Hi, folks, and thanks for being here today, I appreciate your time. I’m assuming I have catalogers, access-services folks including interlibrary loan, e-resources folks, maybe some systems folks, quite a variety. I'll try to reach you all at least sometimes, but I do want you to know I realize I’ll sometimes be talking about stuff that is out of your individual control. Nobody has infinite power over library systems, but you folks do have SOME power, and I hope and believe you want to use it wisely.
A couple of recent news items, first. In the UK, a man was arrested for downloading an electronic copy of our old friend the Anarchist Cookbook.

If you think this couldn’t happen to an ebook or e-journal-using patron on this side of the pond, well, I’m not even sure what to say to you?
And close to my home in Wisconsin, there was a pretty big data breach in the circulation system at a public-library consortium. Whoever the hackers were, they got some good stuff, stuff that shouldn’t be public knowledge, stuff that can absolutely be used to mess with people’s lives, online and off.

And I’m like, did the consortium actually need this information? Email addresses, okay, I get it, but do you need actual birth dates, or do you just need to know whether somebody’s an adult or a minor? Do you need to store the ID number, or is it enough to record that a librarian verified somebody’s ID?

Because basically this breach is the library analogue to Equifax, as far as the information leaked goes. Identifiers connected to personally-identifiable information. Phew. Not good.

And if you think this can’t happen to your library or consortium, I’m not even sure what to say to you? Except that I used to invite my friend, IT manager Mike Simpson, to talk to my library-technology classes about security, and the first thing he’d always say is, “YOU WILL BE HACKED. Get ready for that.”
We have committed to privacy.*

*at least out loud
And among the many reasons it matters that we’ve made that commitment, we are being looked to as ethical exemplars with respect to privacy. Pinboard, it’s an online bookmarking service I use that’s run by Maciej (MAH-chay) Ceglowski (seh-GLOV-ski), who is an amazing privacy advocate in technology-centric communities. And who’s he looking to as an example for tech? Libraries!

I have concerns. I mean, it’s certainly nice to be recognized for our ethical stance, but I have concerns about this. I really do. I’m not sure we’re living up to it, in deed or even in word.
"protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted”

—American Library Association
Code of Ethics
Article III

Now, here’s something Maciej admires, and rightly so.
Guidelines for ALCTS Members to Supplement the American Library Association Code of Ethics, 1994

I want you to keep these in the back of your head as I speak, and measure the things I’m telling you about against YOUR sense of what is fair and ethical. Because, look, lots of stuff that damages privacy is nominally legal. That’s an incredibly low bar, especially in the United States, and I want libraries not just to pass that bar, but leap over it in a single bound like Supergirl. So don’t forget “fair” and “ethical,” okay?
So with that as context, let’s figure out how to think holistically about securing patron privacy.

Professional information-security people say that to protect data and to protect people’s privacy, you have to think like the people who are attacking you to get at that data. It’s called “adversarial thinking.” You ask yourself who your adversaries are, and then you ask yourself how they’re going to get at data that compromises patron privacy… and how you’re going to stop them.

This way of thinking also helps you look for privacy problems and advocate for privacy. “Privacy” is a really big word, so big that even privacy advocates don’t always agree on its definition. So if you can think about privacy in a fairly organized, holistic fashion, I think that helps you see where your organization is making privacy mistakes, and advocate usefully for fixing them.
This taxonomy of patron-data adversaries is my own invention, and I’m not wedded to it? But as a first approximation, I think our adversaries, in the information-security sense, can be boiled down into data omnivores, data opportunists, and data paparazzi.
Omnivores

Opportunists

Paparazzi

The N-S-A is a data omnivore. Google, Facebook, Twitter, Amazon, Taboola and DoubleClick and other online ad and traffic networks, commercial data brokers like Acxiom, they're omnivores. Black-hat hackers are omnivores, typically. If there's data about people, any data at all, omnivores want it, and not just that, they want to—and CAN—match your data TO you. The only way to prevent that is to keep data out of their greedy paws, even when they're actively lying to you, hiding the extent of their data collection and reuse, and trying to subvert any effort you make to kick them out of your systems.

