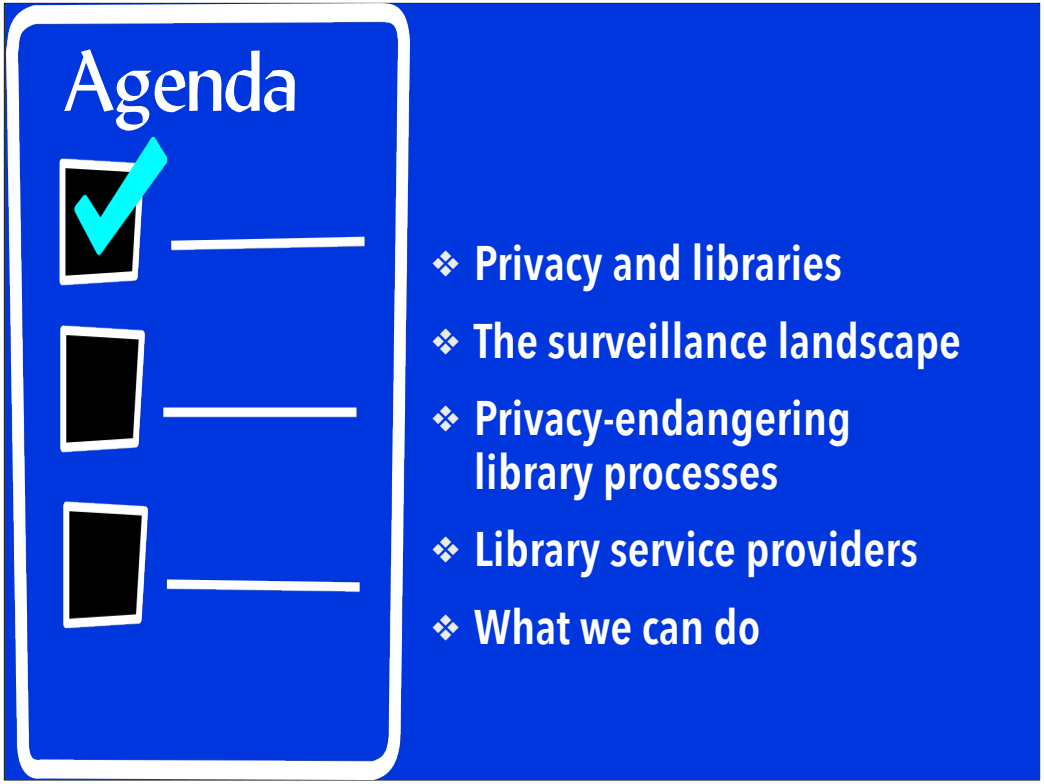
Hi, everybody, and welcome to this session. I am, as you probably noticed, not actually Sarah Lamdan, who's executive directoring now at the Freedom to Read Foundation. Sarah was going to do this talk at the Public Libraries Association conference a while ago but couldn't, so she invited me to do it, so I did it, and apparently people liked it, so here I am to do it again.

Right, so I'm not Sarah. I'm Dorothea Salo, I teach in the Information School in Madison, one state over, and I've been researching library privacy, mostly on the academic-library side of it, for a while now.

Sarah's intended talk title today was Protecting patrons' privacy with digital vendors. I kept that title, I love me some alliteration, but actually…

I do want to say digital service providers instead of vendors, and that's for a non-alliterative reason. We don't usually think of services we're not directly exchanging money with as "vendors," but they're still service providers, and what's important about that for our topic today is that they too can damage patron privacy.

Out of curiosity, anybody have any suggestions for companies I might be thinking about as unpaid service providers to public libraries right now? *(hopefully Google, ChatGPT etc will come up)*

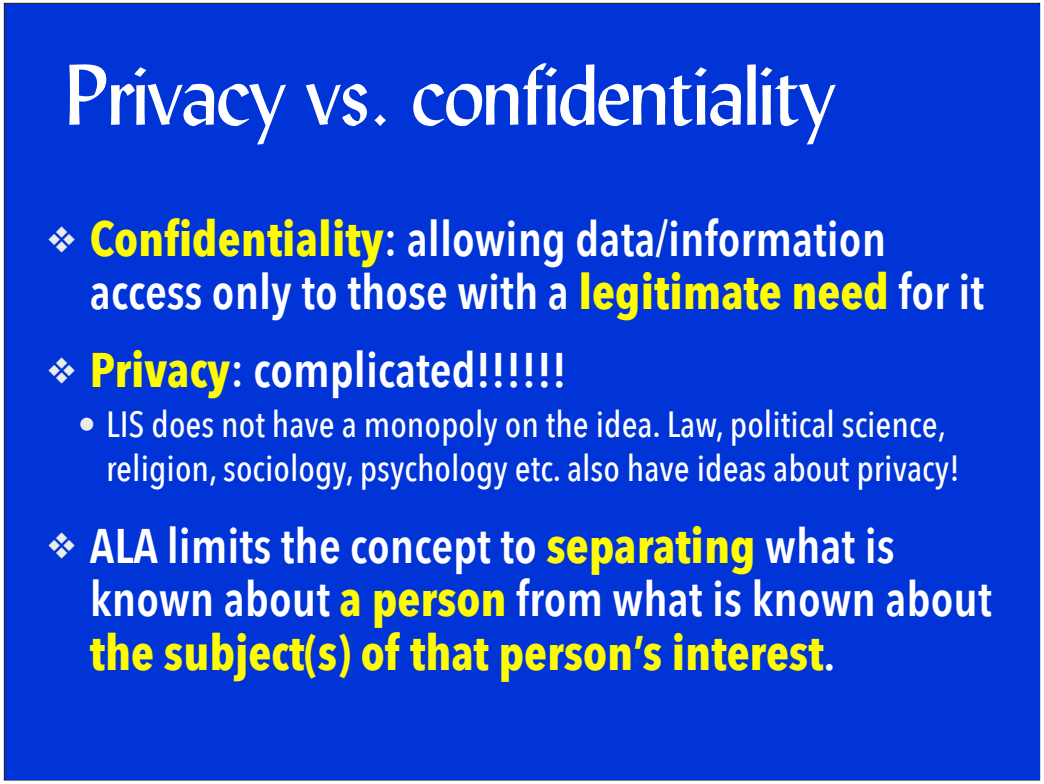


So here's how I'm approaching this. First, I want to do the super-quick nickel tour of privacy and libraries. I don't want to assume that everyone here has that background! It's likely some of you don't, and that's fine! Next, I'll do a nickel tour of today's surveillance landscape, because again, awareness here, research says it's pretty low, and if I can raise it, I want to!

Next is what you're actually here for – library processes, library service providers and how they fit into the surveillance-and-privacy landscape.

And finally, I want to suggest some things we can do, as library workers. Without that, this whole presentation would just be pointless complaining. Now, I love to complain as much as anybody, but it's important to me to motivate change, actually, and I hope it is for you too. Nobody's gonna be able to do everything I'm gonna suggest, I don't expect that at all, but I hope you can find one or two things you and your library CAN do.

So let's do that nickel tour of privacy and libraries I mentioned.

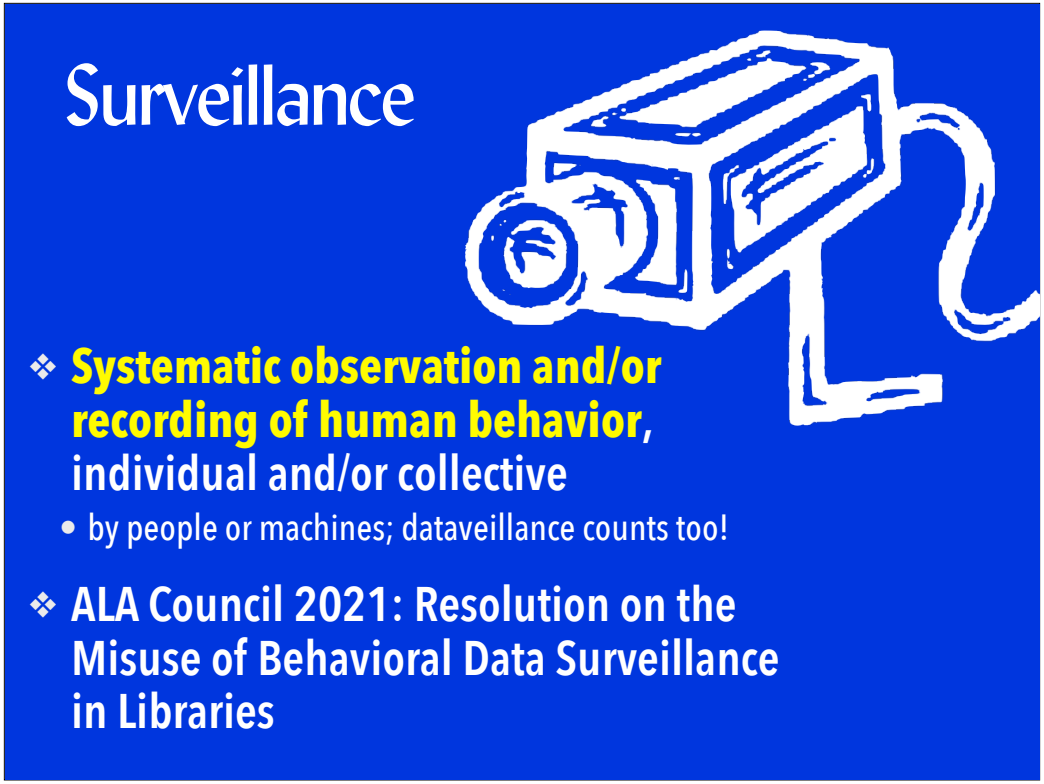


I want to clarify first that privacy and confidentiality are not the same thing, because that's kind of non-obvious. Confidentiality is easier to explain! It just means allowing information access only to those with a legitimate need for the information.

