Digital Privacy Tools for Daily Living

ANDREA JIMENEZ: Recording. Welcome, everyone. Good evening. This is Digital Privacy Tools for Daily Living.

My name is Andrea Jimenez. I'm the program coordinator at Global Connections. And our mission at Global Connections is to bring you engaging co and extracurricular events and activities wherever you happen to be.

Presenting for us tonight is Lorena O'English. She's the Social Sciences and Government Information Librarian at WSU Coleman. So the presentation will be about 45 minutes long.

We will have about 20 minutes for Q&A at the end. But if you have questions throughout the presentation, feel free to leave those in the chat. And we'll go through them. And yeah, if you have any technical difficulties, you can also let me know. I will now pass it over to Lorena.

LORENA O'ENGLISH: My dogs. It's OK. I'm ready now.

So yes, I'm Lorena O'English. And I'm a librarian at WSU libraries.

And I got interested in digital privacy some years ago when it actually all started when too many of my colleagues would not log out of their email. And I kept on seeing their email. And I went to classroom computers and that sort of stuff. And that actually just got me started in thinking a lot about digital privacy and some of the broader issues. And I just got more and more interest.

But before I start, I want to tell you a couple of things. First of all, I'm at home. And my husband isn't here. He was supposed to be here.

So my dogs are going to wild in the background. Hopefully, I won't have to turn on the sonic collar. But I might.

The second thing is that I hurt my back about six weeks ago. And sometimes I tweak my body, and I hurt it. So if you hear me say ow, that's what's going on.

OK, are y'all ready? I can't see the chat. So I'm flying blind here.

OK, all right, come on. Let's try this again. From the beginning, here we are.

OK, when you start talking about digital privacy, it's a very, very broad topic. And so I just wanted to talk a little bit about the things I'm not going to talk about, which is identity theft, scams, bullying, medical records, privacy, et cetera. And these are all really important issues. But they're not within the realms of the time that I have or the scope that I have. So we won't be discussing those.

But sometimes-- I wanted to start off with this idea that people think that privacy protection is difficult. And this is actually from a Pew study, Pew Research study, in 2015. But there's an update in 2019 that pretty much says the same thing.

People are really concerned about their privacy. But they feel that enhancing their privacy protection is very difficult for them to do and should oftentimes be managed more by the government, by legal reasons, by corporate considerations, et cetera. But as we're going to talk about today, the thing is that it actually really isn't that difficult to put a basic level of privacy on what you're doing.

So the way I look at this is I look at this through a harm reduction framework. I'm not trying to totally protect myself because I can't do that. There's just no way. But what I can do is make small tweaks to the way I use the internet, things that I add to my browser, things that I remember to do that will certainly diminish the likelihood of my information being stolen or my privacy being repeated. These things are low threshold applications.

They're not-- they don't cost anything. Well, actually a couple of them do. But there's some ways around that as well. But there are things that can make a big difference without a lot of work on my part. And that's really what I'm interested in doing because I'm self-taught on this.

I actually learned this all myself going. I'm not an expert. I'm just figuring it out as I go along. And I'm also really lazy. I don't want to have to change my behavior in very difficult ways. So I'm going to be offering you a digital privacy tool kit, not a comprehensive one.

It's not necessarily the best or even the best for you. And this is an ever changing ecosystem. The threats and the protections are constantly evolving. So what we have now, what we're dealing with now might be very different from the way it looks in a couple of years.

So I'll be looking at this through three different lenses of digital privacy and digital protections. First one is hardening. Second one is hiding. And the third one is homing.

And, Andria, I actually somehow managed to lose my cell phone. So you're going to have to give me-- can you give me 10 minute intervals over the course of the hour? Because I want to make sure I'm pacing this right.

ANDREA JIMENEZ: Sure thing.

LORENA O'ENGLISH: OK, thank you. We're going to start with hardening. So here's a really basic thing. Cover your webcam.

And this is a picture of Mark Zuckerberg. It was taken a couple of years ago in 2015. And you can see I have a little green arrow there. Right in the corner, he has a little piece of tape over his web camera. And you should, too.

And it doesn't have to be tape. These days you can find-- I hope you all can see this. A lot of places offer these tiny little things that are very, very thin that you can put on your laptop and on your desktop-- I have one on my webcam right here-- to actually be able to close it and open it when you want to.

And you'll have something. A piece of tape is always fine. But cover your webcam because there have been a number of instances where people have been able to break into web cams and get information that they shouldn't get. So that's something really small that is a way to harden the physical likelihood of having your privacy impeded.

Second thing to do is update everything. And I mean everything. And this is something a lot of us are like oh, I don't want to update my software. It'll take forever. But it's really important.

We need to update our software, our apps, certainly our browser extensions, any antivirus that we might have, our firewalls, and our privacy settings. And this is something that can't be something that you do like once a week. When it comes to your own stuff, you have to do your updates as often as they come up because the longer you go without doing updates, the worse it can really cause problems.