And sometimes the only way to prevent THAT is not to collect or keep the data at all. Intentionally refusing to collect or keep data is called “data minimization” and I absolutely think libraries should commit themselves to it. Data you don’t have can’t leak, can’t be hacked, and can’t be misused by a malicious insider—which is absolutely a thing that happens.
Opportunists are people trying to do cool and useful things with data. They’re academic researchers, and data collectors trying to be nice to academic researchers. They’re web and social-media developers, usability wonks. They’re hackathoners. They’re open-data advocates and assessment experts. They’re library administrators trying to talk numbers to provosts and chancellors, or library boards, or municipal government.

Opportunists are people with their hearts in the right place — but that doesn’t mean they’ve thought things through, and it doesn’t always justify their data collection, data use, and data communication practices. Data opportunists are making some amazingly big and scary privacy messes!

And more broadly, data opportunists in libraries are NORMALIZING data surveillance. Like, I don’t have time to talk about why the current digital panopticon is a bad thing, but there are books on this, you can read them, books like Dragnet Nation and Data and Goliath. What I want you to take away is, if our much-trusted libraries participate in the digital panopticon FOR ANY REASON, we’re telling our patrons “it’s okay, just lean back and let Big Online Brother watch you from the telescreen.”

And that’s not okay. That’s not who we are as a profession.
Data paparazzi have a TARGET, a specific person they are tracking, and they pursue that specific target through whatever data they can find. They are people on political crusades. They are doxers. They send SWAT teams to people’s homes. They are death-threat senders, kidnappers, perpetrators of violence, people who hate and who harm. And paparazzi are terrifying, because they are obsessed, they are amoral, and they stop at NOTHING — they will social-engineer you, they will hack your systems and try to use them against their target, they will take over a target’s account to impersonate them, learn more about them, or ruin them, they will correlate whatever they find out from you about their target with anything else they can find anywhere. Don’t be thinking “well, they don’t want the data libraries have” — yes, yes they do!

So. Whenever you’re thinking about patron privacy with respect to data you are collecting, or data you control, you should ask yourself “could an omnivore get their paws on this? what could a well-meaning opportunist do that’s damaging? is somebody going to get doxed or SWATted by paparazzi if these data of ours leak?” That’s adversarial thinking, and I’d love to see tech-services and access-services folks doing more of it.
Here’s another taxonomy I kind of invented, this time a taxonomy of the patron data libraries want to worry about.

So I’ll take these one at a time, and then I’ll give you some library-specific examples of what I mean.
The thing about P-I-I is, everybody knows about it... but too many people think it’s the total extent of the patron-privacy problem. It’s not. But a lot of vendors who don’t give a flip about privacy will do this little Dance of Deceit, where they’re really loud about how careful they are with P-I-I, but they don’t say ANYTHING about what they do with supposedly-anonymized data, never mind long-tail info and behavior trails.

So watch out for the Dance of Deceit! Anybody doing it is probably hiding something privacy-threatening! Don’t let them get away with it! Read vendor privacy policies carefully, and please be prepared to call them on this and demand they do better. Who else is going to call anybody on this, if not us?
"Long tail" information is information about any person that makes them stand out from the crowd, lets an attacker narrow down a big dataset to one person even though that person is not actually identified. There's so much data floating around about us these days that long tail information in lots and lots of datasets can't be assumed to remain anonymous—if somebody tries, they can use long-tail information in a system or database to identify individuals, and then tie them to whatever else the system or database knows about them. Or whatever else any OTHER system or database knows about them.
Such as their behavior trails—whatever traces their behavior leaves in a system, like your OPAC or your collection of electronic resources... or your proxy server, which is a necessary part of library systems but also a huge and scary collection of individually-identified behavior trails.

Behavior trails all by themselves can be identifying, of course; an adversary might not even need a name or identifier to pick somebody out. Take me, for example—my constellation of professional interests is probably unique on campus. I’m betting somebody who knows them—like a lot of you, I shouldn’t wonder—could use my library information behavior to identify me in proxy server logs.

The other thing about behavior trails is that they can be exactly what an attacker is interested in. So the more information our systems collect, transmit, and keep about patron information behavior, the more information those systems can LEAK about patron behavior.