I just want to say, I'm sure this isn't news, but… a whole lot of library service providers will either just straight-up take patron data without asking, or claim they neeeeeeeeeeeeeed it when they absolutely DO NOT need it just to provide whatever service they're providing. It's on us who work in libraries to realize that and call it out!

As for privacy, that's actually a really complicated and vexed notion, if you're confused about it that's NOT YOU, it's got a lot of definitions coming from a lot of people and disciplines, librarianship definitely doesn't own the whole idea. Where ALA takes privacy is separating a person's identity from what that person is interested in. Which is definitely hugely important, but I really think today it's also inadequate! It's inward-focused just on the library and patron use of library-specific materials, which can induce a sort of tunnel vision that I don't think helps us protect patrons.

We'll see some things today that show you why I think that.

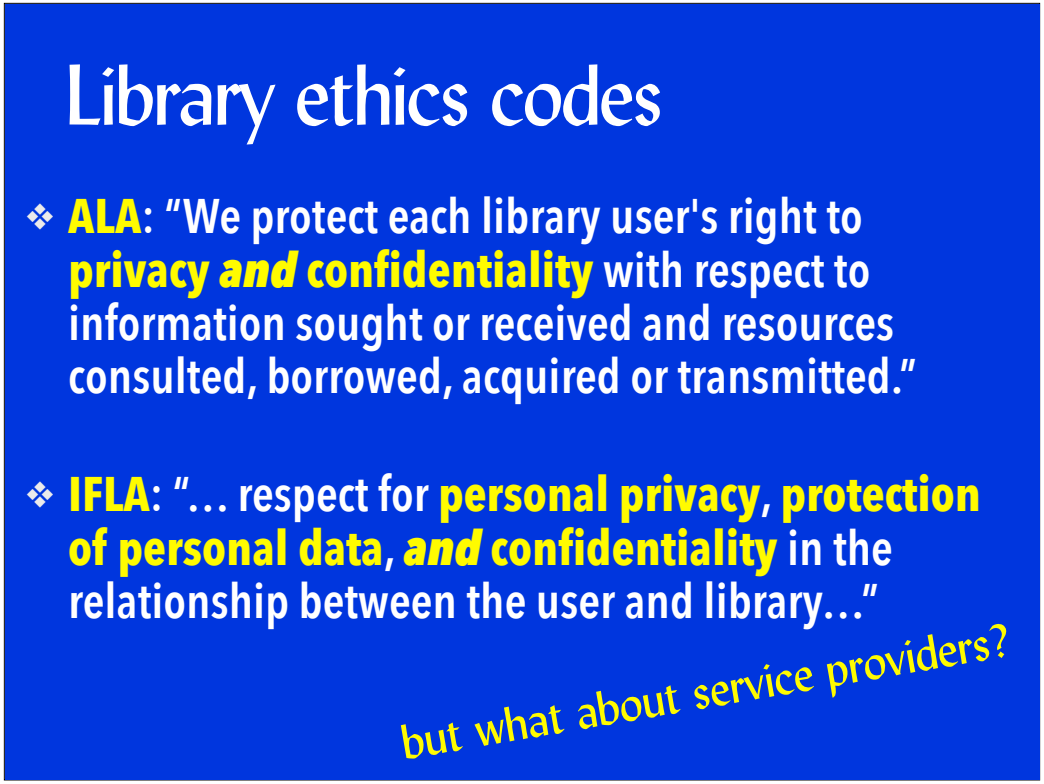


I also think it's helpful in this context to define surveillance, and fortunately that's pretty simple. It's just the systematic observation and/or recording of human behavior, whether that's of individual humans or any group of humans. Direct observation by human eyes counts, video observation and recording count, data collection and analysis, often called "dataveillance," counts. It's all systematic observation and recording of human behavior, so it's all surveillance.

And would you believe librarianship's ethics codes don't say much about it?! They don't actually clearly say "privacy is, among other things, the absence of surveillance." I really think they should, partly because surveillance is so much easier to define compared to privacy, partly because if we took "no surveillance" as an ethical imperative we'd have a LOT more room to push back on some of the stuff I'm talking about today.

So hey, if any of y'all are on ALA or PLA or maybe even IFLA committees that could make this happen, please let's talk?

There is a resolution from ALA five years back that's worth looking at, but it suffers from the usual watering-down you get when something gets written in committee. It's not bad at all, and I'm glad it exists; it's just not as sharp or comprehensive as it could be.



All that said, a couple examples here of what librarianship SAYS it believes about patron privacy. For accessibility I'll read these aloud: *read slide*

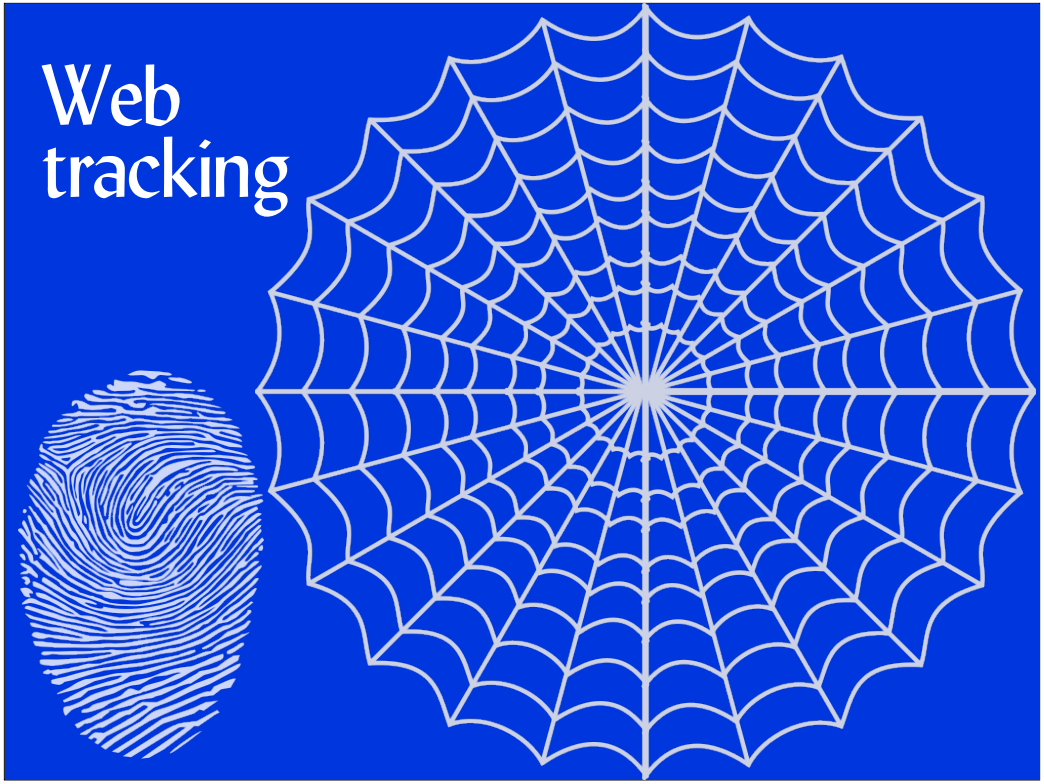
I want you to notice a couple things. First, that ALA says that patrons are entitled to BOTH privacy AND confidentiality. Not or, AND. Sorry, getting a bit Boolean all up in here, but I see some librarians thinking they can violate patron privacy as long as they keep what they learn confidential within the library, and I don't think the ALA Code of Ethics supports that. Patrons deserve to be safe from us and our shenanigans too.

