We may also have online accounts with our banks and health providers, or to request financial aid for school, or to apply for a job. Government agencies and financial institutions are much less likely to ask you to provide information that will compromise your safety.

In other situations, we have options about whether we need to conduct a transaction online or not. Use your judgment about whether you should trust a website that's asking for your Social Security number or credit card information. And remember that you don't need to trust every website with equal amounts of information. You can choose not to give your real name when you open a new email account, or not to give your real birthday when you create a profile on a social networking site. With your doctor's office, it's a different story!

LIBRARY-SPECIFIC QUESTIONS

Library Filters

- What is a content filter?

A filter is a way to choose which types of websites can be viewed on a computer. The filter can be set to allow or restrict certain categories of websites based on their content, and all sites are automatically scanned and categorized by the filter software.

- Why do libraries use content filters?

Certain laws require libraries to install filtering software on computer terminals that are accessible to minors. For example, the Children's Internet Protection Act and the Neighborhood Internet Protection Act requires that funding recipients of the Library Services and Technology Act, Title III of the Elementary and Secondary Education Act, and the Universal Service discount program known as the E-rate (Public Law 106-554) implement Internet safety policies and install software that blocks or filters certain Internet content from being accessible by minors.

The filter also protects library computers from websites that download malicious software, pose security risks, or could otherwise harm a library's network. It further protects patrons by blocking websites known for fraud or phishing scams.

Patron Circulation Records

- Do libraries keep lists of what patrons check out?

Typically, once physical items are checked back into a library's system, a library will not keep the

history of who checked it out unless there is a fine associated with the item. Records of digital item checkouts depend on each vendor's policy.

Public Computer Use

- Is a patron's information safe on a public computer?

  Though libraries typically follow best practices to guard against unauthorized access, libraries cannot guarantee the safety of information transmitted over the Internet.

- When a patron logs off a public computer before signing out of her email or other personal account, can a library or the next user see her email or files?

  Typically, once the computer session ends automatically or the patron logs off, all session user activity is closed and will not be accessible to anyone logging in after them. In addition, all "temporary" patron files should be deleted and all of the computer's settings should be restored to the default. That action deletes all temporary data, such as cookies, temporary browser history including form data and sites visited, and downloaded files. Patrons should ensure they manually log off the computer if they decide to end their session before their time is up.

Privacy and Security of the Library's Wireless and Wireline Networks

- If a patron uses a credit card on a public computer, can someone steal her identity?

  While libraries exercises best practices to protect their systems from unauthorized access, they cannot guarantee the safety of information transmitted over the Internet.

- What can happen on an open wireless network (Wi-Fi)? Is there anything a patron can do to increase her security while on it?

  The convenience of an open wireless network (one that does not require a password) is often offset by its lack of security. Some common ways to improve security are:

      I.   Ensure the security software on your computer/device is up-to-date

      II.   Try to avoid browsing sites that require you to login with your username and password, or ensure the website(s) start with HTTPS, which is more secure

      III.   Never install software while on an open wireless network.

- What is phishing or other fraud schemes, and how should a patron respond to them?

  Phishing email messages, fraudulent websites, and so on are designed to steal personal information. Patrons should be wary of:

      I.   Emails with spelling errors and bad grammar

      II.   Suspicious links in email

      III.   Fake alerts, such as warnings of accounts being closed.

- When using a site that requires you to enable pop-ups, is your information shared or compromised?

  While many sites that require enabling pop-ups are seeking to provide more information, users should exercise caution by considering the site in question. Pop-ups can be used to install

adware and other unwanted software, which can also slow down the performance of the computer and speed of the Internet.

QUESTIONS RELATED TO THIRD PARTY SERVICES

Third Party Service Agreements
- How long do the vendors used by the Library keep data they receive from staff and patrons?

Third parties have their own specific policies regarding privacy protection. Here is a list of examples of various privacy practices of a variety of vendors.

EBSCO: EBSCO tracks your institution's usage by IP address, but does not track usage by individual bar code or username. The IP address report also does not show what resources were accessed, only how many search sessions did a particular IP address generate for a particular time period.

In this way, there is no way to track what databases a particular library staff member or patron searched, or how many. You can only track, library-wide, statistics on the databases themselves (searches, sessions, full text records accessed, etc.)

