

Online privacy and security for basic users – teacher's guide

Before you begin:

This guide assumes that you (the teacher) are familiar with using the tools covered and what they do. If you aren't, download them all and spend a few weeks using them, and review the suggested reading within this guide. You should also review the list of privacy links (it's in the first slide) because every tool I talk about is linked there. You can contact me with questions or to set up an in-depth privacy toolkit training: alison@libraryfreedomproject.org.

This class is ideal for a user who interacts with her computer at least a few times a week, can access basic internet services like email and searching with relative ease, but needs considerable assistance with downloading and using new software. This user understands basic internet terminology like “web browser” and “virus” , but is likely unfamiliar or less familiar with things like “extensions” , “cookies” , and “malware” . When registering patrons for this class, it's helpful to ask a few questions about their computing skills to see if they're ready for a class at this level. I usually go with some questions like the following:

- What is a web browser?
- What is your preferred search engine?
- Could you find the “downloads” folder on your computer with ease?
- Could you find the “settings” or “system preferences” on your computer with ease?
- Why are you interested in taking this class?

Any questions that get the patron talking about her level of comfort and familiarity with her computer will help you understand pretty quickly whether or not she can keep up with this class. If she hesitates for a long time, or just doesn't know the answers to these questions, you might recommend an “introduction to PC” or “introduction to the Internet” course before she's ready for this one.

Bear in mind that even if you try to control for the level of user ability, there will still be people who take the class who aren't quite ready for it. That's okay! In my experience, these patrons will still benefit from what you're teaching. When you introduce yourself at the start of the class, let everyone know that the pace of the class will be dictated by the ability of the majority of students. Those few participants who find themselves slipping behind might find that they prefer to listen and take notes rather than complete the downloads in real time. If you have the staff for it, I recommend having a second teacher to help those students who get stuck. I've offered this one-on-one attention for classes with the help of a second staff member, and the students REALLY appreciate it.

- Be gentle and patient!
- Speak slowly!
- Have a sense of humor and enjoy yourself! Most of what you'll be covering is brand new to these students and the topic is more than a bit frightening.
- One last thing before you begin: print enough copies of your slides (and any supporting handouts) for all students.

- I can't get through this class in under two hours, and that's if I only cover the difficult stuff (VPNs, PGP) very briefly. If you want your patrons to get the most out of each tool, schedule this for a half day workshop (with breaks!). You may also want to modify the structure and only teach some of the tools I've recommended.

Starting the class:

Before the class begins, make sure everyone is connected to the wifi network. If there is a password, write it somewhere where everyone can see.

Introduce yourself and the title of the class, then ask folks to share their reasons for attending. What are their privacy concerns? This is important, because it will vary widely in each class. Some of my students have been concerned with Google keeping such vivid profiles of their online behavior. Others are frightened by the capabilities of the NSA and FBI. Still others are afraid of the ability and ubiquity of criminal hackers. Let people share their concerns as much as they are willing. This is scary stuff, and it's likely that most of the people taking this class have never been in any setting where they can talk openly with other people about their digital security fears.

A note about the format of the class: I use the slides as a kind of outline, then toggle between the slide presentation and the actual tool to demonstrate it in real time. If you have the time for it, I highly recommend allowing time for students to download each tool as you tell them about it. They will need guidance through the prompts (eg "Now click 'install'. Now restart your browser." etc). The ideal setup is the teacher using a virtual machine (or at least one with none of these tools already downloaded) so that students can see all the download prompts on the presentation display.

On to the presentation!

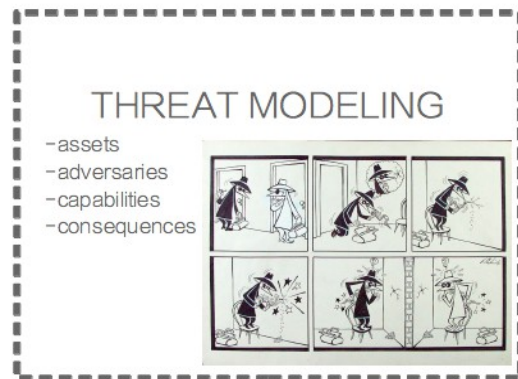
Remember to add your own contact info and library website! Feel free to keep the LFP site in there as a resource, but if you do, please give a little explainer about LFP!



Also, feel free to also use the LFP link to all the tools! If you're not demonstrating the downloads in real time, instruct your students to follow **only** the links listed there when they download the tools on their own time. Later, when you talk about malware, you'll talk about malicious links and fake software downloads.