I also see some librarians thinking that whatever library service providers do by way of data collection and analysis is okay as long as they keep it in-house, and I don't think the Code of Ethics supports that, either! Vendors are not libraries or librarians, do not subscribe to library codes of ethics, and are therefore among the classes of people we are ethically obligated to keep our patrons private FROM.

IFLA also uses and, not or, just to note that. I don't love one thing about theirs, though. Confidentiality is supposed to exist in the relationship between the user and library… *CLICK* but what about service providers? Where are they in this relationship, and what's their duty to user privacy, and what duty does the LIBRARY have to make sure that service providers are respecting user privacy the way the library does?

I just. Think we could be communicating a little more clearly as a profession here.

Okay, so that's our nickel tour of libraries and privacy. On to the noxious bit: today's surveillance landscape.



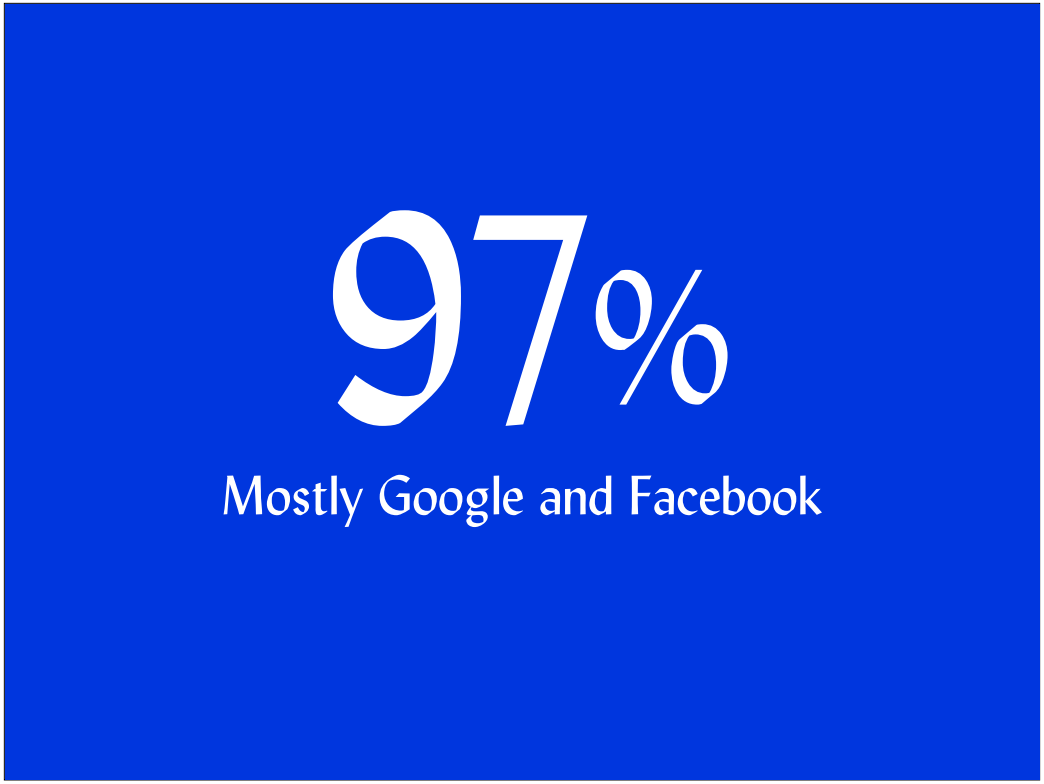
It's probably not news to most of us that our web use is being tracked pretty much anywhere we go and anything we do on the web? Actual trackers, also what are called fingerprinters, which track us by characteristics of our devices and software. If people have questions about the ways and means, I'll happily get specific in Q-and-A, but what I actually want to say about this in our context is a couple-three things:

One, that this is NOT just for personalization and NOT just for advertising! This tracking gets used to follow us around in the physical world and judge us and deny us opportunities and overcharge us for goods and services and turn us in to law enforcement without warrants and get us kidnapped right off the street and NONE OF THIS IS OKAY.

Two, that many library service providers, including content vendors, are happily participating in web tracking. This means we are sending our patrons to be tracked, which I think is a betrayal of their trust, actually.

Three, that way too many LIBRARIES are participating in web tracking. I did some research that I withdrew from a journal after a requested third round of revisions – I'm looking for another journal – on what Wisconsin library web pages say and what they do about patron privacy, where one way I'm defining "what they do" as "how many of them have web trackers and fingerprinters on their home pages."

So let's play a guessing game. I used DuckDuckGo's Tracker Radar data to assess what domains loaded on Wisconsin library home pages were web trackers or fingerprinters. What percentage of Wisconsin public library home pages would you guess had a tracking or fingerprinting domain on them?

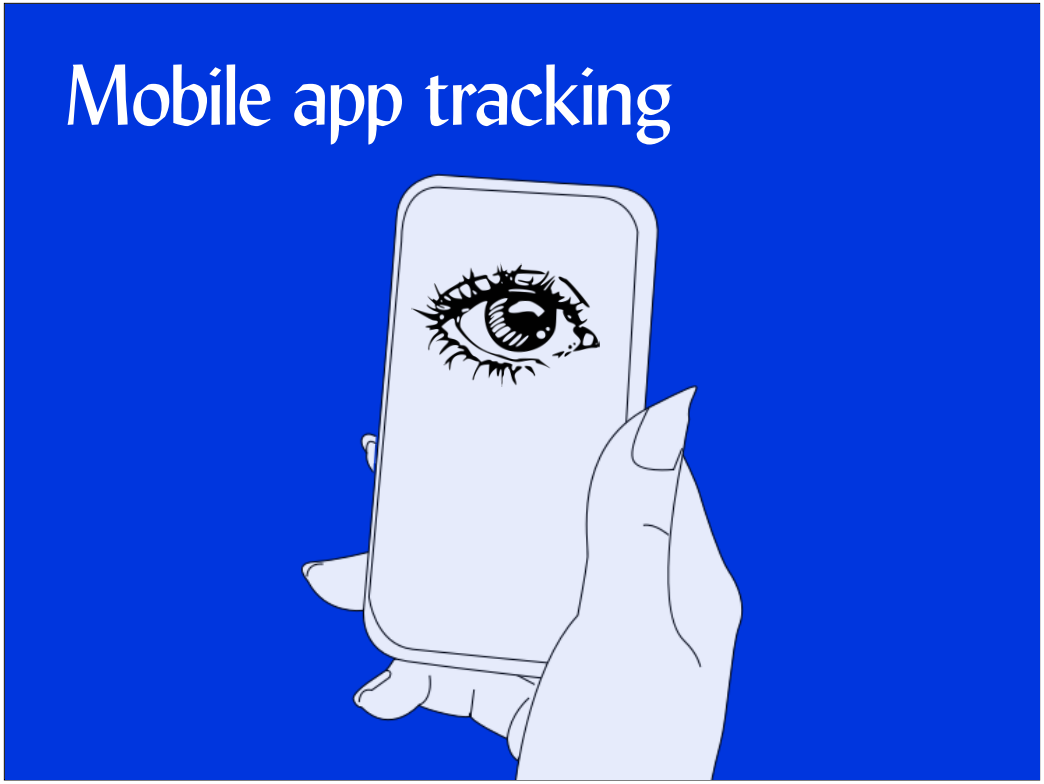


Ninety-seven percent of them. Mostly Google and Facebook, and THIS is why I changed "vendor" to "service provider" in the presentation title. Very few if any of these libraries are paying Google directly, and are any of us paying Facebook? If you are, raise your hand?

Yeah, no, I didn't think so. Basically no money changing hands. But we ARE paying them, actually, when we do this. We're paying them with our hard-won trust and legitimacy – like, any patron is going to think "oh, the library uses this, that must mean it's okay" – and of course we're paying them by letting them do surveillance on our patrons as they do their library-related stuff.

And we are also inviting them into our library service provisioning, which in my head makes us responsible for their behavior toward our patrons. We don't get to wash our hands of service providers invading patron privacy. We let them in, so it's on us too! Especially when, as with Google and Facebook, it's clear that we could make different choices!

Not cool, folks. Not cool at all.



The only thing more pervasive and invasive than web tracking is tracking of mobile apps, and it's worse because phone software developers and cell providers actively facilitate surveillance, including of course by law enforcement.

Libraries mostly didn't get into the mobile-app game, we stick with mobile-friendly websites for the most part, and in hindsight, I'm really not mad about that. What we're stuck worrying about is our content vendors who have mobile apps, and the apps that we recommend to patrons, and honestly I don't even have a good answer here, it's all so bad!

