ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

DECEMBER 5, 2016 | BY GENNIE GEBHART AND KERRY SHEEHAN

Librarians, Act Now to Protect Your Users (Before It's Too Late)

Books checked out from a library and terms searched on library computers can reveal a teenager's questions about sexual orientation, a neighbor's religious leanings, or a student's political interests. Libraries across the country, particularly public libraries, make it part of their mission to serve the most vulnerable and underserved user groups, including users who are homeless, unemployed, or recent migrants or refugees. And when government agents come looking, these library users need librarians to have their back.

Libraries and librarians have long been stalwart guardians of the rights of free expression and inquiry. As part of their profession, librarians protect their users' ability to access even the most controversial information and ideas free from government scrutiny. Since the passage of the Patriot Act in particular, librarians have purged user records when necessary to fight against unconstitutional government demands and pushed back against (unconstitutional) National Security Letters (NSLs). Librarians also stood with EFF and the ACLU when we worked to pass the California Reader Privacy Act in 2011.

With the recent election of President-elect Donald Trump, many libraries are rightfully worried about a renewed a threat to their users' privacy. If the incoming administration sticks to its promises to identify and deport millions of people, monitor individuals based on their religious beliefs, and expand libel laws, for example, libraries could receive unprecedented government requests for information on their users.

To that end, we recommend libraries ensure they're taking the following steps as soon as possible to protect their users' intellectual privacy. In addition, libraries have to think beyond their own actions and take steps to ensure that all of their third-party vendors provide the same level of protections to users that libraries themselves do.

1. Limit collection and retention of user information

The less information you collect about your users, the less you have to surrender. The best policy is to collect the minimum amount of information necessary to provide a particular service, and don't retain that information any longer than necessary. For example, delete check-out information as soon as a book is returned. Further, make a regular habit of purging your logs (including circulation records, event attendance records, computer use and activity logs, search records, Wi-Fi connection logs, database searches, etc.) using a secure deletion utility. If you do need to retain certain records—for example, usage records for resource allocation or funding advocacy—then follow best practices to de-identify and anonymize them to the greatest extent possible.

When you do collect user information, make sure your users are notified about that information collection and offered the option to affirmatively opt in. Further limit data collection by allowing pseudonymous or anonymous use of library services wherever possible. For example, allow people to use library computers without a personalized login, and don't require logins on library web services unless it's necessary to access a user account. Similarly, leave the library Wi-Fi network open, don't keep logs of IP addresses, and ensure your network deletes connection logs immediately after log-off.

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more about what the program is, how it works, and what you can do.

Follow EFF

Librarians play a critical role in safeguarding our privacy and freedom of expression from government data requests. https://www.eff.org/deeplinks

DEC 5 @ 1:55PM

Mexican civil society denounces arbitrary government surveillance at the IGF 2016 #InternetEsNuestra https://articulo19.org/mexica

DEC 5 @ 11:30AM

Data reporters at @FiveThirtyEight examined the FBI's National Security Letter numbers https://fivethirtyeight.com/f...

DEC 5 @ 11:19AM

Twitter Facebook Identi.ca

Projects

Make sure library operated websites and services aren't logging user IP addresses, and if so, purge them quickly and regularly. Educate users about any differences between services provided in the library versus those services accessed remotely—for example, services accessed via library computers will only see the library's IP address, while remotely accessing services can expose a user's own IP address.

2. Maintain policies and procedures for responding to government requests and for notifying users of requests received

Communicate with users about how you will respond to requests for their information. Government requests for information may come in a variety of forms, from simple requests without a warrant or court order, to subpoenas, warrants, and NSLs. Policies must clearly dictate how library staff should respond to each of these requests. Make sure your staff knows how to handle requests for user information.

Note that, without a warrant, court order, or NSL, libraries are not required to provide user information, and may refuse to comply. While search warrants may be carried out immediately, all government requests for information may be examined by library counsel for legal defects. If you receive a request for patron information you should contact an attorney. EFF stands ready to help libraries sort through their options when they receive suspect legal process.