ProQuest: ProQuest defines personally identifiable information as information that, if collected and reviewed, could uniquely identify you, or in some cases, be used to locate you ("Personal Information"). For instance, your full name, coupled with your email address, is likely to personally identify you. Under the law, Personal Information is defined broadly and may include, for example, your full name coupled with other information, such as a national identification number (like a social security number), an IP address, your mobile phone number, your birth date, and/or your residence address could also be defined as Personal Information.

ProQuest uses cookies in a variety of different ways, including allowing you to store your password so that you may access the ProQuest Sites without having to enter certain authenticating information each time. We may also use cookies or other technology to allow you to see, track and/or store such information as your log in information, previous searches and/or research sessions, databases accessed, and other information.

OverDrive: OverDrive may collect certain information about patron's interactions with them and information related to the patron and your use of OverDrive's services, including but not limited to, Personal Information, your online activity, digital content selections, reviews and ratings, as well as Internet Protocol addresses, device types, unique device data, such as device identifiers, and operating systems.

"Personal Information" describes information that can be associated with a specific user and used to identify that person, for example, full name (first and last); a home or other physical address,

including street name and city or town; telephone number; or online contact information, such as an email address or screen name. Personal Information, specifically your name and email address, will be submitted by you when you create, access, and use your OverDrive account. Other information, that is not Personal Information, may be collected automatically by creating, accessing, or otherwise using your OverDrive account.

Individuals under the age of 13 are not permitted to create, access, and use an OverDrive account, and we do not intentionally collect or maintain Personal Information from those who are under 13 years old. By using our Services, you are representing that you are at least 13 years old.

QuestionPoint: For its own purposes, the library using this underlying QuestionPoint 24/7 Reference service may ask patrons to provide name, email address, ZIP code, telephone number, library card number, and other information. While this data is not required for our service to function, the library may be better able to answer questions and deliver more relevant content if the patron volunteers complete and accurate information. Email addresses allow the library to answer questions via email. Full email address is not used for any other purpose, though the domain (the portion after the @ sign) may be used for demographics analysis.

Any personal information collected is disclosed only to the extent necessary to fulfill the request for information. For example, the library may need to refer a question to a librarian in its network, who will have access to your information in order to answer your question and communicate with the patron. OCLC does not provide personal information to any party except as required to do so by law.

3M Cloud Library: Login Information. We use the identification information you provide and email address, if you provide one, that you use when you log in to the Services to create your 3M Cloud Library account, which stores information about checked out materials and lets you access them from other devices. 3M also transmits this information to your library to validate your library account. We may also use this information to contact you regarding your account.

Content of Bookmarks. When you create Bookmarks using the App, they are stored on 3M servers so that you can access them from other devices. 3M will access the content of your Bookmarks only as necessary to verify compliance with the Terms of Service and as required by applicable law.

Location Information. The Services do not collect, use or store the location of a mobile device.

Usage Data. The Services may collect anonymous information relating to the performance of the App, such as application crashes. We use this information in order improve our applications and

services. We do not collect personally identifiable information as part of usage data or crash information.

Other Information. 3M collects and stores additional information relating to your use of the Service, such as your book lending history, your reading position in a book, your bookmarks, your library and library identifier, authentication information and any rating related to the book you provide and your email address, if provided. To aid in the analysis of this information, it is associated with your mobile device through a random number generated when you install the App. However, this information is not otherwise associated with your identity or account information and is collected and used on an anonymous basis. We may use this information for business purposes, such as customer service, fraud prevention, market research, improving our products and services, and for historical, statistical or scientific purposes.

- I have library cards from different libraries using BiblioCommons. Does BiblioCommons keep my data from all these libraries? What data? For how long?
  BiblioCommons: https://support.bibliocommons.com/hc/en-us/requests/19164

  BiblioCommons does not store checkouts, past holds, or recently returned items unless the patron enables the Borrowing History feature. BiblioCommons retrieves that information from the respective Library's integrated system (ILS) when the patron signs in. When the patron signs out, that information isn't stored by BiblioCommons.

  BiblioCommons does store a patron's name, library barcode, PIN/password, and patron number. If your date of birth and email address is in the ILS, or you provide it to BiblioCommons during registration, they store those too. BiblioCommons stores all user-generated content, such as book reviews. But they do not have patron addresses or phone numbers.