Best answer I do have is teaching people how to tweak their phone preferences to protect themselves, as much as their phones will let them.

Another surveillance measure that mobile phones facilitate, and so do some forms of web tracking actually, is tracking us in the physical world. I feel like I don't have to tell people how this is dangerous right now?

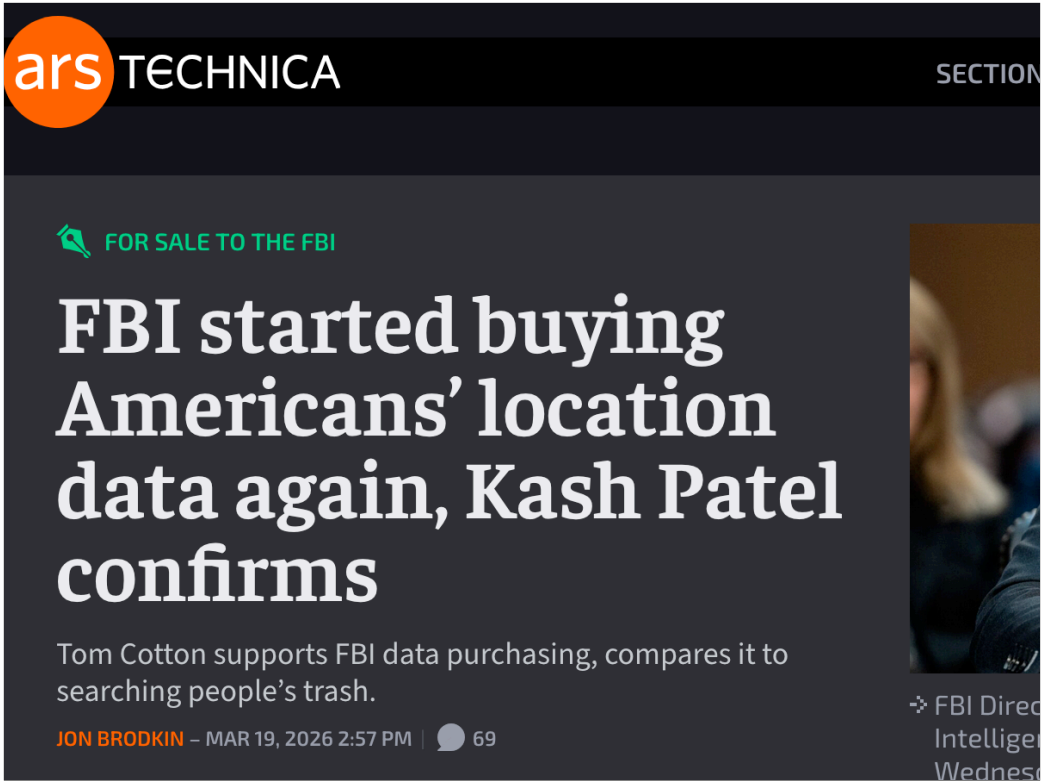
But I've seen some library assessment gizmos or software that track library space usage by recording device identifiers or wifi logins. Y'all. THAT IS GEOTRACKING. That's placing a particular person in a particular space at a particular time, just like a Flock license-plate camera. It's dangerous and not okay. Don't do it, and don't let any vendors con you into doing it. And I don't want to hear "we're only tracking the device, not the person" – for almost all of us it's the same thing, who else uses your phone?

And I want to acknowledge for a sec that this is a new way of thinking for us! How could there possibly be something wrong or dangerous with being found at the library, the single most civicminded and prosocial place in town?! But at the moment we've got people being profiled and even kidnapped from WHEREVER they're at, so yeah, I'm afraid we have to think this way now.

Which leads us to the big money part of all this surveillance: data brokers, the creeps who mass-collect and reidentify whatever personal and behavioral data anybody sells or gives them, so that they can resell whole dossiers on people to whoever's buying. And this industry is basically completely unregulated and has no shame whatever, they're surveillance monsters and they don't care.

If you've been reading in the news about the "data broker loophole," here's how that works. Data that normally law enforcement would have to get a judicial warrant to collect, they are collecting anyway, without warrants, by just buying it from data brokers. Hugely pervasive, hugely dangerous.

Because data brokers will sell data on people to anybody. Including law enforcement. Including kidnappers and stalkers. So any data AT ALL, including from library service providers, any data that gets into their filthy paws presents danger to the people it's about.



I don't even have to dance around this or explain it, THEY'RE JUST ADMITTING IT. And it's NOT just the feds, this nonsense is happening in municipalities, county governments, state-level, yeah, where they can't collect data without the bother of getting a warrant, they're just buying it from data brokers.

So data about library patrons needs not to be purchaseable from data brokers. Ideally that data wouldn't even exist. I also hope that gives you a new perspective on what we're doing when we slap Facebook and Google all over library websites. Both companies have rolled over on people repeatedly. Both companies have been caught lying outright about data they're collecting and what they do with it.

And a common mental defense some of us have against all this tracking is the idea that we're anonymous, just another face in the crowd.

Please abandon that idea. Now, TODAY, I need all of us to let it go. Because it's not true.

Again, I'm going to bypass the ways and means, ask in Q-and-A if you want to know, but the basic idea is this: collect enough decent-quality data about enough people with enough different datapoints in it, and anonymity is gone without recourse. And there's a word for this, the nerd word for taking supposedly anonymous data and finding specific people in it is "reidentification."

There was a vendor at PLA – quite possibly more than one, I only happened across one – whose privacy policy says verbatim "We may use information that has been deidentified or aggregated without limitation." What this most likely means at minimum is, they take obvious identifiers off data, then they sell it and let somebody else reidentify it. Totally not private, not cool and not okay. [The vendor is Cengage.]

If you think some kind of surveillance is okay because it's supposedly anonymous, IT IS NOT OKAY. Okay?

So nudging us a bit more firmly toward libraryland, I want to walk through some library processes, mostly really ordinary and everyday ones, that have privacy implications that we don't always think about hard enough or even realize could get scary.

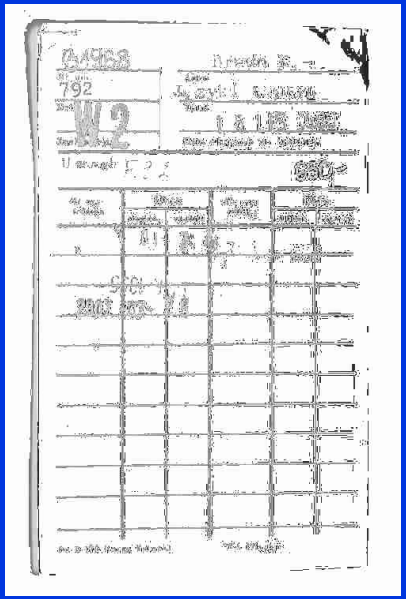
So this is the Saint Paul public library card, I love it, Laser Loon owns my soul.

Signing up for a library card shouldn't feel like an interrogation, and the less data created and stored in the process, the better. When the library actually does have to know something sensitive, like a patron's age or what town they live in? If we can just record that one of us checked whether the patron is local, we should, in preference to recording their address. If we can just record that a patron is or is not a minor and who verified that, we should, in preference to recording their actual age or birth date. All that information can get used for reidentification, among other data-brokery things. All of it can leak or get hacked. The only data that CAN'T leak or get hacked is data that doesn't exist.

And for pity's sake, recording unique identifiers for people like their driver's license number or social-security number is REALLY REALLY BAD and recording and storing images of government IDs is WORSE. Data breaches happen, folks! Don't be the source of identity theft or kidnapping for your whole community!

Like, I wouldn't have thought the images-of-government-IDs thing was even real, but I have a good friend who works on the Evergreen ILS, and he says they've gotten multiple requests for that. What even. What are people thinking.