So I actually went to a digital privacy webinar myself about a month ago. And it was really interesting to me that the person who was talking was a person with a lot more expertise than I had. And yet the things she was talking about really mirror the things that I'm going to talk about today.

So just improve your securkitty. And I hope you all will forgive me, the sort of dad jokes over there on the corner about positively remarkable and warm-and-fuzzy feelings. This was actually something that Microsoft, Intel, and somebody else I can't remember, a campaign they had a couple of years ago to remind people to update. They thought that people would be more likely to update all their stuff if they saw cute kittens.

The next thing we're going to talk about is passwords. And normally, I teach this in two hour long workshop. And we spend a lot more times about passwords.

But passwords are really important. And I want to start off by doing a pre-test. I'm going to go to a website called haveibeenpwned. And I'm just going to pop over into this website.

And I'm going to go over here to where it says home. And I'm going to put in my wsu email address and click on pwned, or "powned," I guess, as opposed to owned-- "powned."

And you can see that I have been pwned, that these are breaches. These are collections of email addresses and general information held by websites and organizations and corporations, et cetera, who had a security breach where people were able to get in touch of this information. And you can see we have a USA business, data and leads, data enrichment exposure, most of these.

I was like, what the heck is my information doing in there? And it turns out that these are data brokers. These are people who collect data and then sell it to other people who they themselves got breached. And so that data is now available over on the internet.

And of course, anytime you're notified that your email address has been breached, you need to go change all your passwords. So that takes things a lot more complicated. But this is quite a lot of passwords being pwned. So I really need to think about my passwords because it turns out that passwords is actually something very complex.

And one of the things is that we're online hoarders. We have an enormous number of accounts. This is from a infographic a couple of years old. And I suspect that the number is actually even harder now.

But the other thing is that because we have more online accounts, we forget our passwords more. So we're always having to go through password recovery. And we oftentimes will use the same password over and over and over again, or else we get-- we create something that's so ridiculous that we're certainly not going to remember it the next time.

So we have to go through password recovery process yet again. And you end up just putting in your dog's name or something else like that. And so that's something called credential stuffing. Actually it turns out that when hackers get these data sets of information, they'll actually run variants of your passwords across all sorts of sites.

Because if you say-- if your Facebook site is lorenafb!, it's very likely that your Twitter site is Lorenat exclamation point. So you got to think about these things. You think you're being careful.

You can remember this. But it's being different. And yet, hackers have an enormous ability to actually break through a lot of these.

So let's go back to that have I been pwned site. And it is a legitimate site. And it's something really important to look at.

If we go over here to the about, you'll see a little bit about who this is. And you can see it's done by someone who works at Microsoft. So he's definitely got some credentials.

I just want to notice a couple of the other things here of who's been pwned. These are corporations. And you can see it's all alphabetical. But there are breaches happening almost every day.

The sad thing is sometimes we don't find out about those breaches until they've been around for a couple of years. And you never had a chance to change your password. You can see also that you can actually put in your email address and be notified if your email site shows up on this.

And I recommend that everyone do that. And I'll show you in a little bit-- I'll show you a link that I have-- And I think I had it on the main slide-- that has most of the links that I have here. So you can go back and do this yourself if you didn't catch it where I'm doing this.

OK, so let's talk a little bit about password hygiene. And I'm not going to talk about it too much. But basically, you want to delete accounts that you're not using. And there are probably a lot of them. You want to make your passwords complex, as complex as possible.

You want to think about things like-- all the things we've been told. Use a passphrase instead of-- you throw in some symbols, numbers, and capital letters, et cetera. Drop, don't reuse old passwords.

And this link takes us to a website about breaches that actually shows how often people actually do reuse their old passwords. And that's just an invitation to problems. Change them frequently or maybe not.

There's actually a discussion happening about whether absolute requirements to change your password every three months are actually more of a problem than of a benefit. So a lot of times what happens is you just have the same old password. You just add in one more character at the end of it.

That's what I do sometimes. And I ask in classes every so often when I'm logging in for a WSU network ID. And a surprising number of students tell me they do the same thing.

Log out when you're done. Make sure-- don't leave-- wherever you are, whether you're on a public computer or a private computer, log out, is the thing to do. And really think about whether or not you want to use the in-browser password savings.

A lot of times it's really convenient to do that. But it's not always the safest thing for you to do. So there are options.

So we're all a little bit more familiar with multi-factor authentication now because it's being used at WSU. And it's multi-factor because the idea is that you go beyond a password. It used to be a single factor.

You had a password. You log it in. You're good to go.

So multi-factor looks at three different things, something you know. And that's usually like your password, something you have. That could be your cell phone or in some cases a little thing you can see here, a security key. This is a Yubico security key. It's a little thumb drive that actually holds all your passwords on it, or something you are.

