Preaching Digital Privacy at Academic Institutions

How to Raise Awareness and Take Action to Combat Surveillance at your School

Welcome to our session today: “Preaching Digital Privacy at Academic Institutions - How to Raise Awareness and Take Action to Combat Surveillance at your School.” We thank you for being here, and welcome questions throughout the session. There will be a few polls, and we will pose a few discussion questions, but we will also be monitoring the chat box for your questions and will do our best to answer them throughout the session.

Who We Are

Megan Kinney

Electronic Resources Librarian - City College of San Francisco

Claire Lobdell

Distance Education Librarian & Archivist - Greenfield Community College

Kelly McElroy

Student Engagement and Community Outreach Librarian - Oregon State University

Presenter: Megan
I am presenting today with my colleagues Claire Lobdell, who is the Distance Education Librarian & Archivist at Greenfield Community College in Massachusetts, and Kelly McElroy, who is the Student Engagement and Community Outreach Librarian at Oregon State University. I am Megan Kinney, and I am the Electronic Resources Librarian at City College of San Francisco.

Today's Plan

- ➔ Talk about the Library Freedom Institute & its guiding principles
- ➔ Explain the concept of threat modeling and how to apply it to your work
- ➔ Delve into privacy and surveillance risks to college students
- ➔ Examine the ways we've brought privacy education to our communities
- ➔ Discuss tools, lesson plans, and techniques for engaging in this work at your institution

Presenter: Megan
Today we are going to share about the Library Freedom Institute and the guiding principles therein, including the concept of threat modeling and how it can help you in your work. We will also talk about some privacy and surveillance risks specific to college students and the ways we are bringing privacy education to our campus communities. While doing that, we'll talk about some of the tools, lesson plans, and techniques you might employ to do this work at your institution.

From Librarian to Privacy Advocate

Library Freedom Institute (LFI) is a privacy-focused six-month program for librarians to teach them the skills necessary to thrive as Privacy Advocates; from educating community members, to installing privacy software, to influencing public policy.

Presenter: Megan
The Library Freedom Project was started by Alison Macrina following the Snowden revelations on government surveillance in 2013. She began working with librarians to better understand surveillance threats, privacy rights, and the tools needed to help mitigate surveillance risks in their communities. After being awarded an IMLS grant, Alison developed a free six month training for library workers called the Library Freedom Institute. The first cohort ran from June - December 2018. A second cohort will start this summer.

Cohort 1

- 13 librarians
- 6 months of online classes
  Each week:
  - 1 synchronous session
  - 5 hours of work/week (employer commitment)
- 1 in-person weekend

Presenter: Megan
The first cohort was comprised on 13 individuals, including public librarians, library technologists, a library school professor, and a few academic librarians (the three of us). The six month training occurred mostly online, in weekly synchronous online sessions. Each week, we were assigned a topic and were provided with several readings. During each synchronous online session, an invited speaker would talk to us about the topic of the week, with time for questions at the end. The work also involved online assignments, involvement in a discussion board, and one in-person weekend in New York. The entire institute is free.

Topics include

- General issues (e.g. CCTV, immigration)
- Library-specific issues (e.g. vendor privacy policies/practices)
- Technologies (e.g. Tor, Tails)
- General concepts (e.g. data minimization)

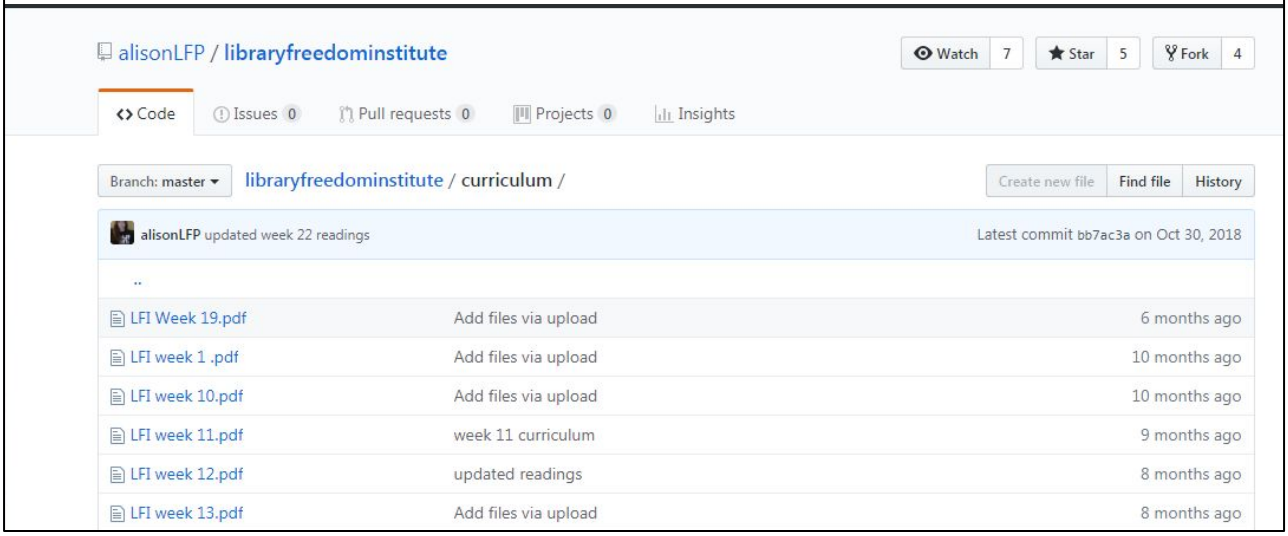
Full course materials at https://github.com/alisonLFP/libraryfreedominstitute

Surveillance Cameras by Quevaal

Presenter: Megan
Some of the weekly topics included closed-circuit televisions, immigration, vendor privacy policies, technology tools (such at Tor and Tails), and techniques like data minimization.

Github - LFI curriculum documents

https://github.com/alisonLFP/libraryfreedominstitute

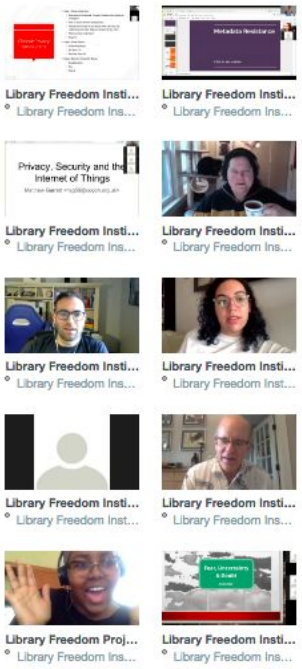


Presenter: Megan
You can look at all of the weekly topics in our github website, which we will link in the chat. https://github.com/alisonLFP/libraryfreedominstitute

Speakers including

- Nasma Ahmed, Digital Justice Lab
- Eric Hellman, Free Ebook Foundation
- Caroline Sinders
- Jessie Rossman, ACLU MA
- Freddy Martinez, Lucy Parsons Lab
- Eva Galperin, Electronic Frontier Foundation
- April Glaser, Slate