Retaining circulation records



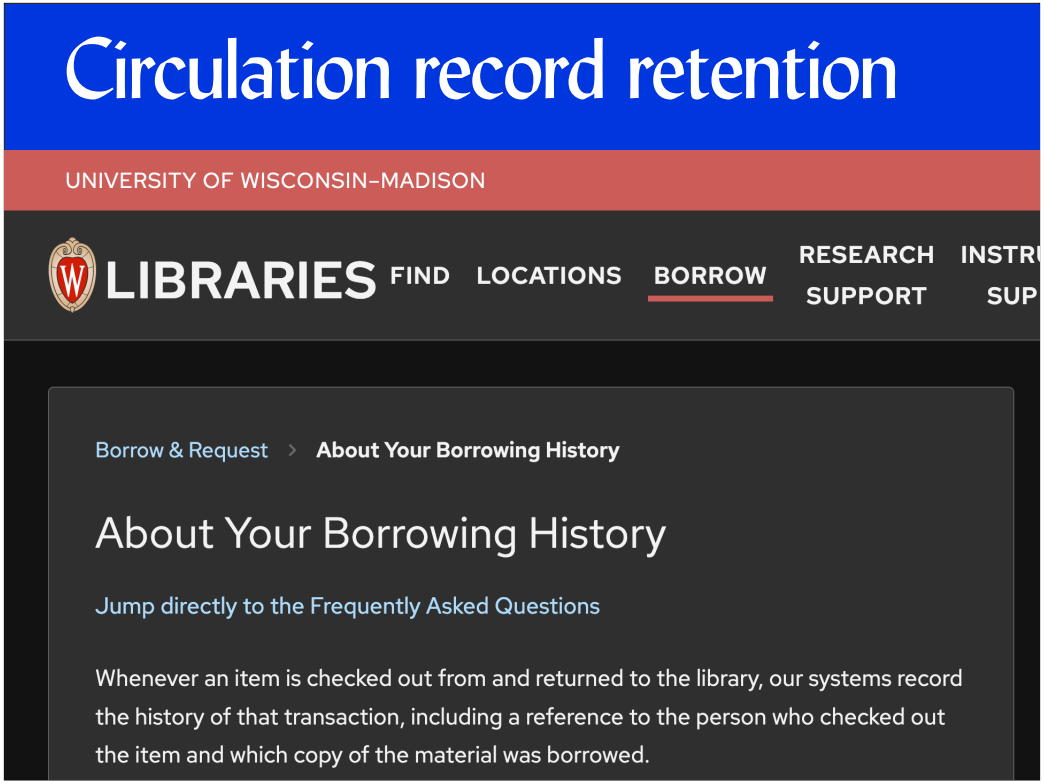
"Library circulation card from Poland."
Wikimedia Commons

https://commons.wikimedia.org/wiki/File:Library_circulation_card_from_Poland.jpg

So a few years back, at a community event I was volunteering for, I was chatting with another volunteer and somehow the topic turned to library privacy, and I talked about how appalled I was that my university library system had twenty years of my checkout records. I mean, twenty years, what the heck?!

And the other volunteer, a bit nonplussed, said "But I like being able to look at what I checked out from the library." And my librarian brain-train immediately jumped the tracks and crashed. I am not proud of myself, I should have expected that response!

So yeah. Retaining circulation records is a serious privacy danger to some patrons and a SERVICE to others. How do we navigate that?

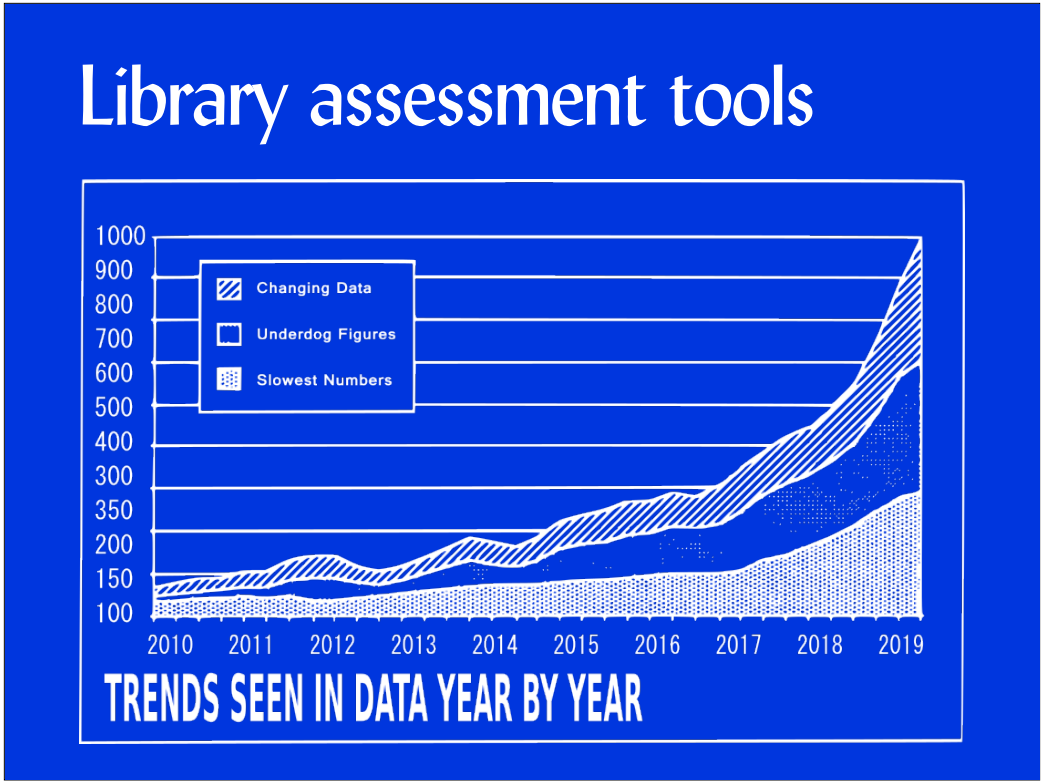


Last year the library system at my university unveiled VOLUNTARY, opt-in circ record retention. And I'm fine with it, even though I myself didn't opt in! The default is privacy, but people who want to take the risk can. People are allowed to take risks, that's basic autonomy. I mean, it does trouble me that most people don't understand what the risks ARE, they don't know that libraries have been Big Red Targets in a lot of past moral panics, but still, people are allowed to take risks. If your library ILS works this way too, it's cool, you're good.

If, however, your library ILS retains identified circulation records across the board indefinitely, that's not private and it is dangerous and I am asking you to get it fixed. I don't CARE if it's for assessment purposes. Assessment is NOT more important than patron privacy.

Again, counting how often something gets used is fine. I have no problem AT ALL with "this book has circulated eighty-seven times." Zero privacy worries there. The real thing to avoid is "here's Dorothea Salo's circulation history for the last however long," or even "here's one person's circulation history for however long" because that's getting scarily close to behavior profiling and reidentifiability; somebody who knows my reading taste could maybe pick me out of the crowd just by my circ trail. I don't think most ILSes do this, though.

But I'll be honest with you, I read stuff that some of the Powers that Be don't like. I need my libraries not to rat me out, and I'm grateful that the libraries at my university won't.



Library space, service, and program assessment. We pretty much can't avoid it any more, unfortunately nobody's just assuming we're good at our jobs, but it shouldn't amount to spying on our patrons.

I hope and believe this is less of a problem in public libraries than it is in academic. Y'all are not dealing with the Library Learning Analytics craze of the twenty-tens, and just, yay for THAT. But if we're not careful, especially online, we CAN end up spying inappropriately and feeding data about our patrons into – or buying that data from – the data-broker abyss. A lot of assessment tool vendors, especially tools for website assessment, sell data from their tools to data brokers!

And again, when we buy or just use an assessment tool WE BECOME RESPONSIBLE for where that data goes! New mode of thinking for a lot of library workers, but a necessary one.

Know what patron-behavior data your tools are collecting and how. When you're considering buying a vendor tool, or using a free tool, it is ON YOU to know what data that tool collects or buys, and where else that data goes. And it NEEDS not to be coming from or going to data brokers. That whole industry is privacy poison and we need not to be supporting or feeding it in any way.

And one more thing. It's good to remember that counting – counting attendees at an event, for example – is a lot safer than taking names. Just in general, counting is way safer than identifying! When you must identify, keep the identified data confidential, and get rid of it as soon as you possibly can.

One kind of tool I’m particularly suspicious of is “customer relationship management,” because this whole class of service is basically a retention tool for data about people! Let’s not make our libraries into mini-data-brokers, yeah?

The 2018–2019 Santa Cruz County Civil Grand Jury
Requires that the

Director, Santa Cruz Public Libraries

Respond to the Findings and Recommendations
Specified in the Report Titled

Patron Privacy at Santa Cruz Public Libraries

Trust and Transparency in the Age of Data Analytics

by September 23, 2019

And if there's anybody here from Santa Cruz I apologize to you – no, really, I do – I'm sorry for calling out your library system's leadership this publicly, but holy cow, folks. It was PATRONS of the Santa Cruz Public Libraries who absolutely SCHOOLED library leadership on the non-privacy of using CRMs a few years back.

I'll say it again: library patrons had to school their own library's leadership on privacy. What. What is even happening to my profession?!