We don't do a lot with something you are. Well, I guess, you might if you are an Apple user because something you are is basically your thumb print, or your retina, or something about

you yourself. But most of the time we really focus on something you know and something that you have.

And there are a number of different modes. And I just want to comment. And you can see I just want to comment on one.

In general, if you can stay away from texting, that's a really good thing to do because texting, out of all of these, texting is the things that can be breached the easiest. So you can have a voice call. They won't leave a message.

I actually have mine to have things set up to go to my work phone number because I can always get to that as well as my home phone number. And authenticator app is something-- is really great. We use OKTA at WSU. And I believe they have one as well.

But I'm using the Google authenticator. And you can see there are other ones as well. And basically, it's on your cell phone.

And when you need to authenticate with your multifactorial indication, you just open up the app. And you'll see a six number combination that you can then type in. And it's not something that went through the airwaves at all.

So it's not something that can be captured. It's a really good safe way of doing this. But of course, you have to have your cell phone.

And in fact, a lot of these, actually, you have to have your cell phone. Or you have to have that physical security, et cetera. So I just want to tell you, I actually had a case last year where I lost my cell phone.

And I just ran into problems because, of course, I wanted to change on my accounts and everything. But it just was a mess. I couldn't-- my cell phone was totally out of power when I lost it. It was a disaster.

So luckily, what I had done was I had a hardcopy. I had a list of emergency passwords that I could use. And most of the time, when you have multi-factor authentication, not with WSU but with other sites, they will let you print out a list of codes. And that's your last stitch thing.

You can put in one of those codes. Use it once and then throw away because it's gone. But here's a suggestion. And this is what I do.

Consider a purloined letter tactic. And that's from a mystery story by Edgar Allan Poe way back in the 19th century. And it hinged upon the letter in question just sitting on a mental place in plain sight to everyone.

So a really good thing to do is to actually take these emergency codes and put them in your wallet or your desk or whatever. But don't say emergency code on them. Put them in a place where you will know what they are.

They're in a list of phone numbers. And there's something that you know. So they're basically-- unless somebody knew that that was the emergency code for your Google account, they would not know what it meant at all. And yet, you do because you put some key there. So you know that.

But really, in the end, that's really important because things happen. You can lose your telephone. You can lose your smartphone. You can be locked out of your smartphone.

You can put your physical security key in the washer and have it be broken. There's any number of things that you can do. So that's an option that you really want to think about.

OK, finally, I want to talk about password managers. And this is the third or fourth time that I've taught this. And every time I taught this in the past, I was like oh, password managers. I know I should use one. I just don't want to.

The last time-- oh, I've tried one. But I can't quite figure it out. Well, since then, I have changed.

I use a password manager program. And it is amazing. It has changed my life. Now, instead of me coming up with passwords, I use it to generate passwords that are very hard to break. If I need to change a password, I can just have it take care of it for you.

It remembers my passwords. I can access it on my phone, on my tablet, on my desktop, anywhere that I am. And I really, really recommend it.

And I've looked at a lot of articles about digital security. And every single one of them recommends using a password management program. And I, at WSU, I went through WSU systems, library systems, which is where we talk about IT in the libraries. And they just installed my password management program onto my computer.

It works. So I have access to that there as well. And I also have it through my browser. Although, that one, you have to be really careful about.

And there are a number of them. I listed three of the ones LastPass, DashLane, IPassword, or 1Password. Which one is right for you, hard to really say. So I just did a little bit of searching. I went to PC Magazine. And they looked at their 2020 list of best password management programs.

I looked at the Wire Cutter, which is a recommender site through the New York Times. When you're looking at these sorts of things, when you go searching on the internet, talk to somebody

you trust. Or when you go searching on the internet, don't look at some arbitrary blog of someone that says password management sites ranked or something.

Look for names that you know. The New York Times, PC Magazine. Look for recommendation-- I hate these things. I can't ever find-- no, now there we are.

Yeah, look for something that gives you a sense that this is valid. Because password management programs and other things are really big business. There's a lot of people out there who want to put up a site that will actually be an Astroturf site, telling you how great their service is because they want to sell it to you because they're the ones who are providing it.

So you do have to watch out for yourself. But PC Magazine, the Wire Cutter, these are some pretty good reliable sites. And you can see here, I just did a Google search for password recommenders. And I'm looking at-- I'm not sure about top 10 cybersecurity.com. I'd probably look at that a little bit more.

But you can see a lot of these are from password manager programs themselves. But as I go down a little bit further, CNet's pretty reliable. PC Magazines pretty reliable. Tom's Guid, probably.

And I want to look at these. And Consumer Reports very definitely reliable. So you're looking for things that are up to date and have that imprimatur of reliability.