Videos available at
https://vimeo.com/libraryfreedominstitute



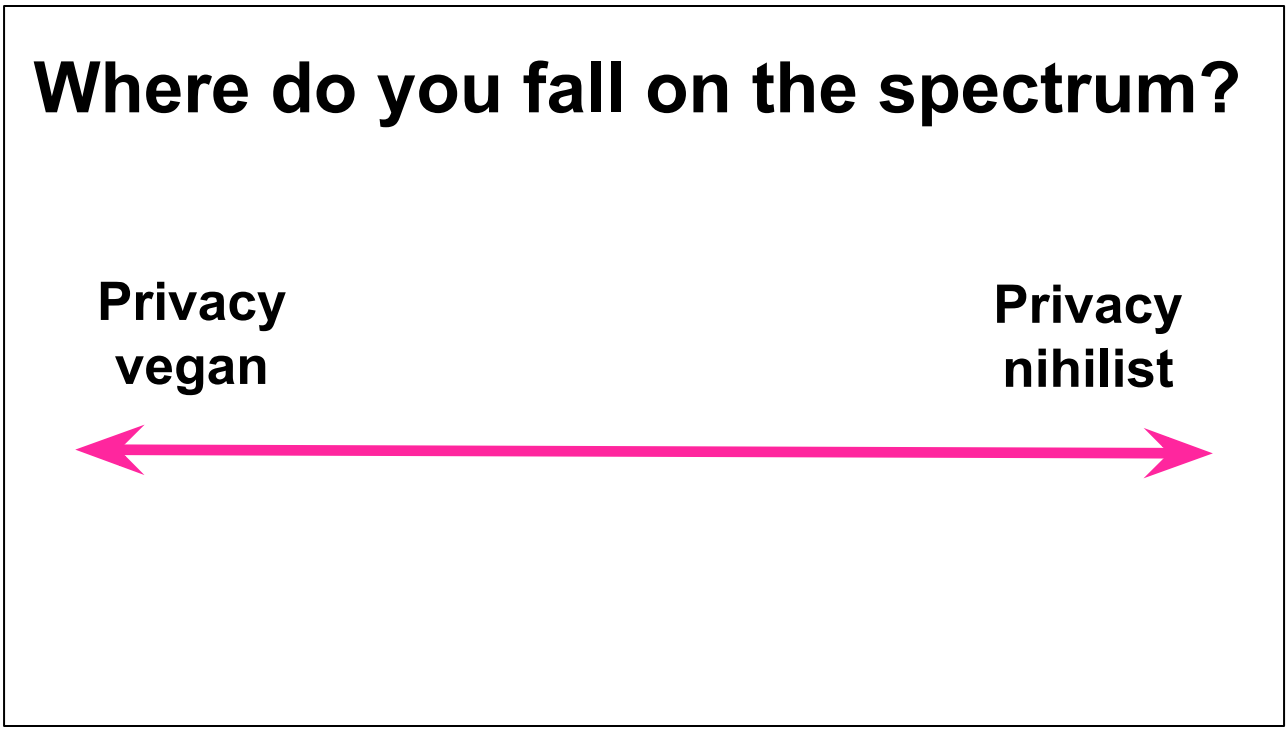
Presenter: Megan
As mentioned before, we were joined each week on our web based conference call by a variety of insightful speakers, including the individuals on this slide. All of the talks are archived on a Vimeo page which we will link in the chat box.

https://vimeo.com/libraryfreedominstitute

Nasma Ahmed from the Digital Justice Lab, Eric Hellman of the Free Ebook Foundation, Caroline Sinders who describes herself as a “machine learning designer/user researcher, artist, and digital anthropologist obsessed with language, culture and images.” We also met with Jessie Rossman from ACLU Massachusetts, Freddy Martinez of the Lucy Parsons Lab, Eva Galperin from Electronic Frontier Foundation, and April Glaser who is a journalist at Slate and co-creator of the podcast If/Then.

What do the words privacy and security mean to you?

Speaker: Claire
This is Claire. I'd like you to take a moment to think about how you personally define the words "privacy" and "security." If you want, you can share your own definitions in the chat box. For the purposes of this presentation, we're using the word privacy to mean the ability to decide who gets to know what about you, and we're using security to mean maintaining the integrity of something against an outside threat. These two concepts can be (and often are) in tension with each other. For example, closed circuit TV cameras on every street corner might make some people feel safer and more secure, but the tradeoff is that people are tracked and monitored as they go about their daily lives.



Enable draw feature in Adobe Connect
Presenter: Claire

We used a sort of shorthand in LFI when conceptualizing different attitudes towards privacy: the “privacy vegan” as one end of a spectrum and the “privacy nihilist” as the opposite end of that spectrum. The privacy vegan wants to live off the grid, disconnected from social media, email, and the rest of the digital world. The privacy nihilist says they have nothing to hide and the NSA knows everything about all of us anyway so there’s no point in fighting it.

Imagine this line is a spectrum between those two extremes. I’d like to ask you to mark where you think you fall between privacy vegan and privacy nihilist--not where you would like to be, but how you actually live your life. Consider what accounts you have, what information you share about yourself online, and what devices you use. You can use the drawing tool to make your mark and initial it.

After everyone has placed themselves on the line, would a few of you volunteer to explain in the chat why you placed yourselves where you did?

A primer...

Presenter: Claire
We're now going to go through and explain some of the broad concepts that guide the work of the Library Freedom Institute and Library Freedom Project. We'll also talk about a few specific tools, but there's also a resource sheet in the handouts for this presentation that lists these tools as well and links to readings about some of the things we'll talk about.

Harm reduction

A bin allowing for safe disposal of needles in a public toilet in Caernarfon, Wales.

Presenter: Claire
One of the guiding philosophies of LFI is the idea of harm reduction, which is a concept that comes from the public health field. In that realm it refers to meeting people who use drugs where they are, minimizing stigma, and promoting evidence-based interventions that reduce mortality, such as needle exchanges and safe injection sites.

In the digital privacy realm, harm reduction is a similarly destigmatizing approach. It means not shaming people for their online habits, but instead teaching about how tech companies mine and monitor our data, so that we can choose safer ways to interact with the digital world.

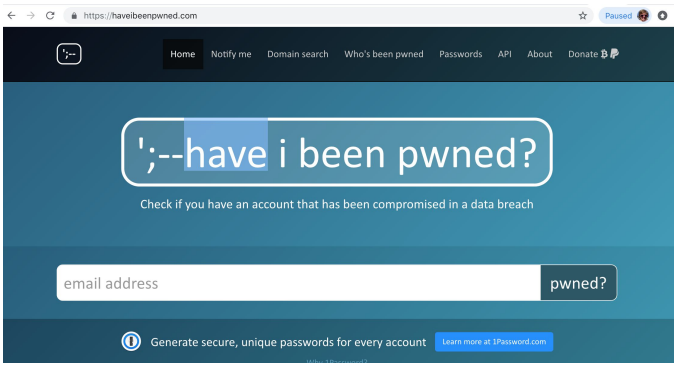
Data minimization

Reducing the amount of information about you out there limits potential misuse.