Don't buy CRMs. Triply don't feed any kind of patron circulation, library visit, or other information-use data into them. It's not okay.

I had a lovely conversation early this morning with a librarian from a small public library who talked about the library's outsourced IT, and how they have trouble making all their systems work together, which is a very old and familiar story… but what I want to say about it is, connections between systems are fragile and data has a way of leaking out of them. If you're doing a privacy audit or something, this is definitely something to ask your IT about, whether it's outsourced or in-house.

But there's one more thing that comes up with outsourced IT specifically, and it's that these vendors usually work for for-profit companies who want All The Tracking All The Time. So that's the mindset they're going to come to you with – they'll tell you how to track your patrons on the library website or in the library building six ways from Sunday. And you HAVE to make clear to them that libraries are different, YOU are different, and you DO NOT WANT THAT.

If you get the right tech person, though, they will LIGHT UP when you tell them this! They will be delighted to help you! All you have to do is stand back and let them.

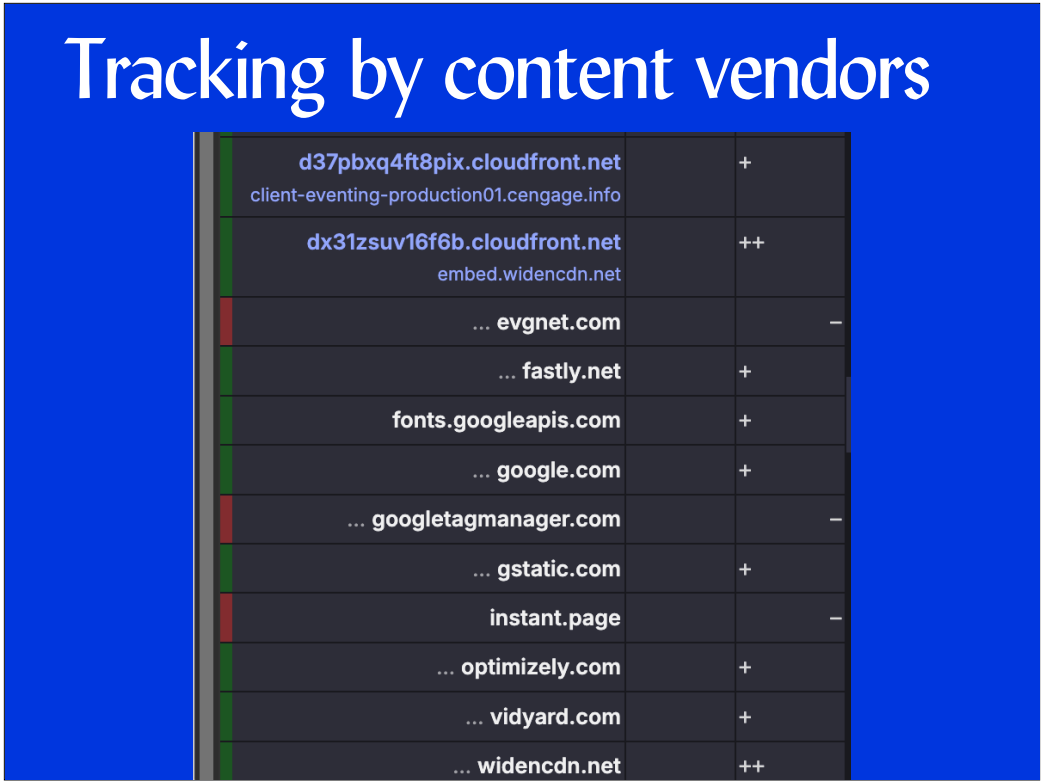
But your typical tech person who's been ground down by for-profit datamongering will do bad things for privacy if you don't stop them.

As I suggested earlier, we HAVE to do better about what we're putting on our library websites. I've gotten in trouble before for calling out Minnesota libraries at a Minnesota conference, so I'm going after Madison Public Library here. This is a screenshot of what my ad and tracker blocker, uBlock Origin, says about their home page.

They're sending information to Google via Google Fonts and Google Tag Manager, which is totally a tracker. They're also loading something called "CloudFlare Insights," which is totally a tracker.

And it's not okay. It's not okay! We have to stop this. Link to wherever you want, just don't embed surveillance directly into your library website, okay?

Now let's move on to library service and content providers.



This is what uBlock Origin told me about the website of a content vendor here at this very conference, and I've obfuscated which one [Cengage] but if you squint you can still figure it out. There's the usual Google garbage. Then there's a bunch of domains I have to sigh and start looking up because they might be trackers.

E-V-G net is associated with Salesforce, and while I can't tell you offhand what it does, based on Salesforce's history I'm not surprised it's getting blocked. Fastly does tracking; that's not how they sell themselves but it's totally a thing they do. Instant dot page doesn't look like a tracker, so that's nice, but they ALSO don't have any kind of policy statements or terms of service on their website, which I don't love, it means I can't assess what they're doing or whether I can trust them. Optimizely does tracking. Vidyard is an AI slop video generator, which is straight-up gross and I hate it, but also, yeah, they're a tracker and as soon as I got this screenshot I told uBlock Origin never to load anything from that domain again.

Notice, by the way, that not all the domains I just called out as trackers are getting blocked here! The tracking's got to be pretty egregious before a vanilla install of uBlock will block it!

So this kind of thing? Is totally what Sarah was coming here to talk about. A lot of the content vendors we pay money to either ARE data brokers or are letting data brokers collect data on OUR PATRONS. And in the current political and regulatory environment, nobody's gonna stop this or even push back on it if we don't.

Another big way that surveillance sneaks into library processes is through free and convenient tools and services. This is THE way libraries became dependent on Google products. Like Google Fonts. Like Google Analytics and Google Tag Manager.

One more time: fundamentally, these tools and services are not free, and we need to stop thinking about them that way. We're paying with our patrons' privacy, and we need to stop being okay with that. Okay?

But the news is not all bad! I actually had to click around a bit to find the screenshot I used in the prior slide, and I am so happy about that!

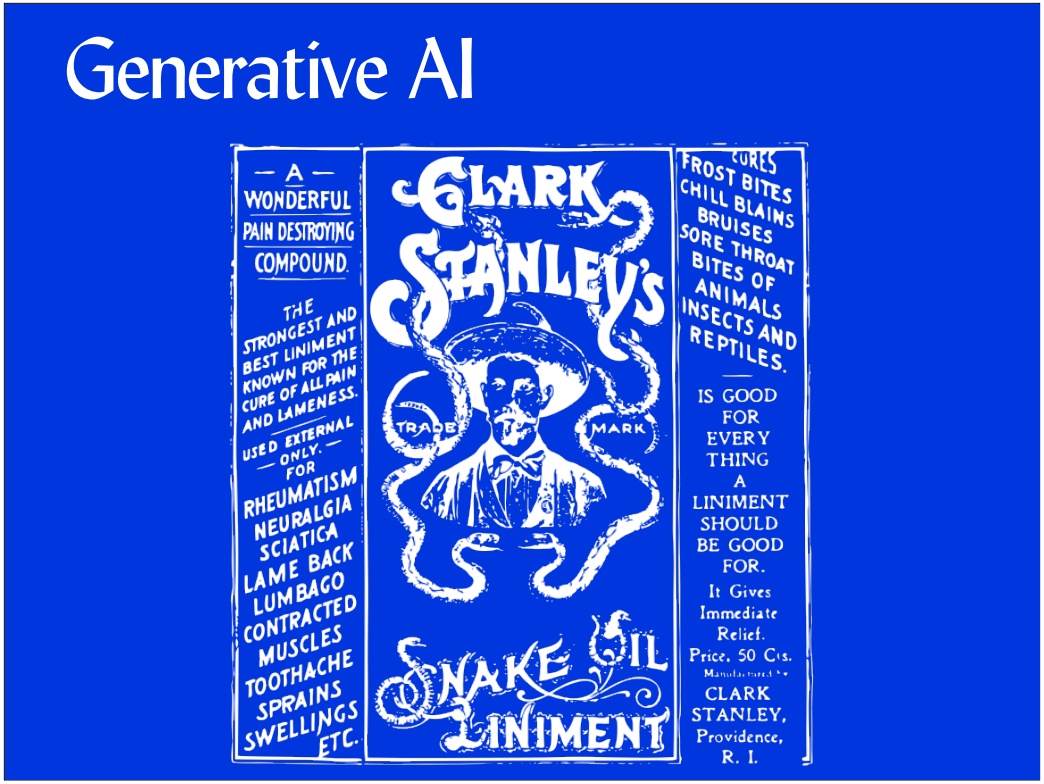
Because I started at OverDrive's home page and I was like, huh. No trackers. And I went to Libby and Kanopy and only found Google. Which, yeah, I'd much rather Google was not there, but that was still so much better than I expected.