But you still have to be wary. The thing about a password management program is that it hinges on the password of the password management program itself. If you forget that, you are-- you're done. You cannot forget that. So you have to remember it.

But occasionally, a password management programs had leak. There was a leak with IPassword a couple of years ago. And this is basically a security flaw that was found. It's been fixed since then.

But even the people who found the security flaws, said, first do not throw away your service. Don't leave your password management running in the background. Make sure you close it when you leave, et cetera. You want to really think about your password and use good strong hygiene, et cetera.

There's different ways you can use it. Most of them use a copy-and-paste thing. You basically-- you copy it, and then you paste it in. Try to make sure that it's-- once you've copied it onto your clipboard in your phone or your tablet, that it stays on there the minimum amount of time before you actually paste it in because that small little bit of time is potential vulnerability if you're not taking care of other sorts of things.

But in general, I've talked to an IT guy at the other libraries, and he was like, don't worry about it. As soon as you copy it, it's gone. It's good.

Some times you have autofill. You can make special changes to the settings of your tablet or your phone so that it will automatically fill it. And you have to opt into that. That's something that I've chosen not to do.

Sometimes they have their own browsers. But they're moving away from that because it was just too much of a pain. I don't want to go through DashLane's browser. I want to use the browser that I'm comfortable with. So they're really moving away that.

Then you also want to think about how much information do you want to put in them. Do you want to put your payment information? I put my credit card in mind. But I didn't put in my PayPal password, except for I hid it someplace in there, in that line letter tactics. So I know where it is, but nobody else is going to know.

Something to think about. Some of these have some really nice services. For example, DashLane has something that others do as well. So that if you die, the information for the password management program will be actually passed on to someone else. And we'll talk about that a little bit later.

Storing-- most of them actually store in the cloud. There are some that store on your hard drive. But you're very limited in that way because you can only use it on that device. So you really want to think about that.

OK, so we've talked a little bit about hardening. And as you can see, hardening is really trying to make your computer a little bit more secure by thinking about these hygiene issues. But now we're going to move forward a level. And we're going to talk about hiding.

And the first thing that we're going to do is to go to a really cool site called Panopticlick. And this is from the Electronic Frontier Foundation. We'll be hearing about them again.

Let's go take a look at this. Because what this is a site that will actually look at your digital or browser fingerprint. And this is essentially all the trackers that follow you and that know who you are.

And I've not used this on this computer. This is a brand new computer. I just bought it in January.

So I'd be really interested to see what this says. So I'm going to go ahead and say test me. Because what it's going to do is it's going to see if I am unique. Am I unique?

And if I'm unique, that means that trackers have information that they can use. So that they know-- they may not know my name is Lorena. But they can pretty much say that it's a person

who lives at 517, North West whatever in Pullman, Washington. And you can see if we look at it, we're going to talk about privacy badger a little bit later.

But I have some protection against web trapping. That's because I'm using Firefox, which is a really good security browser. If I were doing this in Chrome, it would look a lot different.

So I'm getting some blocking of tracking ads because of my browser, some invisible trackers. This one's not working. I'm not getting acceptable ads.

I'm not getting-- I'm not third parties. Nope, and it turns out that my browser does have a unique fingerprint. And that means that I can be tracked. Everything I do in this browser can be tracked to me, the person who sits behind the screen.

So let's go back a little bit. And you can see, there's another one over here-- am I unique-- which does something very similar. But the thing is that these trackers-- these are mainly in cookies.

These are the little bits of software that you save because they make life more convenient for you. Or they're just trackers that just are always watching what you're doing. They're not necessarily linked to cookies. They might be just within the web page that you're looking at.

But all these little trackers are really getting a sense of who you are. And the thing is that your browsing information is valuable. People want to know what you're doing.

They want to use it to build profiles and to advertise to you when you're doing Google searches. It's information that really goes against me as a private person. And there have been any number of stories about that.

But let's go on a little bit. So browser fingerprinting or digital fingerprinting-- it goes by a number of different terminals. This is basically happening because my computer isn't encrypted. That means that there's a lot of information that's leaking out of my computer through these trap-- through these browser trackers that people can find.

And there's a little video here we're not going to watch. But the thing is that's really important is that multiple parts of the website can be encrypted or unencrypted. Most websites now are encrypted because they're required to use the HTTPS designation that basically protects you in some way from some trackers, not all of them.

But not every part of a website is always encrypted. So that means that information is leaking out that can be captured by these data aggregators and then sold because it's valuable information. No matter what you do. You cannot erase your digital fingerprint.

What you can do, though, is you can lessen it by doing certain things. So let's talk about those. First thing you want to do-- and this is a tool I use myself. It doesn't do anything to your memory. Your computer's going to work just as fast as it would before.

This is something from the Electronic Frontier Foundation called HTTPS Everywhere. And it works with multiple browsers. I think beyond these three.