Presenter: Claire
Along with harm reduction comes the concept of data minimization: the idea that when you reduce the amount of information about you that's out there in the world, you can limit the ways that information is used and misused. This can include things like choosing search engines that don't track you, such as DuckDuckGo, changing your privacy settings in Google and Facebook; installing browser extensions like Privacy Badger or UBlock Origin that block third-party ad trackers; and opting your data out of data broker websites like Intellius, whitepages.com, and Mylife. These are some of those creepy sites that show up when you do a search for your name—they're the companies that compile information such as your current address and phone number, where you've lived in the past, how much money you make, and who your family members are.

In order to minimize your data, you need to get a sense of where it is.

You can’t clean up a data spill!
- April Glaser



https://haveibeenpwned.com/

Presenter: Claire
To that end, how many of you have looked yourself up on this website before—haveibeenpwned.com? If you haven’t done it yet, look up your email address, and you can see if your credentials have been leaked in any data breaches. Credentials are your email and password combination, and a lot of us—probably most of us—get into the habit of reusing the same passwords on multiple sites. When I looked up my personal email address and saw that it had been included in 12 data breaches—things like the 2016 LinkedIn breach, for example—this is what really convinced me to start using a password manager and stop reusing the same passwords on multiple sites.

Now, I use a really strong password that I created using something called the dice ware method as my master password, and then I use my password manager to create and store random, unique passwords for every other site.

Basically, there are three factors that make for a strong passwords: a strong password is long, random, and unique… but, human brains are really lousy at remembering lots of long strings of random characters. With dice ware, you roll 5 dice to get a 5-digit number, and then that number corresponds with a word on a long list of words, and you repeat that 5 more times to get a 6 word phrase. Because they’re words, they’re easier to remember, but you’re still getting the randomness because you’re rolling dice. You can find out more about it and get to a long wordlist by going to the Electronic Frontier Foundation website: eff.org/dice

Diceware password method

EFF.org/dice

Presenter: Claire
Along with harm reduction comes the concept of data minimization: the idea that when you reduce the amount of information about you that's out there in the world, you can limit the ways that information is used and misused. This can include things like choosing search engines that don't track you, such as DuckDuckGo, changing your privacy settings in Google and Facebook; installing browser extensions like Privacy Badger or UBlock Origin that block third-party ad trackers; and opting your data out of data broker websites like Intellius, whitepages.com, and Mylife. These are some of those creepy sites that show up when you do a search for your name—they're the companies that compile information such as your current address and phone number, where you've lived in the past, how much money you make, and who your family members are.

In order to minimize your data, you need to get a sense of where it is.

Threat modeling

A method for considering the potential risks to something you wish to protect, and the steps you'll take to protect it.

More info: https://ssd.eff.org/en/module/your-security-plan

Presenter: Kelly

Threat modeling is a method for considering the potential risks to something you wish to protect and working out the steps you are willing to take to protect it. You may also see it called something like risk assessment or risk management. The language may be scary, but it is actually a process that can be empowering -- someone in one of my workshops called it a tool of analysis to think about privacy.

https://ssd.eff.org/en/module/your-security-plan

Threat Modeling

1. Asset = what you want to protect
2. Adversaries = who you want to protect it from
3. How likely is it that you'll have to protect this asset?
4. What are the consequences if you fail?
5. What steps are you willing to take to protect the asset?

Presenter: Kelly

These are the steps in threat modeling. First, you identify whatever it is you want to protect. This is crucial -- it helps you narrow down to something concrete. One of the reasons people end up as privacy nihilists is a sense of overwhelm, that there is just no way . Your asset could be something like your emails, credit card information, or even the metadata from your phone calls.

Then, think about your adversaries, whoever you want to protect your asset FROM. Again, it can be appealing to throw your hands up and say you want to protect it from EVERYONE -- classic privacy vegan move. But realistic threat modeling means considering who you really are concerned about.

Third, think about how likely it is that you'll have to protect the asset. This might include how badly your adversaries want your asset, how vulnerable it is to attack, how skilled or well-resourced your adversaries on, and so on.

Then, think about the consequences. What, realistically, could happen if your adversaries get your asset?

Finally, based on your analysis, what are you willing to do to protect the asset? There may be possible protections that are unrealistic due to resources, inconvenience, or other factors. Threat modeling aims to help you map out the risks and make a plan.

Threat Modeling exercise

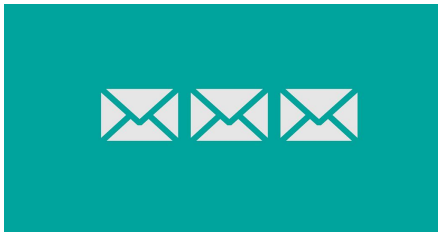
1. Asset = what you want to protect
2. Adversaries = who you want to protect it from
3. How likely is it that you'll have to protect this asset?
4. What are the consequences if you fail?
5. What steps are you willing to take to protect the asset?

Yeasted Banana Bread

Presenter: Kelly
It is way easier to understand threat modeling when you actually apply it to something. This is an activity I have done with students and with colleagues, so I'll ask you to chime in in the chat box with your ideas as we go through this.

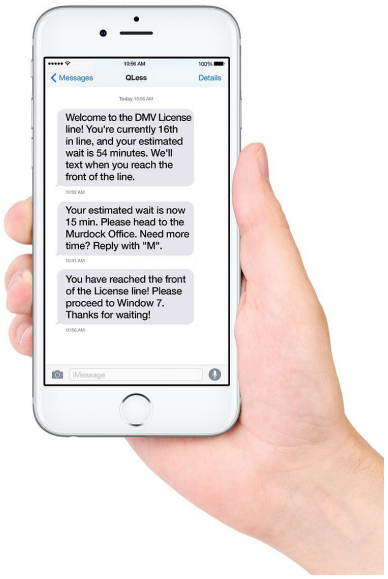
So, imagine that you just baked your famous banana bread for a party. It is cooling on a rack in the kitchen, and you have to run to the store to buy some decorations. As you prepare to leave, you notice your roommates circling the kitchen. Let's do a threat model to assess the situation. In this case, our asset is the banana bread, and our adversaries are the roommates. (There may be other adversaries we can think of, as well.) It seems VERY likely that we will have to protect this asset in some way. The consequences if we fail seem to be that the banana bread will get eaten, and there will be none left for the party. Terrible! So, what are steps we could take to protect this asset? Go ahead and type your ideas in the chat box. [give folks time to share]

This is a light-hearted way to practice something that can feel really grave. It also lets us model some of the things that come up when we use a serious example -- for example, I've had people ask about how to protect the banana bread from random strangers. How likely is it that someone will break into the house to steal the banana bread, if they don't know it is even there? Someone also suggested hiring a security guard for the banana bread -- what a delightfully absurd idea, right? But when it comes to protecting things where the stakes are high, there are still going to be things we COULD do that we really aren't willing to do.