One more thing about behavior trails. Usability and usage-assessment research—and research tools—like behavior trails a lot. I know that both usability and usage assessment are big parts of your job as technical-services professionals. This means I have to ask you to be critical about the research tools you use. What data do those tools collect about your patrons? How long is that data retained? Is that data aggregated with other data not from your organization for analysis? Because that can make individuals easier to pick out from the crowd. Can that data be sold or transferred? You HAVE to know.
Okay, example time! You might think, “there’s no way libraries would compromise personally identifiable information, come on, we know better!” But we do, sometimes, without even thinking.
I am indebted to Angela Galvan for letting me retell this story. She suggested the purchase of a book for the library where she worked, and when the book came in, the cataloger put Angela’s name in the nine-seventy since Angela had made the suggestion… because that’s Just How Things Were Done and nobody had thought about it in over a decade. Angela, in her original presentation, called this a “vestigial” workflow.

A similar story I’ve heard, though I can’t say exactly where it comes from: a library was putting order history information in the nine-eighty-one, and some of those fields included staff members’ staff ID numbers. That’s basically an Equifax-style mistake—you don’t ever want to reveal an ID number that’s the key to a lot of information about people!

This kind of thing is not safe or secure for users, including donors and suggesters. This kind of thing is not safe or secure for staff. Please, audit your catalog and cataloging and e-resource workflows for these “vestigial” privacy violators and root them out!
Here’s one I used to deal with myself. When I was running MINDS@UW, the Wisconsin system’s consortial institutional repository, when a borrowing request for a local dissertation came in, the interlibrary loan folks would scan it to PDF and in addition to getting the PDF to the borrower, they’d put the PDF in the repository, in an open or closed collection depending on the copyright situation. It was a nice little workflow and I appreciated it, and the open dissertations actually got quite a bit of extra use.

Now, way back in the day, whenever someone outside Wisconsin borrowed a dissertation, the circulation department wrote down the borrower’s full name, sometimes their affiliation, and the borrow date on a designated loan page right after the title page. Yikes, right? But in the two-thousands, because nobody told them otherwise, the people who scanned dissertations faithfully scanned the loan page along with everything else and put it online! Once I noticed one in the repository with the loan page intact, I howled in horror, checked all the dissertation PDFs, and ripped those loan pages out of the PDFs that had them so I could replace the files in the repository. It wasn’t just a theoretical patron-privacy threat—I saw names with dates as recent as the nineteen-nineties.

I just. I don’t know who in the libraries back in the day thought that page was a good or even baseline ethical idea, it’s completely contrary to the ALA Code of Ethics… but all we can do sometimes is fix things after the fact, I guess.
Libraries handle a lot of long-tail information around information use. Think about your own library-mediated information use. Who else where you work uses exactly the same ebooks and databases you do? Is anybody even close? Could your constellation of ebooks be compared to, say, your Facebook or your Goodreads reviews to pick you out of the crowd? Don’t laugh—exactly this happened to Netflix and IMDB movie reviewers.

And, you know, just to make the idea of reidentifying somebody by their info use appropriately awkward, let’s imagine somebody who identified me, me myself, by my library usage in, let’s say, twenty-ten or twenty-eleven. Poking around further, that attacker would also have discovered my sudden devouring interest in cancer of unknown primary origin. *PAUSE* Now no, I don’t have this terrible disease—a close family member was dying from it—but a lot of you jumped to that false conclusion, didn’t you? “Why” is a question that behavior trails often lead people to jump to false and dangerous and harmful conclusions about. That’s a concrete privacy harm that long-tail information stemming from patron information use can create.
Here’s a real example. Library Hose happened at Harvard University Libraries, briefly. As an outreach tool, Harvard built a bot that tweeted out the title of each book checked out from its library. The bot would tweet at pretty much exactly the time the book was checked out. Doing the same thing with ebooks or e-journals would absolutely be possible; I’m glad Harvard didn’t try it.

And I’m sure they were thinking “we’re not tweeting the patron’s name or other identifier, so we’re good!” Um, no. Anybody watching the circ desk or the exits at Harvard with the Library Hose tweetstream running? Super, super easy to match people with checkouts, because TIMESTAMPS are classic long-tail information, they limit the checkout dataset to one or only a few people, and in the e-resources realm they’re easy to correlate with server-access logs or even network packet sniffing.

So there was an outcry, and Harvard took this amazingly bad idea offline, but it just goes to show. Gotta watch those timestamps. Leave them out if you can, fuzz them if you must keep them. CERTAINLY don’t tweet them!
And then there’s library research and assessment. This is from a very recent article in College and Research Libraries. In a paragraph laying out the demographics of their sample, *CLICK* they specify down to a group with eighteen people in it. EIGHTEEN.