But what it does is it forces an HTTPS connection, even if the website is HTTP. For example, not that I go there very often. But if we were to go over to-- let's just go over-- whoops, not there. Let's go to my link here, which tells me a little bit about HTTPS everywhere, what I can do with it.

But what I really want to do is I want to open up Drudge Report. I swear it's not something I go to all the time. But let's take a look at this.

Because as we look at the Drudge Report, let's see. Let's take a look. It's been fixed. OK, great.

I was looking at it before. And it had not been fixed. But yes, OK, so this is telling me they're using HTTPS connection. I'm securely connected to this site.

That means that my information should be pretty good. And if I wanted to, I can clear cookies and site data right now, which I probably should do. It's a good habit to get into.

So I'm going to remove all my cookies so that that next time I come here, there's a little bit less likely that they'll know exactly who I am. But they can continue to build up that knowledge on who I am. OK, so let's go back.

Just because you use HTTPS, though, doesn't mean that everything is secure. And let's go ahead and take a look at that in Neill Public Library here in Pullman-- a site that I'm very fond of because I'm really big on library sites. But let's take a look at this.

Aha, and it's good to look over here in the corner. You'll notice that I have a little icon here. So I'm going to take a look at it.

It's telling me this connection is not secure. It's using HTTPS. But it links out to other things.

There might be images. There might be a little third party programs. There might be all sorts of things here that actually are not encrypted, and so potentially could be leaking data about my usage or about what I'm doing on them, et cetera. So even when something has the HTTPS, you still have to be careful.

Now, and I will talk a little bit about how we can be careful, how we can deal with this a little bit later because there is a tool for that as well. Remember what I said, the black hats are out there. And they're always changing. And the white hats are running right behind them, trying to

come up with tools and ways to actually solve the problems that happen, or at least minimize them.

So let's think about website tracking. And when we think about our Panopticon results, I don't remember what this link goes to. Let's find out. Oh yeah, this is actually a study that was done by Princeton.

There are a lot of trackers out there. And this is a whole big study that they did about them. And you can see that it's a really big issue. We're not going to read it in detail.

So in response to the issue of tracking cookies and tracking snippets and bits of code, a do-not-track movement was started. And that was something where browsers would actually place within them a way for people to actually go through and change their settings. And you can see this gives you some information about how to do that so that you would not be tracked in these particular browsers, in Chrome and Firefox.

You can see here this is March of last year. And it'll tell you, which you can see I'm being tracked. I bought some hand sanitizer. And I've looked at this link on Facebook because I turned off my little Facebook tool right up there that I'll mention a little bit later.

And this actually goes through on how you can enable do not track. And do not track was a great idea. Because trackers actually-- most of the time it's just adware. So they can serve up that hand sanitizer ad that we saw.

But occasionally, it's not just innocent adware. It's spyware. It's malware, trojans, viruses, worms, things that are installing little bits of code on your computer to actually steal information, take over parts of your computer, et cetera. And so do-not-track was this great idea. But it turns out that it really failed.

It was just-- a lot of people didn't follow it. It just didn't work. And you see we have this nice little article about how it did not work from the Electronic Frontier Foundation.

I told you we'd hear that term again. And it goes into it in more detail. But essentially, it's a matter of money. Really, when it comes to it, the thing about tracking is that tracking serves ads. That's the adware part of it. And when it's serving ads, that means that I might look at it and decied to buy hand sanitizer or whatever. So it really didn't work.

I mean, it's still there. You can still change do-not-track options if you're going to your browser. And it's a good thing to do. But unless you're using a specific privacy type browser, which we'll talk about a little bit later, it'll help a little bit. But it's not going to do an awful lot.

There was even a movement for acceptable advertising. And this was-- OK, we're going to talk a little bit about tools that actually get rid of trackers. And there was this idea of acceptable ads

that we can't get rid of all trackers. Because if we get rid of all trackers, people won't be able to make any money. And that's what keeps the internet running.

So let's go ahead and choose these acceptable ads that ad blockers will not block so that we can-- I've got way too many things here. Let's go ahead and get rid of them all. I actually didn't get rid of them. They're all sitting someplace where I can get to them when I need to because I probably will.

So let's go take a look at a tool that the Electronic Frontier Foundation built when they realized the do-not-track wasn't going to work. And that's a really cool tool called Privacy Badger. And this is a browser add-on that stops advertisers and automatically blocks, et cetera. It's a great tool.

We're going to go ahead and take a look at it. So I actually have already installed it. But you can see here it is. And this tells you how it works.

It's one of those things where you can use it in two different ways. You can use it in a way where you're just like, OK, I'm just going to use it. And I trust it. And it's going to work.

Or you can learn about all the details sorts of things about what it does and how you can change it. So like I said, I'm kind of lazy. So I just go, oh, it's working. And if it breaks the site, I can fiddle around with it. So I've already installed it.