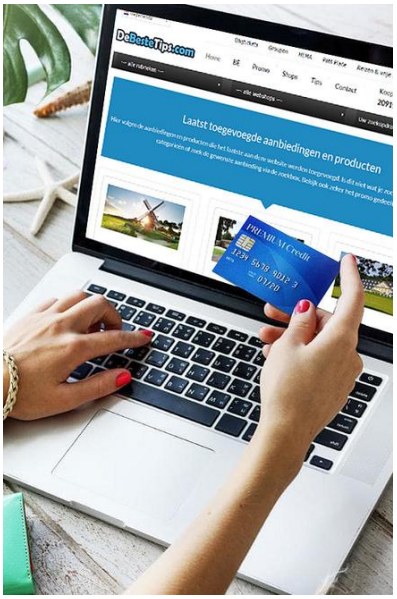


Via Joe the Goat Farmer

Via Quasic



Mobile Phone Messages



Via Elaine Smith

Presenter: Kelly

So, just to reiterate, your assets, when you consider threat modeling, could be all kinds of things -- emails, the content or metadata of a conversation, financial information, health information. And, given the complexity of systems, it may take some research to actually identify who the possible adversaries are. In our banana bread example, it was silly to imagine that some random stranger might break into the house to steal our snack, but in a digital environment it can be harder to identify who might know about your asset or be interested in it.

Privacy and Surveillance Risks to College Students

- Financial information
- Organizational affiliation
- Demographic information
- Immigration status
- Student services (for food insecurity, homelessness, health issues, etc.)

Presenter: Megan
Thinking about the context of threat modeling in our institutions, these were some of the privacy and surveillance risks we thought of (the assets that are important to protect) in a college environment. These risks include the vast amount of financial information our institutions collect about our students, but not just our students - their families as well. It brings to mind not only their FAFSA information, but how protected is scholarship information? Students divulge incredible amounts of information about themselves in order to be eligible for specialized grants and scholarship opportunities.

Additionally, our students also participate in a variety of student organizations, which identify them as interested and engaged members of various kinds. For me, I think about our Muslim Student Association, and other student groups that can become the target of hate incidents. At our institutions, we are also host to a variety of demographic information related to our students. In California in particular, I know we are engaged in work related to the opportunity gap, and the learning analytics around the different kinds of students we have at our institution are used heavily in assessment efforts. At our institutions, we may also be privy to the immigration status of our students, as well as whether our students are accessing student services for some of their needs, such as visiting the food pantry, our wellness/health centers, and more.

Can you think of any other privacy and surveillance risks specific to college students?

Can you think of any other privacy and surveillance risks specific to college students? Please use the chat box.

Threat Modeling in the Library

- What information do we collect, and in what systems?
- How do we protect those assets?
- Do student workers have access? What training do they get?
- What do we leak to our vendors?
- How are our public-facing computers and servers configured?
- What retention policies are in place?

Presenter: Claire

Now thinking about those risks to college students, bring it back to the library. What information do we collect on students? And in what systems? Are we collecting demographic information? Card swipe entry? Vendor logins? Search histories?

How do we protect those assets (the data we have)? What is our retention policies around these bits of information? Who is in charge of clearing it out? I know in the community college context, our students come in and out over a large span of time - sometimes right out of high school, a decade later for job training, and still again later for lifelong learning opportunities. While we may not be starting with the larger information held by the school, is it really necessary to hold on to their information just in case?

It's also important to think about who has access to the information. Do you have student workers? What training do they get around privacy?

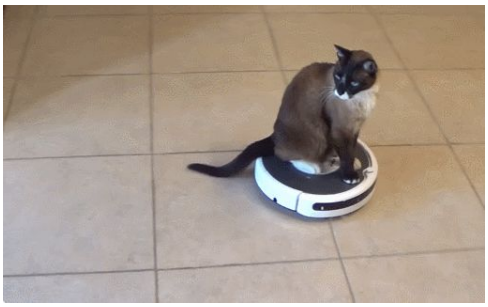
With regard to all the services we subscribe to, such as databases and e-services (like research guides), what information are we leaking to our vendors? Some libraries are subscribing to services to crunch the numbers on which library users are using which materials, and how these are impacting their success in the school. In this period of "showing our value," are we being thorough with what our vendors can see, and their security around said information?

Another thing to consider are the technologies students are engaging with in our spaces. For example, do students have to log in to use library computers? How are the servers configured? In many schools, student complete sensitive documents on library computers - are those files wiped so no one else can access them?

Lastly, retention policies are a must for working with the sensitive information we collect, and enforcement of said retention policies is critical.

As we think about the technologies we use in our personal lives and also the technologies we acquire and use as librarians, there are two guiding questions that I find particularly helpful to keep in mind.

Can this technology/information be used in ways besides the ways it's marketed?



Presenter: Claire
The first question is: can this technology or information be used in way besides the ways it's marketed? I think the roomba here is a great example of this. So, the way a roomba works as your cat rides it around your house and bonks into furniture and walls is that it's creating and storing a map of each room. In 2017, the CEO of iRobot, the company that makes roombas, did an interview with Reuters in which he said that they're going to begin selling those individual house maps to other companies, and then they was a big backlash and iRobot was like, "woah, woah, did we say sell? We meant share those maps with your consent," but either way, I think a lot of people hadn't realized that their robot vacuum was also a mapping technology.

Does this technology/data collection disproportionately endanger specific populations?

Presenter: Claire
The second question asks: does this technology or data collection disproportionately endanger specific populations. Megan already talked about some of the surveillance risks that our students face. It's important to keep in mind that the same features that may enhance convenience for some people—things like the ability to use biometrics to log into a device or gain access to a building, or the ability to remotely turn on apps that can locate a device—those same features can compromise other people's safety.

Greenfield Community College

- Presenter: Claire

I work at Greenfield Community College, which is a small institution in rural Western Massachusetts. Our student FTE is only a little over 1,000, and our students come from MA, VT, and NH. A number of the surrounding towns have only dial-up internet access, and the county in which we are located is one of the poorest in the state. At the same time, our graduation and transfer rates rank either number 1 or number 2 among MA community colleges—it keeps going back and forth—and we have a really awesome library and library staff.

I've tried to bring LFI to GCC in a number of ways, including by creating a privacy policy for the library, offering professional development, and creating classroom lessons and public workshops.

GCC privacy policy

4 months of conversations, info gathering, and drafts

Articulating who we want to be helped us change what we do.