Those of you conducting research, for tenure or assessment or usage analysis or usability or any other reason, DO NOT DO THIS. This is classic exposure of long-tail information; the term of art is “accidental disclosure.” I bet you if the underlying dataset ever leaked, those eighteen Hawaiian students would be individually identifiable at the drop of a hat, along with their majors and lots of other information about them in the dataset that’s just plain nobody else’s business.

A colleague of mine called College and Research Libraries on this, but they responded that it was okay because the study only examined library use—never mind what other information is in the dataset!—and library use is not protected information. *pause* It’s not?! And you’re not even slightly concerned about what other information about these patrons might get correlated with these data? Then what does ALA Code of Ethics Article III mean exactly? It is NOBODY’S BUSINESS which individuals do or don’t get information from a library. College and Research Libraries made the wrong call here. If you do research and assessment, please make the right call: DO NOT PUBLISH SMALL Ns.
So, the main takeaway I want you to take away with respect to individuals’ behavior trails is that they are the Big Data gold rush, they are what data omnivores are chiefly after, and they really help data paparazzi hurt people. Behavior trails are mine-able. They are combinable. They are identifiable, with or without actual personally-identifiable information. They are sale-able, no questions asked, and they are in fact sold and reused all over the place. The N-S-A doesn’t even have to snoop a whole lot of information about people because they can JUST BUY IT from ad networks and content vendors! They are everywhere—and because they are everywhere, almost any new behavior trail is trivial to attach to the live human person who created it.

The inevitable corollary is that collecting and keeping behavior trails, never mind facilitating their reuse by researchers, vendors, assessors, WHOEVER, is a clear and present danger to individual patrons’ information privacy.

So. Where do behavior trails turn up in technical services?
The omnivores are inside the library.

The answer is, I promised to come back to this and now I am... and if you think I'm riffing on a classic horror-movie trope, you're right! Because this is just horrifying.

The data omnivores are inside the library, and they're called “e-resource vendors.”
Our buddies at Adobe got caught red-handed transmitting individual users’ reading behavior back to the Adobe mothership—not even just what books they were reading, which is bad enough, but HOW MUCH of each book and WHICH PARTS of each book. All of this tied to a user identifier, of course, so not even TRYING really to anonymize it.

And they were transmitting the data in the clear, not encrypted, and they got caught, and they said “oops, we’ll fix that”—but what was their fix? Just encrypting the data in transit. They’re still collecting it. They’re still storing it. They’re still mining it. I wouldn’t be surprised to find out they’re selling it to the big data brokers!

And what did we do, given that Adobe fuels a lot of our ebook programs? Once Adobe started encrypting the data in transit, not a thing, that’s what. Not a DANG THING did we do. We have let data omnivore Adobe destroy the privacy of ebook-loving library patrons, and we have done NOTHING.

Do you see now why I have concerns when Maciej Cegłowski holds us up as privacy exemplars?
Then there’s this one, and let me tell you, ad networks are THE WORST OF THE WORST data omnivores. You KNOW they’re selling the data they collect to anybody with a credit card, that’s their business model, it’s what they’re in business for! Privacy issues aside, ad networks commonly spread malware, as we saw recently with Equifax and TransUnion. So yeah, when our vendors put ad networks on their journals, that’s privacy endangerment, it’s wrong, and we shouldn’t put up with it in silence.

I would also love it if e-resources folks and library administrators argued with library IT to include tracker blockers by default on library patron computers. Ad-blockers, okay, I get that there’s an intellectual-freedom argument for not using them. But there ARE blockers that can be configured to focus on tracking only, and until we can shame content producers into not collecting or selling behavior-trail data, I’m in favor of trying to reduce the privacy harms in other ways.
I called out College and Research Libraries earlier, so I want to say something nice about them. Here it is—this article is fantastic, it’s open access, and you should read it if you haven’t already. As you may recall, I started this talk with the ALA Code of Ethics and the ALCTS supplementary guidelines to it. Here’s a thing about that: e-resource vendors DO NOT EVEN HAVE analogous ethics codes. They don’t promise ANYTHING with regard to patron privacy!

So, spoilers, the conclusion this article comes to is NO, library vendor policies DO NOT meet our standards. (I mean, you probably guessed that, right?) And all of you who choose vendors, who negotiate with vendors, who set up library technology to work with vendor offerings, who use vendor data in assessment—you are the only people with any hope of changing that.
I can value privacy all I want... but it’s workflows and systems that determine how accurate this is for my patrons.


