

Refusal as Instruction

Equipping Patrons to Resist AI, Data Brokers, Big Tech, & More

Hannah Cyrus

A PATRON WALKS IN FOR ASSISTANCE...

Picture a common scene in a public library setting: a patron comes into the library and asks for help creating an email address in order to apply for a job, make an account to receive a needed benefit, submit documentation to an agency, or one of a host of other reasons. The patron has never used email before (and doesn't want to!), but things have gotten to the point where it's unavoidable for them—an email address is now required for them to meet their basic needs.

If the patron doesn't express their own preference for what email service they'd like to sign up with, library workers might take the path of least resistance and choose an email provider that seems so ubiquitous as to feel "neutral," which is typically Gmail. If they are conscious of a patron's privacy needs, that library worker might take the time to uncheck the boxes that Gmail automatically selects, so as to limit the amount of data that is voluntarily shared with Google during account creation. Beyond that, the patron might get a quick tutorial on how to use email before moving on to the task they actually wanted to do: their application or account creation elsewhere.

None of this feels unreasonable when getting through the day-to-day demands of providing library services, but when stopping to reflect on these situations, it becomes clear that there are impacts that often run counter to library values. It is our job as information professionals to help patrons access the information they need, and increasingly this can only be done via digital platforms and services. And yet, it is also our responsibility as library workers to do this work in accordance with the library profession's values. This means we need to protect patrons' privacy and intellectual freedom rights, which are directly under threat from the corporations that have monopolized the tech sector, and to inform patrons of the risks of these services and what alternatives are available, so that they can make the best decisions they can under the circumstances.

Sometimes, as in the scenario described above, providing all the information we might wish a patron to know about a piece of technology is simply not feasible due to the stressful setting and time constraints. But after a decade in the library profession, half of which has been spent focused specifically on technology instruction, I am increasingly committed to finding ways to inject even the most mundane patron interactions with information about the negative impacts of the technologies that we're using. Being a "tech-hater-as-instructor" has helped me build solidarity with my patrons, serve them better in the long-term, and keep my work aligned with the stated values of our profession.

WHY IS THIS WORK IMPORTANT

As library workers, patrons come to us for help navigating the digital landscape, and we have a responsibility to share the truth with them—because, let's be clear, there is nothing "neutral"

About the Author

Hannah Cyrus (hannah.cyrus@bangorpubliclibrary.org) is Digital Media Librarian, Bangor Public Library. © 2026.

This contributed column was submitted on 15 February 2026 and published on 16 March 2026.

about Gmail.¹ There's nothing neutral about AI,² or Microsoft,³ or Facebook.⁴ These tools, systems, and platforms endanger our patrons and communities in ways that are both direct (subjecting them to surveillance and selling their personal information to data brokers and government agencies⁵) and indirect (via the growing political influence wielded by their CEOs⁶). As values-driven organizations, libraries have a role to play in facilitating patrons' rejection of technology, just as much as in their adoption of it.

Patrons are catching on, too. Over the past year, in response to increasing numbers of questions from patrons, I have taught a slew of classes focused on technology refusal, and these have been some of the best-received tech programs I have ever run. While I'll never run out of folks looking to take an "Intro to Computers" or "Smartphone Basics" class, the interest, energy, and excitement around classes like "Data Brokers 101" (wherein I teach patrons how to find out who has their data and try to get it removed), my "Dump Big Tech" series (including "Break up with Meta," "Break up with Amazon," and "Break up with Google"), and especially "Avoiding AI," has been unparalleled. "Avoiding AI" alone attracted seventy participants, attending in-person and live online, to my small and relatively rural library, and they burst into applause at the end of the class. People, whether beginners or seasoned computer-users, can tell that technology is no longer working for them. They know when they are being sold a false bill of goods. They may still be locked into some of these systems, but they are ready to start figuring out how to resist.