Based on ALA Privacy checklists

Presenter: Claire

I started working on a privacy policy for the GCC library as part of an assignment for Library Freedom Institute, but it ended up being about a four month long process start to finish. I looked at policies for other libraries, and had numerous conversations with IT staff and the library consortium that runs our ILS in order to learn exactly how our different systems were configured—things like whether and for how long we keep server logs. I used the ALA privacy checklists as a guide, worked hard to keep the policy under two pages, and ran it through several reading level checkers to make sure that it came in below a twelfth grade reading level. It went through multiple drafts and revisions with library colleagues, including some heated discussions in library staff meetings about who we are and who we want to be. This process of articulating who we want to be led us to change some of our procedures, including what information we collect when creating library card accounts.

Poll: Does your library have a privacy policy?

Poll: Does your library have a privacy policy? (options: yes, no, I don't know, in progress)

Professional development

Privacy & information security baked into student worker training

In-depth retreat workshop for library staff

College staff training co-taught with IT

Presenter: Claire
Over the past year, I've also created digital privacy professional development for GCC staff. Privacy and information security are now baked into our student worker training. We start with having students read the ALA code of professional ethics, and then have one-on-one discussions with them about what those ethics mean, as well as specific scenarios they might encounter and how to address those.

I gave a digital privacy presentation at our library staff retreat this year and led staff through several activities that they can use with patrons, including threat modeling and creating dice ware passwords.

A member of GCC's IT department and I also worked together to create an information security training for the wider college staff.

Lessons & public workshops

Thinking about digital privacy lesson plan (on Framework sandbox), part of Don't Cancel that Class program

Public workshops open to larger community

Presenter: Claire

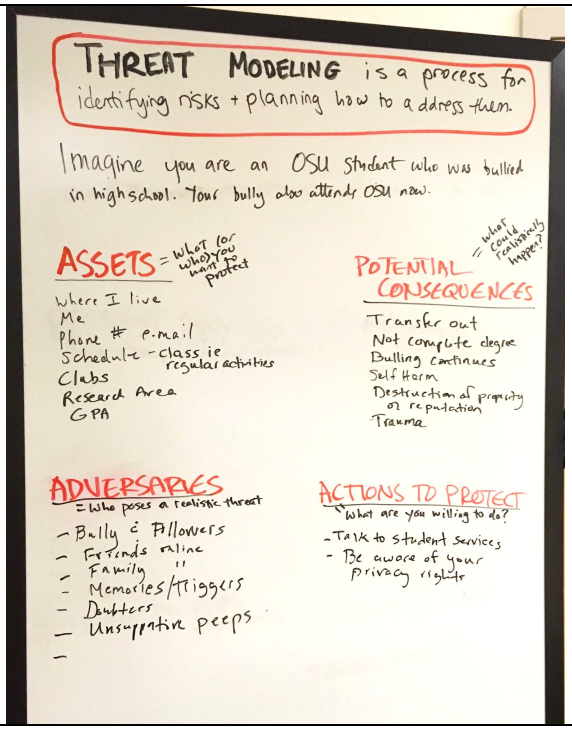
GCC has a Don't Cancel that Class program, which offers professors an alternative to cancelling class sessions, with a menu of workshops from offices across campus. I created a digital privacy lesson for Don't Cancel that Class (there's a link here to that lesson plan on the Framework Sandbox), but I didn't have any takers until I offered a lunch time privacy workshop that was open to students, staff, and faculty. I think sometimes faculty need to see for themselves that something is worthwhile before they take a chance in bringing it to their students. After I gave that public workshop, two different professors asked me to teach that lesson in their classes. I actually just pilot-tested one of the activities this past weekend with a group of Simmons library students. It's called the Rewards and Risks of Convenience, and in it, students debate the pros and cons of various app and software features. ("Does this technology disproportionately endanger any specific groups?") It was a lot of fun and sparked some really great discussion.

Oregon State University

Presenter: Kelly

This is Kelly again, and I'm going to speak about what I have been doing at Oregon State University. OSU is a large, research-intensive university with land, sun, space, and sea grant missions. There are about 31,000 students, about 5000 of them graduate students. To implement what I learned through LFI, I have mostly focused on incorporating them into my teaching and outreach, which is my primary assignment.

Student workshops

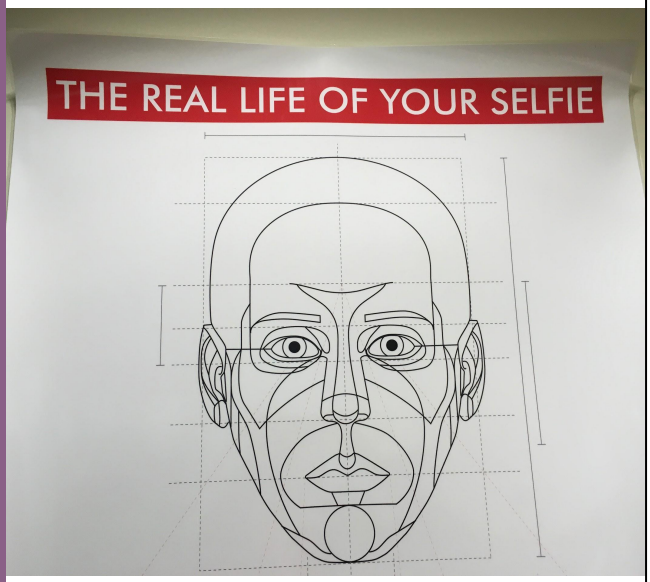


Presenter: Kelly

Because my main role at OSU is in student engagement and outreach, I have tried to find ways to incorporate digital privacy and security into that work. One way has been through direct instruction to students. Some of this has been through credit-bearing courses, like a one-shot focused on protecting financial information for a first-year experience course focused on financial literacy. But I have also looked to do workshops for groups of students, with a focus on peer educators. One example of this is with the peer advocates in our Office of Peer Advocacy. These students work with other students who are navigating difficult situations on campus -- for example, navigating a student conduct issue, or . We practiced threat modeling, using the banana bread example, and then walking through a more complex example relevant to their work, which you can see on the slide. We discussed tools including the Tor browser, which was new to students, and password managers. I'm hoping to follow up on this with a Pizza and Privacy event, inspired by the New York Public Library's Privacy Week programming, partnering with this office and others on campus.

I want to say specifically that I have encountered colleagues who think that students aren't interested in or concerned about privacy, but I have never found that to be true. The students I've worked with have all been curious and shared their own worries. They often were surprised by the tools available -- the peer advocates had never heard of Tor browser, for example -- but they certainly recognize that there are things to be worried about.

