Public Libraries Leading the Way

On Educating Patrons on Privacy and Maximizing Library Resources

T.J. Lamanna

ABSTRACT

Libraries are one of our most valuable institutions. They cater to people of all demographics and provide services to patrons they wouldn't be able to get anywhere else. The list of services libraries provide is extensive and comprehensive, although unfortunately, there are significant gaps in what our services can offer, particularly those regarding technology advancement and patron privacy. Though library classes on educating patrons' privacy protection are a valiant effort, we can do so much more and lead the way, maybe not for the privacy industry but for our communities and patrons. Creating a strong foundational knowledge will help patrons leverage these new skills in their day to day lives as well as help them educate their families about common privacy issues. In this column, we'll explore some of the ways libraries can utilize their current resources as well as provide ideas on how we can maximize their effectiveness and roll new technologies into their operations.

Though many libraries have policies on how they deal with patron privacy, unfortunately some policies aren't very strong and oftentimes staff isn't trained in the details of these policies. Fortunately, for libraries who don't have these necessary policies, there are some, such as the San Jose Public Library, that offer their own as a framework.[1] Those that do have a strong comprehensive policy must make sure they are enforcing and regularly updating it to comply with new technologies being released. It's a daunting task, but as Article VII of the Library Bill of Rights says, "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information."[2] This means we have a responsibility to our patrons to do everything in our power to protect them and teach them to protect themselves.

This requires a concerted effort not just for technology and IT librarians, but for all library workers. A privacy policy means little if those on the front lines are either unaware of the policy or unsure how it is to be implemented. Therefore, all library staff should both understand the fundamental reasons behind library privacy policies and be trained in maintaining them. Libraries may consider implementing this training during staff development days or offer independent training sessions as needed.

Since the introduction of the Patriot Act, libraries stopped collecting patrons' reading habits, but so many library integrated library systems (ILS) snag massive amounts of patron information we are unaware of. I've been administering our ILS for over two years and I just found another space where items are being unnecessarily retained that I didn't notice before. An instance such as this calls for limiting personally identifiable information (PII) to what is strictly necessary.

T.J. Lamanna (professionalirritant@riseup.net) is an Adult Services Librarian, Cherry Hill Public Library.

In limiting the PII gathered in the first place, library staff should consider the following questions: What information do libraries really need to collect to offer library cards or programming? Does your library really need patrons' date of birth or gender? Probably not. If so, you shouldn't be collecting it, and if you do, make sure you anonymize the data. Using metrics is vital to how libraries function, receive funding, and schedule programming. You can still use the information, but it should not be connected to a patron in any way.

After educating staff, we can educate patrons on developing better and safer practices regarding personal privacy and security in their daily lives. Practical examples range from teaching patrons how to create strong passwords and backup sensitive files to explaining how malware works and what the "cloud" actually is. This is a start, but it goes far beyond that. I've served many patrons who, even after taking courses on the subject, are overwhelmed by the security measures needed to protect themselves. This isn't necessarily a sign that our classes are ineffective, but it does imply that new tactics are needed. Let's look at a few examples.

Another version of PII that we often overlook are security measures such as closed-circuit television (CCTV) or security/police officers in our buildings.[3] They often are either forgotten or outside the purview of the library itself. As the College of Policing states, "CCTV is more effective when directed at reducing theft of and from vehicles, while it has no impact on levels of violent crime."[4] While there are justifications for bringing this technology into the library, they should only be set up where needed, taking great care not to point them at patron or staff computers. If CCTV is needed, make sure to follow local retention laws and remove the footage as soon as its time has expired. This idea applies to all collected information. There is no reason to archive data beyond the date they can be destroyed as it puts the library and its patrons in a compromised position.