So what else can we DO about all this? I like Angela Galvan’s formulation here, she says… Workflows and systems.

Now, I’m going to assume y’all know how to do a workflow audit, a catalog audit, the kind of thing that will catch Angela’s nine-seventies, so I’m going to skip it—again, not because it isn’t important, it TOTALLY is, but because I’m running out of time and I’m not the best person to talk about tech-services workflow and catalog auditing anyway.

I want to talk for a minute about systems.
For systems stuff that’s directly actionable, hey, I don’t even have to walk through this! Which is good, because that would take me a while.

There are specific actionable guidelines thanks to ALA’s Intellectual Freedom Committee and a bunch of volunteers. The ones most applicable to tech-services and e-resources folks will be... well, most of them, really, but cheer up—the lists aren’t hugely long and they’re pretty understandable, so dive in and make things better!
But let me pull out a few examples and another related document I suggest you read, okay? I’m indebted to Andromeda Yelton for this example—sometimes privacy violation is baked right into the standards our systems are based on.

SIP2 was designed to communicate between self-checkout machines inside the brick-and-mortar library and the library circ system. And SIP2’s designers reasonably assumed that the network hookup there would be wired Ethernet, which is pretty secure and private, so they didn’t demand that the data be encrypted for communication. I mean. They should have, just on principle, but I can kinda see why they didn’t.

And then library ebooks happened, and so libraries needed a way to communicate with ebook vendors to make a checkout happen, and SIP2 was just SITTING RIGHT THERE, so they used it. So now data about patrons and their ebook checkouts is flying unencrypted over the PUBLIC INTERNET.

Y’all, I can teach an UNDERGRAD how to sniff unencrypted data over the Internet. I’m actually gonna teach network sniffing this summer, I’m launching a mixed grad/undergrad class on digital privacy, safety, and security. I’m just sayin’, okay?

So two questions out of this. Do you know whether your ebook vendors encrypt SIP2 communications? Are you sure? And do you know what patron data you’re transmitting to your ebook vendors over SIP2—because it actually asks for a whole lotta patron data—and maybe the vendor doesn’t need or shouldn’t even get all that data?

Nobody intended this privacy-destroying outcome, it was an accident, I get that, but who’s going to prevent and remedy accidents like this if not us? Ask about the technology you’re working with. Ask where it collects patron data and where that data goes. I know that can be hard because nobody wants to admit they don’t know something. I’m saying, do the hard thing anyway! Ask anyway! Make people draw you diagrams. Whatever it takes to find the mistakes.
The URL for this is terrible, just plug the title into DuckDuckGo to find it, okay? Now, I’m not a huge fan of this document. I don’t think it goes NEARLY far enough in the direction of protecting patron privacy. I think it’s toothless and wishywashy and far too invested in the bankrupt notion of notice-and-consent, and way too easy for flagrant privacy violators to hide behind.

But. But this document has SOME guidance for our systems and how we treat them that I think is useful and actionable, and it’s something you can use to advocate with your higher-ups for good privacy and security practices that I think they’ll take seriously, so here we go.
2. Transparency and Facilitating Privacy Awareness

Library users need to be able to determine the extent of privacy protections provided and the boundaries of those protections as they use library resources. Libraries, content, and software-providers shall make readily available to users specific, non-technical statements that describe each stakeholder’s policies and practices relating to the management of personally identifiable information. These policies should also inform library users how they can protect the privacy of their data themselves. Such statements shall identify what data are collected, why data is collected, who has access to the data, how the data are stored and secured, when that data might be disclosed and to whom, and what the organization’s data retention and/or deletion policies are.

Library users can best take advantage of the privacy protections afforded by libraries if they understand the extent to which their privacy is and/or is not protected. Means of communicating privacy choices to users include outreach, inclusion of library-user communication methods in systems design, and user education. All parties involved in providing services should effectively communicate those choices to users. Systems should be designed in a way that facilitate understanding of policies through the use of simplified management of options.