Glass Room Experience

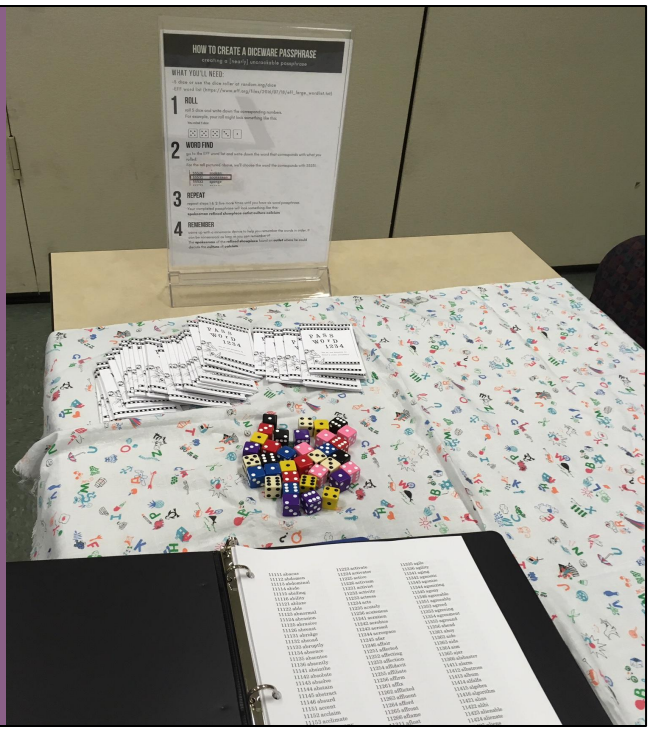


https://theglassroom.org/host-your-own

Presenter: Kelly

Another mode I've used is exhibits and other outreach activities. In January, we hosted the Glass Room Experience, which is a public exhibit, self-guided tour exploring issues of digital privacy and security. It is a project of Tactical Technology Collective, which does social practice art focused on technology, and the Mozilla Foundation. Libraries can sign up to host the exhibit at the URL listed on the slide here -- it is free to you, and pretty easy to set up. In my library, we set it up in a high traffic area, and just made sure that we kept making copies of the handouts as they were depleted. I believe that some instructors encouraged their classes to come through, but we didn't hold any formal events in the space.

Trainings for library workers



Presenter: Kelly

Finally, most of what I've been able to do so far is actually training and conversation with library staff. Much like we have in this presentation, I have focused on the harm reduction approach, and the use of threat modeling to identify potential changes in practices.

When I speak with library workers, I emphasize that privacy and security is everyone's work. So, even if I don't work directly with vendors, it is important for me to understand the privacy implications of using our online database when I teach students. This photo shows a diceware set-up, like Claire described, which can be used to develop a strong passphrase. Something like passwords cuts across many types of work -- our info desk staff often help users navigate resetting or creating a password, and certainly all of us in our work have passwords for different systems.

I have done a few workshops within my own library, and am currently working with Madison Sullivan at the University of Washington to prepare some trainings for the Orbis-Cascade Alliance, a regional consortium. We got a grant to do all-day trainings to build capacity on digital privacy and safety. We'll be doing one in Seattle in May, another in Portland in August, and one totally online. If you're in the Pacific NW, please keep your eyes open for those announcements!

Megan's Implementation

- In one-shots
- In an embedded project
- In a consortium committee

Presenter: Megan
This is Megan again, and I'm going to use the next set of slides to show how I have been working topics of digital privacy and surveillance into my work at City College of San Francisco, mainly, during one-shots, in my embedded project, and in a consortium committee.

City College of San Francisco

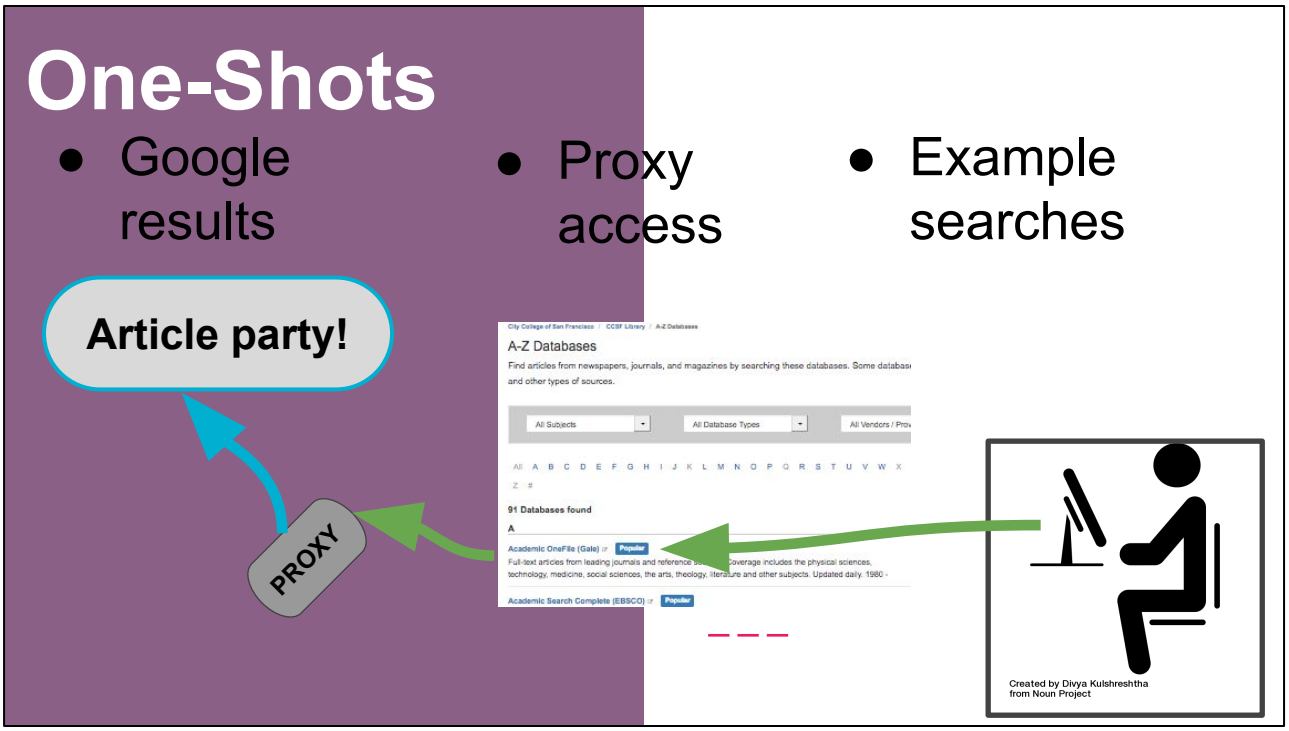
STUDENT INFORMATION			(view historical trend)
Students			33,179
Gender		Ethnicity/Race	
Female	52.8%	African American	7.5%
Male	44.7%	American Indian/Alaska Native	0.3%
Unknown	2.4%	Asian	30.7%
Age		Filipino	5.9%
Less than 20 years old	16.9%	Hispanic	25.0%
20 to 24 years old	26.6%	Pacific Islander	0.7%
25 to 39 years old	37.6%	White	23.1%
40 or more years old	18.9%	Two or more Races	5.0%
Unknown	0.0%	Unknown	2.0%

INSTITUTIONAL INFORMATION	
Full Time Equivalent Students	20,772.9
Credit Sections	5,619
Non-Credit Sections	0
Median Credit Section Size	21
Percentage of Full-Time Faculty	72.8%
Percentage of First-Generation Students	45.6%*
Student Counseling Ratio (FALL 2016)	587:1