So I'm going to go over. And I'm going to move my little chat window here over and take a look at my add-on. You can see all my add-ons. I've lost all my privacy here.

And I'm going to-- you can see I'm going to turn on HTTPS everywhere there. And I'm going to turn on Privacy Badger because I disabled them. So now, let's go back over to the new public library.

Let's see. In fact, let's-- you can see there is my little tracker here. And you can see, there are no trackers on the Electronic Frontier Foundation's page. That's amazing. Oh, let's go look at the Drudge Report.

OK, politics aside. Whoops, I don't think that's the one I wanted. Oh well, let's go ahead.

And you can see that there are nine trackers on there. And I can look at them. Now what it's going to do over time is it's going to learn by what I do. And I can actually-- I can let it change its settings.

But I can manually-- I can change it over here if I want. But I'm like, OK, look at this. If this puts this in the red column, it means it is blocking trackers from being. It is blocking trackers from DoubleClick.net.

It's dropping-- blocking these, blocking these. This one is like, eh, it's OK. But it's blocking these.

All those trackers that were there now are being blocked. And over time, Privacy Badger learns how I do things. And it does a better job. Sometimes it'll break a site. And then I have to go no, no, it's OK. I have to move it from the red to the yellow or from the yellow to the green.

But most of the time, it doesn't. And it basically really does a good job of dealing with all of the evil trackers that are there. However, you have to watch out.

It says-- oops, let's go back over there. It has limited functionality and private incognito browsing windows unless you opt in your settings. And that's when you download if it says, do you want this to have functionality and private windows? And I say, yes, because I do. And then it will work in those as well. Let's talk a little bit about incognito windows a little bit later, too.

OK, so let's talk a little bit about-- oh, goodness, I only have 20 minutes. These are some other tools you can use. And I have the links for this on the web page that we're going to look at.

uBlock Origin is the one that I use actually. But there are others. Adblock Plus is used, Ghostery is used. There's a lot of things about it.

One of the things is that I don't always use uBlock Origin actually, which is even more strenuous than my little Privacy Badger because I'm actually OK about having a few trackers. You're always kind of balancing things. I want the web to remain free.

I'm pretty careful about what I do. So I'm like, in my case, I'm actually not going to use this. But if I were someone in a different situation, I would be like UBlock Origin all the way. And I would use it all the time. So you really want to think about the kind of surfing that you do, the kind of things that you do, how much you evaluate it, et cetera.

OK, so the last thing we're going to do is talk about homing. So we're going to do another test. This is what is my IP address test, except we're not really going to do it because I don't want you to see my IP address.

So I actually-- this is me when I turned on a VPN. And when you click on it, it'll tell you. Look at this. This is her IP address.

Your IP address is one of the major engines for tracking because your IP address, in general, is static. It's connected to this particular computer. It doesn't change. So it's a huge thing there.

So and because they know my address, they also know where-- oh, suspected network sharing device. Yeah, I took this picture when I was using a VPN, which we'll talk about soon. But it says you're in San Francisco.

So it's really good to take a look at this. And you can see it's got some really cool tools over here that I recommend as well. Because this is where we get in to network security in a different way.

This is where we get into the fact that if you're on an open Wi-Fi network, and you're not really thinking about things, someone can sniff your Wi-Fi. And they can take out things that are not protected by HTTPS that might actually not be not be that way. And they're just being transmitted in the clear over in your coffee shop or in your hotel.

This is a site for-- this is from the Federal Trade Commission. They talk about Wi-Fi sniffers and what a deal it is. And you see they recommend using your own mobile hotspot or a VPN, which we'll talk about now. Let's go back and find this.

OK, so what is a VPN? We're just going to go look at it on Wikipedia. But essentially, a VPN is a network that essentially creates a tunnel from where you are to where you're going.

And what that tunnel does is everything is encrypted going through. So no one can capture your passwords. No one can tell where you are. No one can tell what you are doing.

And so there's three reasons why you want to use something like this. The first reason is because of eavesdropping and interception. Somebody's listening to you, stealing your passwords, et cetera. The second thing is because of geographic tracking.

Because, again, my geography tells me that they can serve me up ads related to Pullman. That's where beacons come into play where they see me walk by. And they're like, oh, let's start throwing information at you.

But also there's issues of surveillance, surveillance by corporations, surveillance by the government, surveillance by your own ISP. And with the changes in net neutrality in the last couple of years, all your activity, your ISP, your internet service provider, can capture that and sell it. It's information that's available now. It's very powerful information.

So I'm not so worried now about people stealing my Wi-Fi password. But I am worried very much about my stuff being surveilled. So that's why I use a VPN.

So choosing the right VPN is really important because some VPN's actually are not so good. It turns out that there's a lot of free VPN's out there. And if you capture-- if you use a free VPN, you'll think oh yeah, I'm being so safe. But you're not being safe because as we can see in this article, it's a little bit old, but nothing much has changed with this.