And I think y'all did this. I think public librarianship did this. And I am glad and proud to see it. Sometimes when we fight, we win.

And if you need to explain to somebody why it's a bad thing for vendors to be able to identify your library's patrons, here's a horror story that probably some of you know already. When the pricing model for Kanopy got to be too expensive for the New York Public Library back in twenty-nineteen, Kanopy went around them to email their patrons directly, hoping to control the discourse and stir up enough anger to get the cancellation cancelled. TOTAL jerk move!

So yeah, you don't want vendors getting data they can use to stab the library in the back. That includes personalization data – which is, I believe, actually how Kanopy got those email addresses, N-Y-P-L didn't hand them over. I have a couple of license negotiator friends who say that they explicitly forbid vendors from contacting patrons directly, and I have to say I think that's a good idea. Better still to forbid them from collecting email addresses and phone numbers altogether, if you can pull it off.

Generative AI



I'm not going to do a whole rant on generative AI, you can find a couple of my rants about chatbots on my Speakerdeck if you want to, I do think it's oversold unethical snake oil but right now that's not the point.

The point is that these things are not in any way private. They all retain everything you put into them and use it any way they feel like. Absolutely NOTHING WHATEVER relating to library patrons and their information use can go ANYWHERE NEAR a chatbot. Cannot, full stop.

And watch out for genAI transcription and translation tools too, okay? If you're talking about patrons in a Zoom meeting, you need not to be letting Zoom or any AI gizmo transcribe or summarize that meeting. There have already been hacks and leaks, and even without that it's one more way to sell patron privacy into the panopticon, because AI companies have NO SHAME.

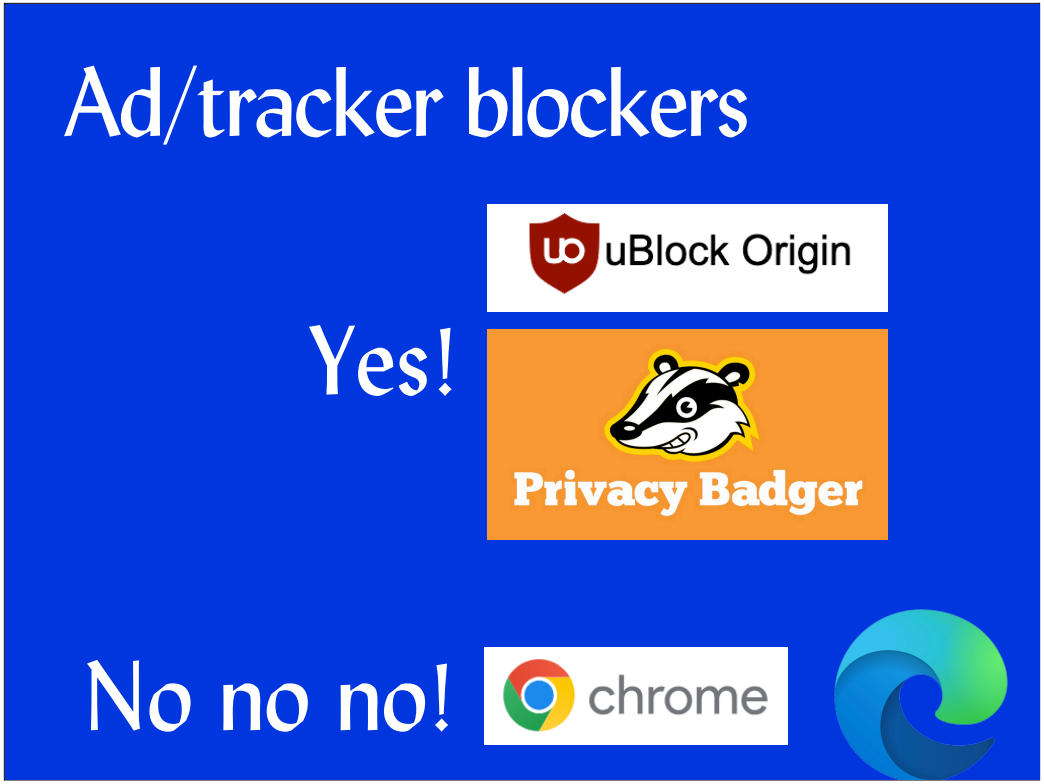
Okay. So after that lengthy list of horrors… here's what I think we can do about them. I probably don't have to tell you there's no quick or easy fix. But as I said earlier, sometimes when we fight we win, so here are some ways to fight.

I think the first step is to not be hypocrites. We – and I mean this at a whole-profession level here, this applies to all of librarianship – we don't have any business trumpeting a commitment to privacy that we're not actually living up to. So that means cleaning our own house. Doing a privacy audit, though again, ALA's guidance for those is painfully last-century and needs a major update. Looking at what we do around circulation data and patron computer-use data and card-signup data. Looking at the assessment we do and where it's leaking privacy. Looking at free convenient tools we use that sell our patrons into the data-broker-verse.

It's no fun at all, but we do have to do it. Let's really be examples for the rest of the world on not exploiting people through their data, and not ALLOWING that exploitation from others.

There's a phrase I want you to take home with you, and use on everybody you can but ESPECIALLY your library leadership, your library board, your library IT, and your library vendors. And that phrase is DATA MINIMIZATION. It just means a conscious practice of collecting the smallest amount of data possible and keeping it for the minimum necessary amount of time.

CLICK Big data is so ten years ago, people! We don't want big data, especially about patrons. We want the smallest data we can possibly have, in terms of what data we actually collect and how long we keep it. We want both those numbers as small as possible, and every piece of data we have, we need a real justification for. "We might need it someday" is not a real justification. If we don't need it NOW, it needs to be gone.



Do I have any IT folks in the room? Yeah, there's a thing y'all can do on the library's patron-facing computers to fight back against web tracking and fingerprinting. And it's adding ad and tracker blockers to the web browsers you're providing. The two I like and use are uBlock Origin and Privacy Badger, but there are others.

If you have an intellectual-freedom person at your library who doesn't want you to block ads, I think you have two counterarguments: first, these blockers can be turned off by the patron in max two clicks, and second, malware through web advertising is totally a thing these days and there is no intellectual-freedom argument I can think of that says we have to let malware through.

CLICK Unfortunately, this does mean ditching Google Chrome and Microsoft Edge, because Google and Microsoft changed how they work so that ad and tracker blockers DON'T work. So yeah, go with a different browser, and explain to your desk staff why you did that and how they can talk about it with patrons.

If you're fancy there are things you can try at the network level too, but most of us don't need to be that fancy, especially because navigating the intellectual-freedom stuff gets harder. Browser ad and tracker blockers are enough.

And of course this recommendation will not surprise anybody at this point: we need to look at the domains that load on library websites, and how many of them are trackers or fingerprinters.

As a quick heuristic for this? Install uBlock Origin into your favorite non-Chrome web browser, and see what it blocks from loading on your site. That's pretty much where I started for my research.

And then you kick the trackers and fingerprinters off the library site.

If we could do ONE THING profession-wide, honestly, I would want it to be de-Google-izing. Can we just. Can we just boot Google to the curb. Please. I am BEGGING here.

Now, I do understand that many of us are not in total control of our web presences. Any of y'all stuck with a corner of your municipality's website? Yeah, sorry about that, it's rough. But if you've got the energy to raise this with your municipality, I AM WITH YOU. I shouldn't have to be tracked and sold to data brokers by my city government either!

Defaulting to private

- Default search on patron-facing computers **should not be Google**!
- The usual recommendation is DuckDuckGo…
- … but investigate your options at https://udo.se/

And another thing we can do besides kicking Google off our websites is kicking its search engine out of our computers' browser defaults, especially now that they've stopped running a search engine in favor of being generative AI slop pushers. There are better and more private options! The usual recommendation is DuckDuckGo, and it's what I usually use, but there are actually several more options out there, and somebody I follow on Mastodon posted this tool, u-d-o dot s-e, which lets you take a bunch of search engines out for a stroll and see which one has the most privacy and the least AI slop.

Okay, great, fine, let's say we've cleaned out our OWN house, now what do we do about the vendors? Especially since for most of us, we're not even the ones negotiating the content contracts or buying the software we use.

So we're going to have to start having conversations with our municipalities around software and websites – and our consortia around content.

And oh my gosh, I am not saying you have to go in there and tell your consortial people that every contract has to ensure the total privacy of every patron, because that ain't happening and it's unfair to ask of your poor license negotiators. But you can, I think, agree on data-collection and data-handling questions that the negotiators can be asking of every single vendor, and maybe you can work together on license terms to look for and strike.