* Insufficient data

Presenter: Megan
City College of San Francisco is a community college in San Francisco with 10 locations. San Francisco is both a city and a county, so our ten locations operate as one school. Our full-time equivalent count currently at just above 20,000. You can also see the demographics of our students on this slide. We provide library services at all ten locations, but in different amounts.

https://scorecard.cccco.edu/scorecardrates.aspx?CollegeID=361

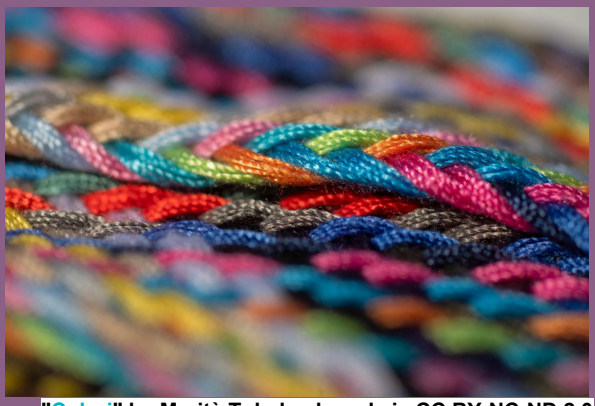


Presenter: Megan
I have been at my institution for a little over six months, and while I work on the relationship building it takes to make institutional change, I am bringing privacy concepts into my teaching. For example, in one-shots, I try to have a critical moment about algorithms. For example, when we are looking at a Google result list, I ask "How are these items ordered? Why are they listed the way they are?" We talk about search algorithms, how they can have bias baked in, and how if you have a Google account (such as our school accounts), how those searches are logged. I also briefly explain how proxy access works in a small discussion about how to log into our resources. I explain that by logging into the school system, it then lets us translate their IP address into the school's IP address, and this address is what the database vendor uses to let them in. Lastly, when I am in a one-shot, I often do demo searches. In many of the classes I work with, the research topics are open ended, and students are still deciding. When I run a demo search in Google or our discovery system, I often use a technology topic as my sample - such as digital privacy, facebook, and democracy, etc. I haven't seen many students choosing technology topics over something "hot" like marijuana, but a small part of me hopes that students will see that the technology in their lives is ripe for academic/issues based research.

Can you think of any places to include privacy & surveillance topics in your instruction?

Can you think of any places to include privacy & surveillance topics in your instruction? Use chat box to respond.

Embedded



"Colori" by Maritè Toledo shared via CC BY-NC-ND 2.0

- More detail on “what librarians care about” and “how librarians can help”
- Class research topic: technology / big data

Presenter: Megan
One of my other privacy integration points has been in my embedded project. At the request of our english department, we are engaged in a pilot project this semester, where five librarians are embedded in five different transfer-level english courses. In these embed projects, the english department is funding 20 hours of time for each librarian to teach a series of workshops, and collaborate with the english instructor. As luck would have it, the instructor I am working with has technology as the topic of the class. In my first session with the students, in explaining how what librarians can help with, I talked about my training with the Library Freedom Institute, and the variety of topics they can come talk to me about. In the second session, the students were in the process of reading *Dataclysm*, which discusses big data through the lens of online dating.

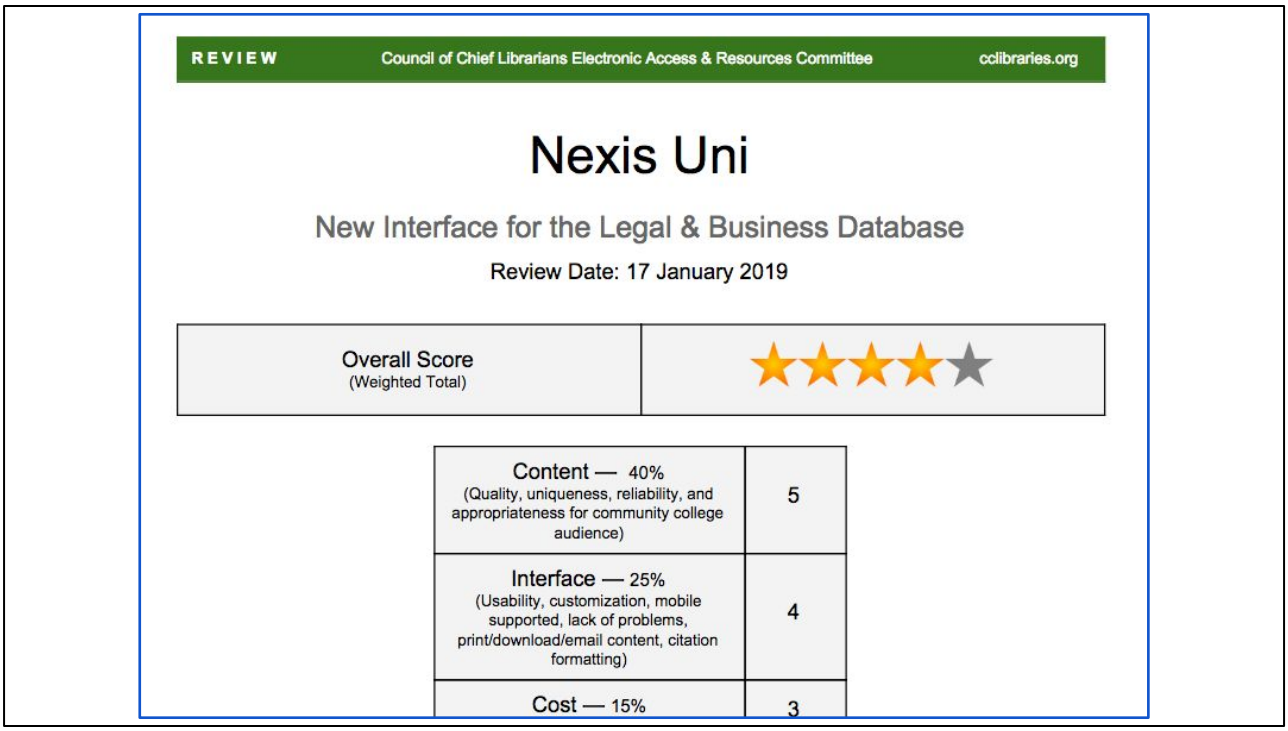
Presenter: Megan
Students then choose a research topic related to big data and whatever they like, and in our second workshop, the instructor asked me to talk further about digital privacy and surveillance issues to help them think of potential topics. We spent about 45 minutes brainstorming places where "big data" exists, when we "felt: the shift move from interesting to creepy, and how we feel about that. I briefly explained that they could come meet with me one-on-one if they had concerns, where we would come up with a plan (threat model together) for how they could mitigate their risk.