So, whoa, this is a wall of text and I don’t expect you to read it all on the spot. The point of this is, a lot of today’s digital panopticon exists because NOBODY REALIZES IT’S HAPPENING or how pervasive it is. There’s no transparency around it, and nobody’s educating anybody on it. So one of the things tech-services and e-resources folks could conceivably do, and I’d love to see it happen, is deliberately make some of this more visible.
So, just as an example, who has OverDrive invited into their patron data? Google, it turns out—look, one thing, could library computers please change browser search bars away from defaulting to Google? DuckDuckGo doesn’t track searchers—and, OH JOY, a behavior-trail collection company called NewRelic. Awesome. I spent like half an hour puzzling through NewRelic’s privacy policy to figure out if it’s selling behavior-trail data it gathers for its customers, and you know what? I STILL don’t know, and all by itself that makes me suspect they are.

Is this information in your catalog? Database descriptions? Your outreach materials for OverDrive? Your knowledgebase? Your staff-training materials? Well, why not?

How did I find this out? With a well-known browser plugin called UBlock Origin. Simple to install, not too hard to glean information from. If it’s not installed on every patron and staff machine in your library, I think it’s worth considering, even if you don’t actually tell it to block anything. If you’re not using it to figure out and COMMUNICATE out about how your vendors are selling out your patrons’ privacy, I really think you could be!
How about our good buddy, our good ol’ pal Elsevier? Oh wow. Social-network behavior-trail web bugs from AddThis and Twitter, Google of course because everybody’s sold out to Google—seriously, if your library is using Google Analytics, just on principle, get that stopped—our unreliable data-omnivore buddies at Adobe, and then Optimizely, look them up, they’re another behavior-trail collector like NewRelic.

Awesome. Again, Elsevier is getting away with this why? BECAUSE IT’S NOT APPARENT TO PEOPLE. So let’s make it apparent, yeah?
9. Supporting Anonymous Use
Libraries and content- and software-providers must recognize the right of library users to be anonymous, should they so choose, and users should be provided appropriate affordances. Not all service capabilities may be available while a user remains anonymous, but reasonable accommodations to provide basic services should be made. When the collection and retention of a user’s personal data are required in order to access library resources or deliver library services, the library user should be informed that anonymous service is not possible.

So that leads me to this NISO principle, “supporting anonymous use.” I hate the word “anonymous” here. Actually, I dislike this whole so-called principle, it’s total weaksauce, but let me just focus on the word “anonymous.” It DOES NOT go far enough. It covers personally-identifiable information, sure, but it’s not clear to me that it covers behavior-trail and long-tail information. There’s much too much cover for information omnivores and even opportunists here.

So I want to make a stronger statement. *CLICK* Libraries should support information usage that is NOT TRACKED IN ANY WAY beyond what is ABSolutely necessary—and not just necessary for anybody and any reason, that’s weasel-wording in action, I mean necessary for the library to function at all. Will I trash assessment in favor of patron privacy? I sure will. Watch me.

We know how to keep behavior around analog materials like print books private, right, access-services folks? Keep minimal information, keep data on the stuff not the people, keep data secure, and only keep data as long as the book is out of the building. Why are we not carrying the same principles into e-resource system design?
And these two principles from the NISO document I’ll leave you with, because—surprise!—I agree with both of them, though I do think the flavor text on accountability is kind of weak.

We can’t get all this right, right away. No lie, it’s hard and we’ll have to pick our battles. There’s a lot of moving pieces here, and for data opportunists especially, a tremendous amount of very scary pressure from the Powers that Be to compromise on patron privacy. Figure out your ethical stance on patron privacy, work out how close you are to achieving that stance, and then do a little bit better every single day. That’s all I or anybody can ask of you.

But hold yourself accountable, please. Don’t hide behind “but research!” or “but assessment!” or “but the Powers That Be!” or “but personalized learning!” (which is a total dog whistle for surveillance of students) or “but it’s the vendor!” The library is the conduit between vendors, researchers, assessors, the Powers that Be, and the patron—if any of these people or organizations sells out the patron’s privacy, that is absolutely on the library, and since you work for the library, it's on you.

It’s on us, really. It’s on all of us.
People worth watching* **

- ALA Office for Intellectual Freedom
- Alison Macrina, libraryfreedom.org
- Angela Galvan
- Kyle M.L. Jones
- Andromeda Yelton
- Yasmeen Shorish
- Andrew Asher
- Tara Robertson
- Gabriel Gardner

*very abbreviated, unordered list
**not in the "paparazzi" sense
Thank you for caring.

Copyright 2017 by Dorothea Salo.
This presentation is licensed under a
Creative Commons Attribution 4.0 International license.
Questions?

Dorothea Salo
salog@wisc.edu