This is where libraries can come in. Yes, our traditional jobs have been to teach patrons how to use technology. But, we can also provide information on how to circumvent, resist, disable, and refuse technologies. If ever there was a time to share this information, surely it's now, as the cycle of "enshittification" degrades the usefulness of technologies we've come to depend on,⁷ the U.S. government begins to leverage the massive commercial surveillance infrastructure that has been built up for decades,⁸ and the forced adoption of AI threatens livelihoods, the information ecosystem, and the environment.⁹

ALIGNMENT WITH LIBRARY VALUES

The idea of tech refusal as a form of library instruction may feel overly "political" (a word that is much feared in the library world!). Is teaching patrons how to dump Google and use a different search engine, browser, and email provider "neutral"? No, no more than is automatically signing them up for a Gmail account when they say they need an email address. While it's a popular fiction to imagine that all these technologies are "just tools" and that whether they are good or bad depends on how you use them, the truth is that none of these decisions are neutral. All technology use has impacts on our lives, our privacy, our habits, our politics, and our shared environmental future. Rather than aiming for "neutrality," I argue that libraries should align themselves with their stated values when talking to patrons about technology.

What are those values? Here are the [Core Values of Librarianship](#), according to the American Library Association:

Access: ensuring everyone "can freely access the information they need for learning, growth, and empowerment."¹⁰ For access to truly be "free," patrons must be able to access what they want without trading away their private information, or at the very least while understanding whether and when they are doing so and what the repercussions might be.

Equity: "recognizing and addressing systemic barriers, biases, and inequalities."¹¹ It's well-documented that the harvesting of personal information inherent in many popular technologies

has disproportionate impact on vulnerable groups,¹² as evidenced perhaps most acutely in this moment by concern around ICE using both commercial and governmental data sources to track people's locations.¹³

Intellectual Freedom and Privacy: “empower[ing] people to think for themselves and to make informed decisions” and preserving “the right to develop their thoughts and opinions free of surveillance”¹⁴ is at the heart of the matter of technology refusal!

Public Good: “working to improve society,”¹⁵ which can certainly mean trying to counter the public harm that major technology corporations are wreaking on our citizenry.¹⁶

And finally, **Sustainability:** “making choices that are good for the environment, make sense economically, and treat everyone equitably.”¹⁷ The environmental harm done by data centers powering unwanted and unregulated AI tools alone is enough to make technology resistance align with this professional value.¹⁸

PRACTICAL NEXT STEPS

Though my experience is in public library settings, I believe information workers in all settings can benefit from taking action to promote our values during technology instruction. With the eternal caveat that every library and every community is different, here are some steps based on my experience that library workers can take to start to facilitate values-driven tech refusal in our communities:

Educate ourselves. Many of us learn about technology issues on the fly, accumulating knowledge over time based on what we've had to teach ourselves in response to patron questions or institutional needs. While time is always scarce, prioritize learning about technologies that threaten library values like privacy and intellectual freedom, and experiment with the types of tools that can help neutralize those threats, like alternative web browsers, search engines, and email providers; adblockers; VPNs; and settings changes on different devices. These issues are constantly changing, so remain vigilant and up-to-date in your knowledge. There are ample sources for this information, including the [Electronic Frontier Foundation](#), [Library Freedom Project](#), [the Tor Project](#), and more.

Prioritize privacy on library computers, and use that as an educational opportunity. Many libraries set their public computers to erase saved information at log-off or shut-down, which is essential to protecting patron privacy, but there is much more that can be done to reduce the ways in which patrons are being surveilled while using the internet. Do your public computers only have Edge and Chrome as web browser options? Install browsers with more robust privacy settings, like [Firefox](#), [Brave](#), and [Tor](#).¹⁹ Go through all the browsers and adjust the settings to maximize privacy and minimize features that track or save information.²⁰ Install ad blockers²¹ to protect against invasive cookies and trackers on websites. Consider switching the default search engine to one that does not track a user's searches, like [DuckDuckGo](#), [Qwant](#), [Startpage](#), or [Kagi](#) (which has a free pilot program for library memberships!). Put up signs at the computers about these changes. Patrons will still be free to use Chrome or Google Search if they wish, but they will be presented with additional options and the rationale for why they might want to use them, as a form of passive programming for increasing digital literacy.

Go over the issues with patrons during reference interactions. Ask them questions about their concerns and priorities! Even when they are stressed out, even when using an alternative service

is going to be less convenient or more complicated, give patrons a choice. For example: “Sounds like you need to create an email account. You could use a popular service like Gmail, or a more private service like Protonmail. Do you know what you might want to use, or would you like me to give you more information about those options?” I find that, nine times out of ten, patrons are relieved to hear that someone who knows about these technologies understands and shares their concerns about privacy. These casual conversations can help people reframe generalized anxiety and worry about using the internet into knowledge of specific threats with actionable solutions. Another sample script: “If your main concern is that you don’t want someone else to be able to access your account, I’d recommend focusing on using a really strong password and turning on 2-factor authentication; the browser you use won’t matter as much in this case.” This can take more time than going with the fastest, easiest solution, and some patrons will still choose the easier road, but at least they will travel it in a way that gives them the knowledge and agency to make informed choices.