Policies should also address how and when users will be notified of government requests for information. In response to government requests accompanied by a gag order, some libraries, like the Internet Archive and the Library Connection, have fought to lift the gag. Again, EFF stands ready to assist.

3. Maintain accurate, accessible privacy policies, and notify users when they change

A library's privacy policy should, at a minimum, tell users what types of information are collected, how long that information is stored, how it may be used, and who may access it under what conditions. Users should be immediately notified of any changes to library privacy policies, and should have an opportunity to opt in to continued use of affected services.

But the library's privacy policy alone may not cover all of the catalogs, databases, e-books, checkout systems, and other third-party services a user may encounter in the library. At a minimum, users should be alerted when they are interacting with a third-party vendor, and should be notified of those vendors' privacy policies. Libraries should also allow users the opportunity to affirmatively opt in to services that do not allow the same privacy protections as the library—or, even better, wherever possible libraries should require third-party vendors to match their privacy practices. (See EFF's privacy policy as an example.)

4. Use HTTPS for your whole website at all times, and push your vendors to do the same

While many libraries already use HTTPS on parts of their websites, this strategy is ineffective at securing user information. Use a service like Certbot to migrate your *entire* website to HTTPS, and push your third-party vendors—including e-book vendors—to do the same. Without such protections, your users' information may be at risk in-transit and vulnerable to anyone logged onto the same network.

In addition, you should limit the use of cookies used to track users' preferences and activities. If your website does use cookies, allow users to affirmatively opt in to accept the cookie. Don't condition access to your site on acceptance.

5. Secure library computer browsers

Unsecure browsers can leak information about what users are doing online—including the searches they run and websites they visit—providing a detailed picture of their online activity. Library computers should default to browsers with built-in privacy protections, like Mozilla Firefox or Google Chrome. Enable privacy-protective tools and extensions like EFF's Privacy Badger and HTTPS Everywhere, and update both the browsers and extensions whenever an update becomes available.

6. Require third-party vendors to match library privacy practices for patron data

Bloggers' Rights

Coders' Rights

Free Speech Weak Links

Global Chokepoints

HTTPS Everywhere

Manila Principles

Medical Privacy Project

Open Wireless Movement

Patent Busting

Privacy Badger

Student Activism

Student Privacy

Surveillance Self-Defense

Takedown Hall of Shame

Teaching Copyright

Transparency Project

Trolling Effects

Ways To Help

As noted above, libraries today use an increasing number of third-party vendors who have access to user data. Libraries must work to ensure that their third-party vendors adopt practices and policies in line with libraries' own privacy policies. Third-party services can track, collect data about, and analyze user behavior—and that information can in turn be demanded by law enforcement. This can include highly sensitive user information, like name and account identifiers, IP addresses, demographic information, search history, and reading history.

Librarians can also take control of how they use and present third-party services, including configuring default settings in as privacy-protective a manner as possible and conducting regular reviews of privacy practices and options.

In addition, analytical and behavioral profiling services can pose particular risks for users—producing detailed records of users' identities, reading habits, and behaviors. Avoid allowing these services to access user information without obtaining users' explicit, opt-in consent.

Looking to libraries

As the new administration takes office in January, we will need librarians more than ever. We need them to safeguard our access to information and our intellectual privacy. We need them to limit the amount and specificity of data available about users. We need them to fight back against government requests for user information.

And now it's essential that all librarians go beyond these crucial steps to consider the full range of threats to their users' privacy, and act to protect that privacy in a changing environment. We applaud libraries for the work they're already doing, and urge the entire library community to take additional action before it's too late.

National Security Letters Privacy Free Speech

MORE DEEPLINKS POSTS LIKE THIS

MAY 2015
What Every Librarian Needs to Know About HTTPS

FEBRUARY 2012
Comparing Privacy and Security Practices on Online Dating Sites

NOVEMBER 2015
New Report Rates Peruvian ISPs: Who Defends Your Data?