COUNCIL OF
CALIFORNIA COMMUNITY COLLEGES
CHIEF LIBRARIANS

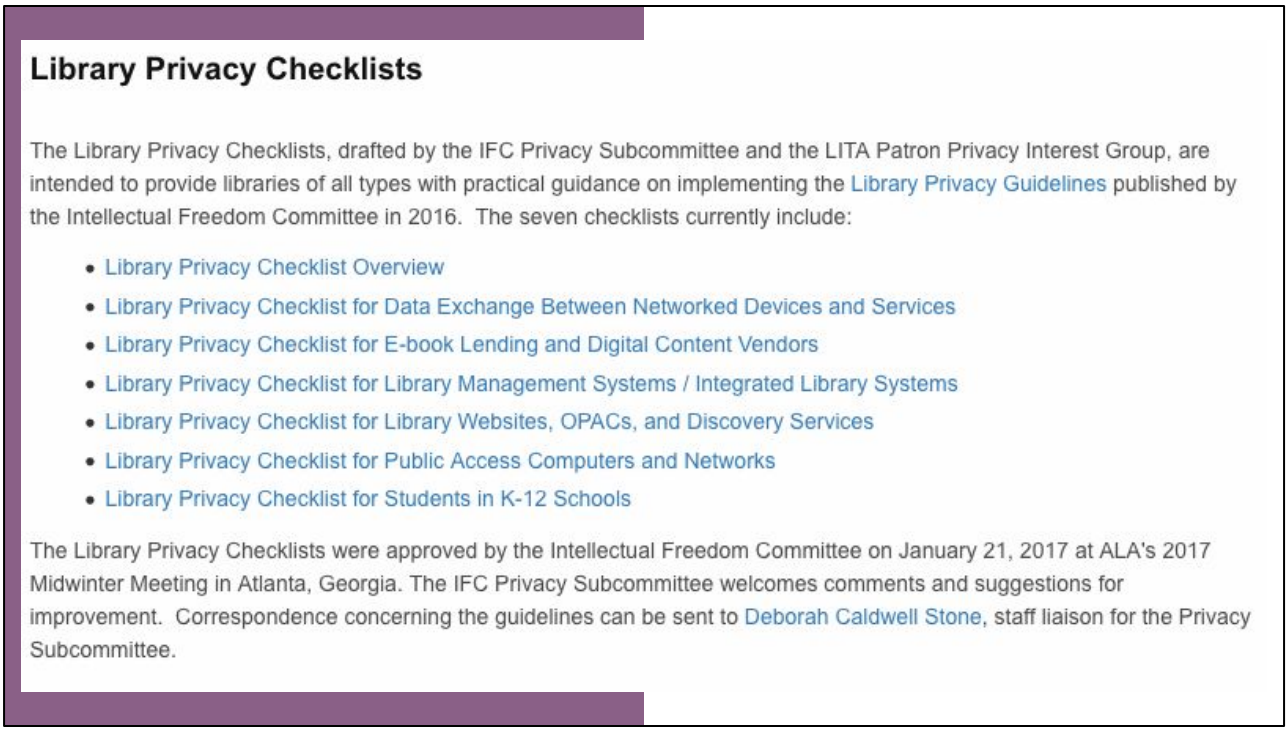
Consortium Engagement

- Who do you buy your databases through?
- Do you have the ability to include privacy in your considerations?

Presenter: Megan
Lastly, I wanted to bring privacy and surveillance awareness to my electronic resources work. California has 114 community colleges in our system, and many of us purchase resources negotiated by the consortium. I recently joined the Electronic Access and Resources Committee of our consortium. We talk about vendor issues, as well as evaluate potential consortial purchases. In this evaluation process, we write and publish reviews.



Presenter: Megan
Since joining the committee in November, I asked that we discuss the move of vendors from anonymous proxy access, to unique user logins. I also share information of interest among our committee, such as the “Statement on Patron Privacy and Database Access” posted by Stanford recently. (https://library.stanford.edu/using/special-policies/statement-patron-privacy-and-database-access) I have also asked that we consider “What data are we passing to the vendor? What is their retention policy?”



Presenter: Megan
Most recently, I brought up the Library Privacy Checklists from ALA (http://www.ala.org/advocacy/privacy/checklists), and asked if we could incorporate some of these elements into our review process. Moving forward, a privacy category will be added to our reviews (https://cclibrarians.org/consortium/reviews), so libraries considering a subscription can make choices with privacy in mind.

So, what does all this mean for you?

Presenter: Kelly

So, we've outlined major concepts from the Library Freedom Institute, and talked about how each of us has begun to implement them on our campuses. Our hope is that our stories have sparked ideas about how you might deepen your engagement in digital privacy and security in your work. Hopefully you are thinking about where you might bring up conversations about these issues, plan to make concrete changes in practices and policies, and teach as you yourself learn. Consider what barriers exist and who your allies might be.

What you can do right now

Do

- Data Detox
- Look at NYPL Privacy Week programming
- Use strong passwords
- Duck Duck Go yourself (and then some)

Don't

- Tag people without their consent
- Provide unnecessary info
- Keep old accounts

Claire's list of resources: http://www.gcc.mass.edu/library/files/2019/03/Privacy_resource_sheet2019.pdf

Presenter: Kelly

We have found that when we talk about these issues, whether with students or colleagues, folks often want some concrete things they can do right now. These are some of the low-barrier starting points we recommend:

- The Data Detox is a project of Tactical Tech and the Mozilla Foundation, and is a simple 8-day program to begin to change your habits around data hygiene. It can be fun to do with a group -- invite your department or your family to do it with you.
- New York Public Library did fantastic programming for Privacy Week last year, and browsing their listings is a good way to get inspired for what you could do in your library.
- Claire talked about creating a diceware passphrase -- using strong passwords, and a password manager, is a behavior change that you can do incrementally and immediately.
- We had "google yourself," but changed this to Duck Duck Go yourself, so you might consider BOTH changing your default search engine to DDG, which does not track the way that Google does, and also, doing searches for yourself on basic search engines, but also in more specialized marketing and data broker websites.

As for simple things to NOT do, these mostly fall under approaches to data minimization:

- Don’t tag people on social media without their consent. In fact, don’t post photos of people without their consent -- remember the definition of privacy that Claire gave, about the ability to decide what gets shared about you. You can enact this with your own friends and family.
- Don’t provide unnecessary information. If a field isn’t required, don’t fill it out!
- And don’t keep old accounts. If you no longer use Animal Crossing, delete your account. Policies and practices vary about deleting data after an account is closed, but it is one way to start trimming your data footprint.

Finally, Claire has a great list of resources to get you started, which you can download at the URL listed on this slide.

Questions? Ideas to share?
We are watching the chat box!

Megan Kinney

mkinney@ccsf.edu

@mkinney0

Claire Lobdell

lobdellc@gcc.mass.edu

@claibrarian

Kelly McElroy

kelly.mcelroy@oregonstate.edu

@kellymce

Presenter: Kelly

Thank you for attending “Preaching Digital Privacy at Academic Institutions - How to Raise Awareness and Take Action to Combat Surveillance at your School.” We have a few minutes left, and will be happy to answer questions we see in the chat box. Thank you for your time!