Share this information in programs. This could be in the form of handouts and flyers or putting together a curriculum to teach a class on a subject you hear a lot of questions about. Again, there are some great resources already available (from sources like [the Library Freedom Project](#)) that provide passive programming opportunities, like a stack of [handouts about data brokers](#) located near the public computers. If you teach any technology classes at the library, you can incorporate information about the negative impacts of major technology corporations, and ways to protect against them, into your existing frameworks. For example, my introductory internet class has a slide that starts with, “Corporations track & monitor you as you use the internet.” This is established fact, and it’s worth sharing if someone is just learning to use the internet! If you have the capacity, consider teaching a class explicitly focused on technology refusal—explaining why someone may want to ditch a popular tech platform or product—and providing steps to reduce dependence on certain types of tech and options for alternatives that are more aligned with library values. [Contact me](#) if you want to use my slides as a starting point!

Organize. Whether within your institution or across libraries, there are other workers out there who you can collaborate with to spread these practices throughout your library and across different settings. Community organizations like senior centers, adult education departments, and social service agencies provide excellent opportunities to learn what concerns are most relevant in your community and work together to provide ways to fight back against surveillance and threats to their privacy and values. Individual action can only go so far; ultimately, part of this work is raising awareness so that patrons, as well as colleagues, can advocate for regulation and rejection of these invasive tools on a larger scale. Share your experiences fielding patron concerns with your local legislators and ask them to advocate for data minimization and privacy laws. Partner with organizations that work with immigrants, survivors of domestic violence, LGBTQ+ youth, or other groups more vulnerable to surveillance, and offer to tailor programs to them and their clientele. Find allies, because pushing back against some of the biggest, richest corporations out there is hard work.

I have been asked by concerned coworkers if this attitude is too political for a public library setting. My response is that this work is aligned with our stated values. If information professionals can’t teach the public that large language models are not a reliable source of information, what can we teach? If we don’t stand up for privacy when it’s literally one of our core values, who will?

At the end of my “Avoiding AI” class, a patron came up to me, visibly relieved. He described his experience of having felt like he was the only one among his colleagues who had doubts about the efficacy and ethics of this technology. Attending the class and learning more about how the tech actually worked, plus seeing a room full of others who shared his skepticism, reaffirmed his belief in his own judgment and equipped him with the information he needed to go back to work and express his concerns. This is the difference that embracing refusal and resistance as a teaching tool can make in a library setting. Spread the bad news. Take up your mantle as a hater and guide your patrons on the path of technology refusal. They will thank you.