When I went to update things, it was like eh. It actually turns out that over 38% of the free VPNs contain some malware presence and adware, riskware, spyware, et cetera. You can get a sense of these.

And that's just a really big deal. Because if you're trusting something with your-- it's just like your password management program. You're trusting your password management program to keep track of all of your passwords.

And here, I'm trusting my virtual private network to keep track of what I'm doing. And if it doesn't work, then I'm really in trouble. So the Electronic Frontier Foundation has a nice guide on choosing the right VPN that's for you.

But again, just like with the password management program, I might talk to someone who I trust. Or I might go and I might look for a VPN reviews. And I'm going to be looking for reviews from sites that actually are sites that I've heard of before, sites that I know are reliable. I might look at Gizmodo, which is a really good tech blog.

I might certainly look at PC magazine. I might look at the Wire Cutter, which is that-- you can see these are the ones that they do. Here's mine, Tunnel Bear. It has its issues, but so do they all.

Here's the Wire Cutter talking about their best VPN service. And you can see they're actually recommending Tunnel Bear. Although, it has its issues. They all do. But-- and I pay for it.

You can get-- Tunnel Bear you can get for free for a while. But if you want to have it on multiple devices, and if you want to actually not run out of bandwidth, then you need to actually pay. So whoops, I'm going-- let's talk about some VPN issues because it's not as simple as saying I'm going to protect myself.

I'm going to use Privacy Badger. I'm going to use HTTP everywhere. I'm going to use a VPN that I've purchased. It's not that easy. Because it turns out, things are more complicated.

First of all, you always have to remember that if you're using a work VPN, as many of us are, anything that you're doing using that work VPN, your work can see because that's reasonable. They're paying for it. You're supposed to be doing things on work time.

So all that information is findable because it's your work VPN. So you go buy your own VPN like I did so I can have my work VPN and my personal VPN. Well, first of all, sometimes things get a little bit mixed. Can't really do about that.

But it turns out that it's really more complicated in so many different ways because VPN sometimes are required to actually show information. So sometimes they don't have information to show, which is why you really want to take a look at your VPNs. Because if they don't keep logs, they can't be required to show logs.

But this is actually a really good analysis of something called five eyes, nine eyes, and 14 eyes, which actually you don't need to worry about too much. But essentially, what they all mean-- but essentially what it means is there's a number of countries who are involved in essentially

surveillance pacts where they share information. And these countries have the ability, have the legal ability to actually go to a VPN and say give us this information.

So most VPNs, good VPNs, will not keep any information. So they cannot be required to give it if they are served up with a warrant by the US government or the Canadian government or something else like that. So these are things you have to think about.

And that's what comes in here under key disclosure law. And you can see a little bit about this. These are some recommended ones here.

This site actually-- and this is something you can take-- these people are pretty good about recommendations. These are probably legitimate recommendations. But if we go down a little bit further, eventually they'll be talking about some of the issues around this key disclosure law, which is a law that says that they have to disclose information if it's available.

Now when I buy my corporate or my commercial blogs, I really do have to worry. I really need to do my research because again, if I get one of the free ones, they might be selling my data. This is something that's pretty egregious. This just makes me hot to think about.

Facebook paid money to teens to install a virtual private network VPN that actually spied on them. And that just makes me so angry that they do that. So VPN is really important. But you want to be really careful.

Get a reputable one, do your research, and again, have a good password for it. Because really what it all comes down to in the end, all these tools really come down to passwords. Password hygiene, being careful.

OK, finally, I want to talk about browsers. These days, actually, Google-- Google's businesses is ads. And they give us this wonderful Google search engine. And it's great. And it turns out that it's actually getting a lot of data from us along the way.

So there's options. DuckDuckGo is pretty much one of the main privacy browsers. And you can see they block trackers. They have secure connections.

They search privately all for free. And it goes through. So this is something that you might want to take a look at. And the blog goes through it a little bit more.

You can see their blog is even more privacy. They're very privacy conscious. I actually don't use Chrome anymore unless I have to.

I use Microsoft Edge, which is built on the Chromium platform and doesn't have Google's ad consideration. But I really like Firefox. And you can see that this is why when look at my trackers, I was actually OK because my browser is blocking stuff without me having to do anything. It's basically providing me a lot of protection.

And there's a lot of other things that they do as well. There are others. I can take a look at some others.

There's the Brave browser, et cetera. But these, once you start moving into some of these other ones, you're moving in to something that's a little bit more-- remember I'm lazy. I'm trying to find things that are low overhead that give me a decent amount of security without me having to change my behavior too much.

So this is good reminders about privacy risks. And they're going through a number of other browsers. You want to think about which one you choose very carefully. Finally, though, a lot of people say I don't need to actually worry about my browser because I use incognito or private browsing. So nobody's catching anything.