Law enforcement in the library is a tough thing to argue against in our current political climate. But studies have shown that police presence does little to deter crime and may actually disproportionately impact marginalized communities.[5] Consider the purpose of law enforcement personnel and if their presence is actually necessary to the proper functioning of your library. In the event that you should have law enforcement come in with a subpoena that requires you to turn over your patron data, it's important to have a canary warning that can be removed so your patrons understand what has happened.[6]

Another way libraries can lead the way in protecting patron privacy both inside and outside the library is by supporting legislation that bans facial recognition software. This type of technology is becoming ubiquitous, but places have already started pushing back and libraries can be the epicenter of this movement. It's already been banned in Oakland,[7] San Francisco[8] (one of the homes of this technology), as well as Somerville, Massachusetts, with groups like the Massachusetts Library Association unanimously putting out a moratorium on facial surveillance, which is the practice of recording ones face to create user profiles.[9] There are other states that are working down this path and it's overwhelmingly heartening to see libraries step up and in front of something they know would damage our communities. We ought to be activists, standing on the front lines and showing our patrons our deepest commitment to them.

Surely there are greater strides we can make, such as revising WiFi policies. WiFi is one of the most used services libraries offer and many libraries don't use it to their full potential. For instance, some libraries turn off their WiFi when the building is closed, severely limiting patrons' usage. It's a service we pay for and there is no reason it shouldn't be available at all times. Your IT service should make sure the WiFi is secure (it should be where it's available at all hours or not). Unlimited access to WiFi becomes invaluable to users who need it for emergencies including completing work or accessing important online services when the library is closed. While we do have limited bandwidth and IT services must actively maintain WiFi security, libraries should make sure it's available to the public as often as possible.

Now that we've covered using bandwidth when we aren't open, let's talk about libraries with excess bandwidth. No resource should go unused in the library. We have a limited budget and we should make sure every penny is used to serve our communities. One fantastic use of excess bandwidth — especially during closed hours — would be to set up a Tor relay in your library, an anonymity network that allows people to surf the internet with extra security and privacy in mind. It's quite easy to set up and you can limit how much bandwidth it uses so you aren't shorting anyone in your library. It's a service used by groups such as journalists or activists who want to make positive change in the world and need a safe place to do so. Some are concerned that the Tor network is used for malicious intent but the Tor Project, the organization that runs the network, constantly works to ensure nothing like that is taking place. Also, anything solicitous you can find on the Tor network is available on the regular internet including places like Facebook or Craigslist, so the stigma of the network should be taken in context. The Tor Project routinely monitors the network and searches out illegal material (there are no hired killers on the Tor network). Given all this, you could help the network greatly by just partitioning a small amount of your bandwidth.

Libraries have the unique ability to be transformative. Unlike other non-profits or organizations, we have the ability to *pivot*. We can both change directions as needed and pave the way for our communities as leaders in the movement toward patron privacy. I leave you with a quote from Hardt and Negri: "...we share common dreams of a better future."[10] That should be our motto.

ENDNOTES

[1] "Our Privacy Policy, San Jose Public Library, accessed August 15, 2019, https://www.sjpl.org/privacy/our-privacy-policy.

[2] "Library Bill of Rights," American Library Association, last modified January 19, 2019, http://www.ala.org/advocacy/intfreedom/librarybill.

[3] "Importance of CCTV in Libraries for Better Security," accessed August 14, 2019, https://www.researchgate.net/publication/315098570_Importance_of_CCTV_in_Libraries_for_better_security.

[4] "Effects of CCTV on Crime," College of Policing, accessed August 14, 2019, http://library.college.police.uk/docs/what-works/What-works-briefing-effects-of-CCTV-2013.pdf.

[5] "Do Police Officers in School Really Make Them Safer?" accessed August 14, 2019, https://www.npr.org/2018/03/08/591753884/do-police-officers-in-schools-really-make-them-safer.

[6] "Canary Warning," Wikipedia https://en.wikipedia.org/wiki/Warrant_canary.

[7] Sarah Ravani, “Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns,” *San Francisco Chronicle,* July 17, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

[8] Kate Conger, Richard Fausset, and Serge F. Kovaleski, “San Francisco Bans Facial Recognition Technology,” *New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[9] Sarah Wu, “Somerville City Council Passes Facial Recognition Ban,” *Boston Globe,* June 27, 2019, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html.

[10] Michael Hart and Antonio Negri, *Multitude: War and Democracy in the Age of Empire*, (New York: The Penguin Press, 2009), p. 128.