ENDNOTES

- ¹ A class action lawsuit was just brought against Google, accusing them of allowing their “Gemini” AI tool to scan and scrape email contents (Robert Burnson, “Google Accused in Suit of Using Gemini AI Tool to Snoop on Users,” Bloomberg, November 12, 2025, <https://www.bloomberg.com/news/articles/2025-11-12/google-accused-in-suit-of-using-gemini-ai-tool-to-snoop-on-users>). This harkens back to their 2017 decision to cease the same kind of surveillance in service of ad targeting, which they had been doing for years (Laurel Wamsley, “Google Says It Will No Longer Read Users' Emails To Sell Targeted Ads,” NPR, June 26, 2017, <https://www.npr.org/sections/thetwo-way/2017/06/26/534451513/google-says-it-will-no-longer-read-users-emails-to-sell-targeted-ads>).
- ² Olivia Guest et al. “Against the Uncritical Adoption of ‘AI’ Technologies in Academia,” Zenodo, September 5, 2025, <https://doi.org/10.5281/zenodo.17065099>.
- ³ Aminu Abdullahi, “Microsoft Shared BitLocker Keys With FBI, Raising Privacy Fears,” TechRepublic, January 26, 2026, <https://www.techrepublic.com/article/news-microsoft-bitlocker-keys-fbi-privacy>.
- ⁴ Samantha Cole, “Meta Users Feel Less Safe Since It Weakened ‘Hateful Conduct’ Policy, Survey Finds,” 404 Media, June 16, 2025, <https://www.404media.co/meta-users-feel-less-safe-since-it-weakened-hateful-conduct-policy-survey-finds>.
- ⁵ “All About Data Brokers Explainer,” Library Freedom Project, Accessed January 29, 2026, <https://libraryfreedom.org/wp-content/uploads/2025/11/All-About-Data-Brokers.pdf>.
- ⁶ Jacob Silverman, *Gilded Rage* (London: Bloomsbury Publishing, 2025).
- ⁷ Cory Doctorow, “Tiktok’s Enshittification,” Pluralistic, January 21, 2023, <https://pluralistic.net/2023/01/21/potemkin-ai/#hey-guys>.
- ⁸ Joseph Cox, “Inside ICE’s Tool to Monitor Phones in Entire Neighborhoods,” 404 Media, January 8, 2026, <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods>.
- ⁹ Brian Merchant, “How Big Tech is Force-Feeding us AI,” Blood in the Machine, July 22, 2025, <https://www.bloodinthemachine.com/p/how-big-tech-is-force-feeding-us>.
- ¹⁰ “Core Values of Librarianship,” American Library Association, Accessed January 29, 2026, <https://www.ala.org/advocacy/advocacy/intfreedom/corevalues>.
- ¹¹ “Core Values,” American Library Association.
- ¹² For example, higher risks for LGBTQ+ people, such as being outed in the event of a data breach or having their sensitive queries related to sexuality and health status exposed (Em. “The Importance of Data Privacy For The Queer Community,” Privacy Guides, June 3, 2025, <https://www.privacyguides.org/articles/2025/06/03/importance-of-privacy-for-the-queer-community>); safety risks for survivors of domestic violence (overwhelmingly women), who may be targeted by abusers (Catherine Fitzpatrick, “For Domestic Violence Victim-survivors, a Data or Privacy Breach can be Extraordinarily Dangerous,” *The Conversation*, December 3, 2023, <https://theconversation.com/for-domestic-violence-victim-survivors-a-data-or-privacy-breach-can-be-extraordinarily-dangerous-216630>); and the greater likelihood of people of color to be surveilled by police and mis-identified by the technologies they are using (Nicol Turner Lee and Caitlin Chin-

Rothmann, "Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color," Brookings, April 12, 2022, <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>).

- ¹³ Joseph Cox, "ELITE: The Palantir App ICE Uses to Find Neighborhoods to Raid," 404 Media, January 15, 2026, <https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid>.
- ¹⁴ "Core Values," American Library Association.
- ¹⁵ "Core Values," American Library Association.
- ¹⁶ If the references thus far aren't enough to demonstrate these harms, I'd like to point to another: the negative mental health consequences of AI chatbots on members of our communities, particularly for vulnerable patrons already grappling with mental illness. I have personally witnessed patrons having unhealthy, parasocial, and even delusional conversations with AI chatbots in my library, and it is heartbreaking (see: Keith Robert Head, "Minds in Crisis: How the AI Revolution is Impacting Mental Health," *Journal of Mental Health & Clinical Psychology* 9, no. 3, September 05, 2025, <https://doi.org/10.29245/2578-2959/2025/3.1352>).
- ¹⁷ "Core Values," American Library Association.
- ¹⁸ Projections show that growth of electricity demand from data centers will outstrip growth of green energy generation, actually increasing the use of fossil fuels in the coming years if they are constructed at the current rate (see: Ketan Joshi, "Green Energy Transition at Risk from Unrestricted Data Centre Development," *Renew Economy*, May 15, 2025, <https://reneweconomy.com.au/green-energy-transition-at-risk-from-unrestricted-data-centre-development>).
- ¹⁹ To be clear, none of these applications are perfect. There's no "best" browser (as I often answer to my patrons' chagrin); it all depends on the situation. These are some relatively good options.
- ²⁰ Settings options are constantly changing as applications and operating systems update, so I recommend exploring what's on the list frequently, and researching terms you're not familiar with. Some other good sources for recommendations around prioritizing privacy in settings can be found on [Privacy Guides](#) or [Activist Checklist](#).
- ²¹ I recommend [PrivacyBadger](#) from the Electronic Frontier Foundation for its focus on blocking only privacy-invading ads, and/or [uBlockOrigin](#) for its ability to customize blocking elements on a page that aren't necessarily ads (like Google's Gemini icon that appears in the top corner of the Gmail webmail interface), but there are many options.