DECEMBER 2010
2010: E-Book Buyer's Guide to E-Book Privacy

JUNE 2015
New Report Shows Which Mexican ISPs Stand With Their Users

RECENT DEEPLINKS POSTS

DEC 5, 2016
The World Wide Web Consortium at a Crossroads: Arms-Dealers or Standards-Setters?

DEC 5, 2016
Librarians, Act Now to Protect Your Users (Before It's Too Late)

DEC 4, 2016
San Franciscans: Help Protect Your Right to Choose Your Internet Service Provider

DEC 2, 2016
The Problem of Our Surveillance Laws: Report Exposes Deeply Rooted Governmental Secrecy—Underscoring Why Obama Should Act Now

DEC 1, 2016
Fighting NSL Gag Orders, With Help From Our Friends at CREDO and Internet Archive

DEEPLINKS TOPICS

Fair Use and Intellectual Property: Defending the Balance
Free Speech
Innovation
UK Investigatory Powers Bill
International
DRM
E-Voting Rights
EFF Europe
Electronic Frontier Alliance
Encrypting the Web
Export Controls
FAQs for Lodsys Targets
Patents
PATRIOT Act
Pen Trap
Policy Analysis
Printers
Public Health Reporting and Hospital Discharge Data

- Know Your Rights
- Privacy
- Trade Agreements and Digital Rights
- Security
- State-Sponsored Malware
- Abortion Reporting
- Analog Hole
- Anonymity
- Anti-Counterfeiting Trade Agreement
- Artificial Intelligence & Machine Learning
- Biometrics
- Bloggers' Rights
- Border Searches
- Broadcast Flag
- Broadcasting Treaty
- CALEA
- Cell Tracking
- Coders' Rights Project
- Computer Fraud And Abuse Act Reform
- Content Blocking
- Copyright Trolls
- Council of Europe
- Cyber Security Legislation
- CyberSLAPP
- Defend Your Right to Repair!
- Development Agenda
- Digital Books
- Digital Radio
- Digital Video
- DMCA
- DMCA Rulemaking
- Do Not Track
- File Sharing
- Fixing Copyright? The 2013-2016 Copyright Review Process
- FTAA
- Genetic Information Privacy
- Government Hacking and Subversion of Digital Security
- Hollywood v. DVD
- How Patents Hinder Innovation (Graphic)
- ICANN
- International Privacy Standards
- Internet Governance Forum
- Law Enforcement Access
- Legislative Solutions for Patent Reform
- Locational Privacy
- Mandatory Data Retention
- Mandatory National IDs and Biometric Databases
- Mass Surveillance Technologies
- Medical Privacy
- Mobile devices
- National Security and Medical Information
- National Security Letters
- Net Neutrality
- No Downtime for Free Speech
- NSA Spying
- OECD
- Offline : Imprisoned Bloggers and Technologists
- Online Behavioral Tracking
- Open Access
- Open Wireless
- Patent Busting Project
- Patent Trolls
- Reading Accessibility
- Real ID
- Reclaim Invention
- RFID
- Search Engines
- Search Incident to Arrest
- Section 230 of the Communications Decency Act
- Shadow Regulation
- Social Networks
- SOPA/PIPA: Internet Blacklist Legislation
- Student Privacy
- Stupid Patent of the Month
- Surveillance and Human Rights
- Surveillance Drones
- Terms Of (Ab)Use
- Test Your ISP
- The "Six Strikes" Copyright Surveillance Machine
- The Global Network Initiative
- The Law and Medical Privacy
- TPP's Copyright Trap
- Trans-Pacific Partnership Agreement
- Travel Screening
- TRIPS
- Trusted Computing
- Video Games
- Wikileaks
- WIPO
- Transparency
- Uncategorized

Thanks | **RSS Feeds** | **Copyright Policy** | **Privacy Policy** | **Contact EFF**