All incognito or private browsing mode means is that your kids can't go look at your history and see what links you were at, which is really great for peace in the home. But that still means that your ISP knows exactly what you're doing, that all those trackers that are all these websites are able to capture your data, and that you actually-- when we look at Panopticlick, you are identifiable.

You are unique in this world. But on one hand, it's great. We all like to think we're unique. But I don't like thinking that I'm unique in terms of the pattern of my searching, the filter bubble, the thing that all these little bits, where I live, how I search, what browser I use, what computers, what programs are on my computer, all of those going into that.

So when you're threat level is really high, and when you go beyond my ethos of harm reduction, remember, I'm not trying to get rid of everything. I'm just trying to reduce harm. Then you need to be more serious about it.

There are resources out there for you. There's the TOR browser. Whoops, let's go back up here. TOR browser is what they call an onion browser.

I didn't actually make that a link. OK, we'll look at the Epic browser. You can see over here.

It is a private secure web browser that blocks ads, et cetera. I can go look at the TOR browser. The TOR browser actually is heavily used for a non-anonymity. But the problem with the TOR browser is that sometimes, if you only use it to hide things, if you're the only person in an area that's using it, then it's kind of like well, this is one of those things where there's a network effect.

The more people who use it, the more protection it actually gives people. But this is serious heavy duty and not something that I'm worried about at this point. That might be something you want to think about.

I, of course, get my email from Gmail. So all my considerations of security actually literally get thrown out the window because of that. If I wanted to, maybe one day I will, I should move to ProtonMail, which is an encrypted email that will not actually sell my data or make it available for advertisers, et cetera.

This is a nice little document from the Electronic Frontier Foundation. They do one every year, a year in review. And you can see they're going over some of the legal issues that happened. And they're going through various links that they had.

I did want to mention very briefly that the European law that I can't remember the name of, GDPR, or something like that, that actually is something that has a very likely chance of decreasing our filter bubble because of people having to accept cookies. Except most of the time, we just accept the cookies. We don't say minimal cookies or anything else. So I'm not really sure. We'll know a little bit more in a few years after it's been in practice for a while.

Finally, what I wanted to do is give you some resources for further information. I've talked a lot about the Electronic Frontier Foundation. They are an excellent source. And they really will give you a lot of useful information in explaining everything that I've talked about far in more detail than I have.

Privacy tools is really good. They'll also give you suggestions for VPNs, Consumer Report Guide for digital security and privacy. This is an excellent one, privacy house clearing house. So there's some resources here that are available. And I want to go to the web page that I created for this class.

Let's see. And you can see this is really excellent. They go through a lot of things. So I'm going to just go web guides. Let's see, it's hidden down within my subject guides.

I hope I remember what I called it. Yay, I did. So this actually is-- I'm going to put the link in the chat box once I actually go back and look at the chat box. I'm going to copy it now.

But this actually-- when the link comes out from Global Connections with the video, I'll put the link here. And you can see I've put in a lot of links that I did. I actually put in some better links here.

This is the more recent Pew Research Center study on Americans and Privacy, which has some really good information. I actually have to put my librarian hat on for a second. Pew is just the best source.

They do survey research very, very, very, very high quality. You can see politics, media, social trends, religion, internet science, global surveys. It's just the best resource. I really recommend you take a look at it. Always have to have that librarian thing there.

OK, so I am done now. And I'm going to try to go find the chat. And the first thing I'm going to do is paste in the link to the site that I gave you.

All right, everything that I share, like I said, when I teach technology classes, I teach things that I use. And I do. I teach a number of technology classes.

And these tools I use. Sometimes I don't use them. I told you that I don't use uBlock Origin. I chose not to.

But if I'm ever going to go do some research that I might need to do where I felt I might be moving out of the things that I usually look at into something that might be a little bit more slippery, then I would very definitely turn uBlock Origin on. These are-- and I turned off all my tools. I turned off everything for this presentation.

I'm not using my VPN. I'm not doing anything. But in general, when I'm off work, I try to have my VPN on all the time.

Partially, when they say, oh, you don't have anything to hide, I don't. I'm like a total Girl Scout. But the thing is that the more I hide my stuff, the more I protect other people who are hiding stuff, that might matter to them even more. And so I'm doing this part-- I hate to say this because Herd immunity. The more of us use these privacy protection tools, the better it is for everyone.

So they don't slow you down very much. They don't cost anything in most cases, except for the VPN and the password management program, which are worth the money. Let me tell you. And they can really help you out a lot.

ANDREA JIMENEZ: All right, well, I just pasted the link once again that Lorena shared. So I'd like to thank you all for coming and thank you, Lorena, for presenting for us. And have a good evening, everyone.

LORENA O'ENGLISH: You, too.