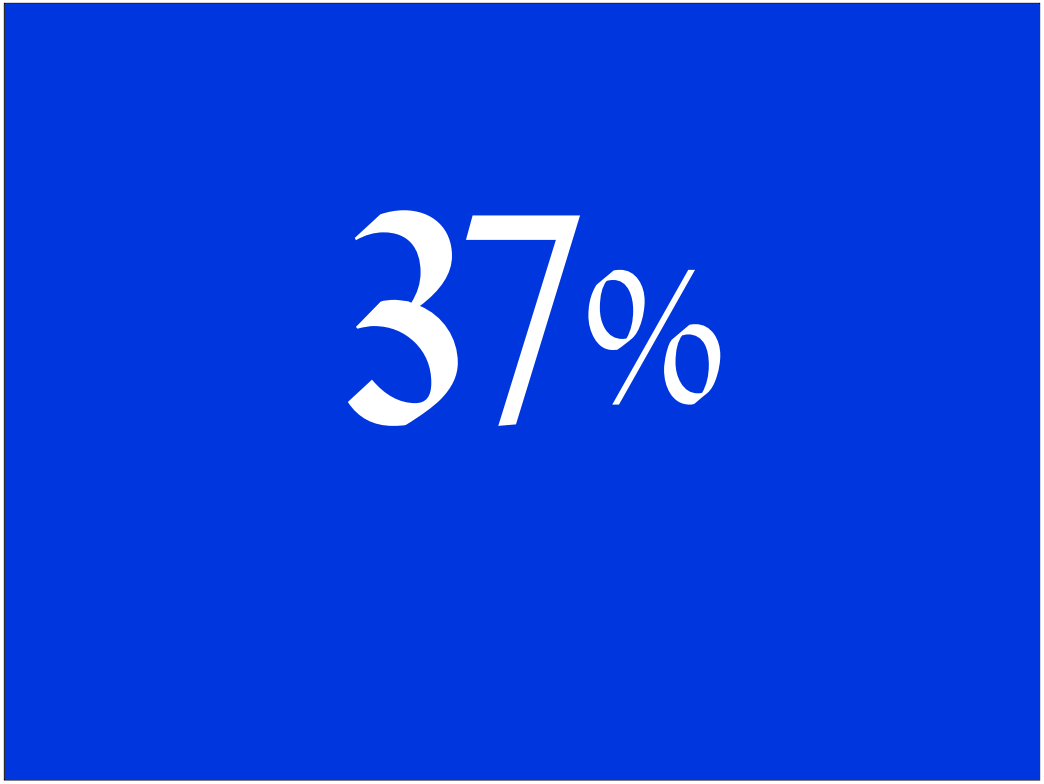
You won't see immediate results from a lot of this. Vendors can and do say no. But I do think it's this kind of pressure, vendors hearing from us over and over that we're not happy with their data practices, that led to OverDrive's home page being free of web trackers. Together we can win!

There's been some work on content contracts in the academic-library context, and in all honesty I don't know how much of it will make sense to public libraries and consortia? But it's a place to start, at least, and if nothing else it will clue you in to dirty tricks vendors try so you can look for them. I've given you the URL there, and I think if you do a web search for "library licensing privacy" and ignore all the AI slop you should find it.

You can also find scathing reports on Elsevier and Springer-Nature from an organization called SPARC with a C, s-p-a-r-c open dot org is their website. These were super-thorough, written by my friend Becky Yoose of LDH Consulting Services, and again, the reason to look at them is to calibrate your sense of content vendor privacy-violation techniques.

The last thing I want us to investigate at our own libraries is whether and how we are communicating to patrons about our privacy values and how we implement them. Because that was another thing I looked at in the article I've been working on, and honestly, y'all, it's kind of dismal. Those of us who even have privacy policies tend to bury them in employee handbooks or a six-click-deep policy page.

In fact, let's do another guessing game – guess what percentage of Wisconsin public libraries have a privacy policy anywhere in their public web presence? I'm not counting website privacy policies, I mean LIBRARY privacy policies. What percentage, do you think?



Thirty-seven percent.

PAUSE

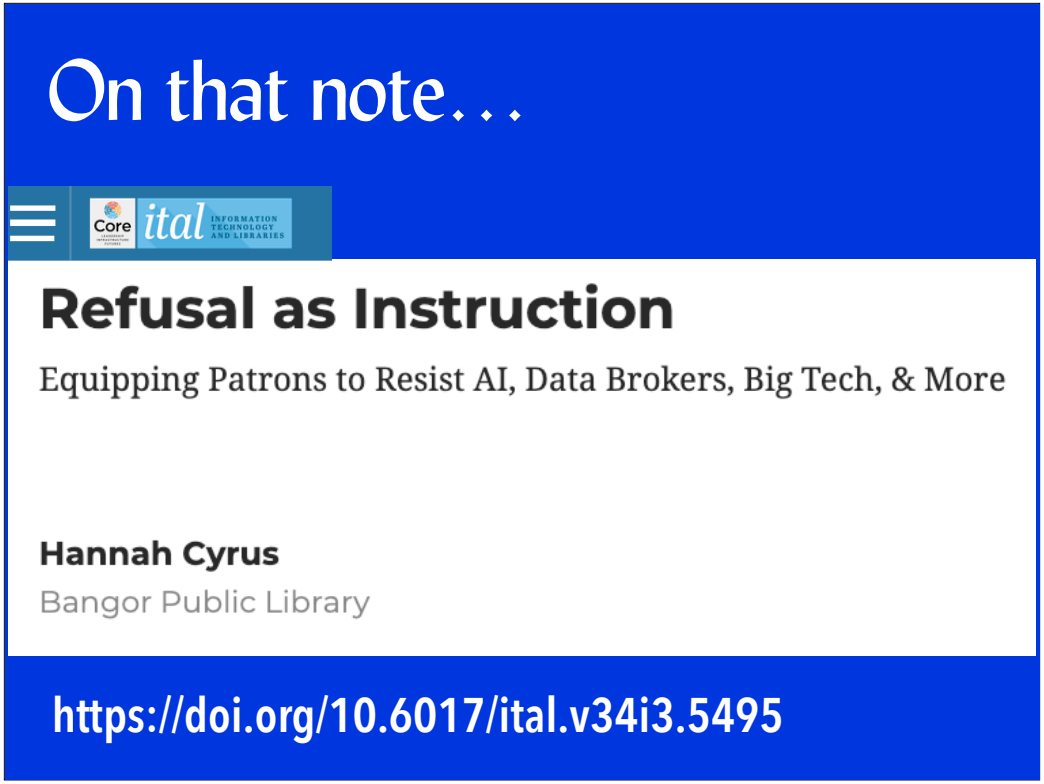
Yeah, y'all, we kinda gotta fix this? Why should patrons even BELIEVE that libraries and library workers value privacy if we cannot be bothered to say so?

And really, who reads policies? Only the most desperate or the most rules-lawyerly. I'd really like libraries to communicate MUCH more clearly and MUCH more often than this. Grab that megaphone and use it!

And look, if you know your library doesn't have a privacy policy, I invite you to consider that an opportunity! Ask your community to help you write one, and unveil it with big fanfare, why not?

Because I don't know if you've noticed, there's just way too much happening right now for anybody to stay on top of it all, but… anti-surveillance is kind of having a moment? Whether it's getting rid of Flock cameras or detoxing from Big Tech or stopping legislators from outlawing encryption online, people are finally starting to say louder than a whisper and in greater numbers than just us privacy advocates that maybe all this surveillance is uncool!

I don't think there's going to BE a better opportunity for library workers to show our colors. Again, if anybody's here from ALA or PLA and wants to get a campaign started, I'm with you, let's DO THIS.



On that note, I want to mention to you a piece that came out just a little bit ago in Information Technology and Libraries, also open access, it's by Hannah Cyrus of the Bangor Public Library in Maine and it's called Refusal as Instruction: equipping patrons to resist AI, data brokers, big tech, and more.

And it's outstanding. It's SO GOOD, y'all. It offers several ideas for library programming, too. And let me tell you a thing, I'm in my university's speakers' bureau, I do maybe half a dozen talks a year? A couple weeks back I switched out one of the talks I offer for a "detox from Big Tech" talk – and I had a taker in just three days.

I really think that anti-surveillance is a smart way to engage our communities right now, and for all we're not perfect, we librarians are the best people to lead on this. Hannah shows us how. Let's do it.

So thanks everybody, that's what I've got for you today, and I'll be around if you want to talk further.

Be safe out there. Can I take questions?