Instruct the students that you'll be following this list of links as you go.

- Make sure they've all got the list open in their browser before you get started.
- Note: since many of these students will be using Chrome or Internet Explorer when they begin, you will need to instruct them to copy and paste the link to all the links into Firefox after they download it.
- Read EFF's Surveillance Self-Defense introduction to threat modeling before you begin:
<https://ssd.eff.org/en/module/introduction-threat-modeling>



Summarizing SSD, you can determine your threat model by asking yourself these questions:

- What do you want to protect? (assets)
- Who do you want to protect it from? (adversaries)
- How likely is it that you will need to protect it? (capabilities)
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to prevent those?

Explain this to your class and ask them to consider these questions as they are going forward in the training. If you have time, this is a great time to engage the class in discussion.

- Talk about the tradeoffs between privacy and convenience. For example, KeePassX is not at all as convenient as storing all your passwords in your browser, but the latter is very bad for privacy. You might want to make it clear that not all of the tools you're about to teach are disruptive or inconvenient! Some are quite simple and won't change the user experience at all.



- Briefly explain the definition of free software (you should mention that “open source” and “FOSS” are terms that are often used interchangeably. I don't recommend getting pedantic about “free” vs “open source”).
- Name some proprietary software providers and explain the difference between them and FOSS.

The key points I usually go over about privacy and FOSS are: transparency of code means it's much harder for something malicious to get hidden, proprietary software

companies like Google and Facebook participated in PRISM (<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>) and those same companies are collecting tons of user information for their own ends, and how decentralization in general is good for privacy because then you're not giving one application or company an all-access pass to your data.

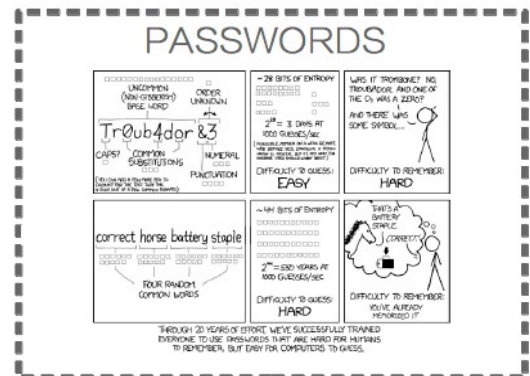
- This is also a great time to talk about the trust relationship with software.
- You should also note that most FOSS tools are also free-as-in-gratis, but that the services rely on donations to exist.
- Most of the tools we're about to cover are FOSS, noted if otherwise.



date software.

Talk briefly about the importance of software updates for privacy, making sure to cover operating system and application updates. You might want to show an example update that outlines security patches. Explain how easy it is for an attacker to see that you're using an out of date version of software and how this can easily lead to compromise. Most attacks on privacy are the result of poor endpoint security like out-of-

Hey! This is a funny comic and also a pretty good password strategy. Let your students read it and absorb the message, then move on to the next slide to discuss the actual strategy.



Your passwords are bad.
So are everyone else's.

- high entropy
COMPLEXITY! LENGTH!
NO PATTERNS!
- password managers
KeepPassX
KeepPass
LastPass
- diceware list and die

Yes, everyone's password is bad! It's okay, we've earned terrible password strategies. This is a good thing to talk about - our passwords are too short, they use patterns and personally identifiable information, and we use the same ones over and over for everything. Fortunately, strong passwords are not that difficult!

- So, first, NO PATTERNS. No lines from your favorite song or book. Not your dad's middle name plus his birthday. Adding some complexity, like capitalizing some letters and adding a few numbers, won't help much if there is already a pattern. You need randomization or pseudorandomization to get real password strength.
- Fortunately, both KeePassX and KeePass(2) have password generators. I advise students to reset their passwords one by one in one of these password managers, and use the xkcd method (modified to 5–8 word passphrases) with the diceware list and die to create a strong master password. This piece by Micah Lee explains everything you need to know about using the diceware word list and die:
<https://firstlook.org/theintercept/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>.
- I mention LastPass in here because I think KeePassX can be difficult for ordinary users. LastPass is a cloud-based browser extension for password management. Make sure you warn your students about the dangers of storing sensitive data in the cloud. Also, mention that LastPass is non-free software.
- KeePass is sort of medium level difficulty. You might want to stick with KeePassX and LastPass as your two options just to keep things simple.
- For an additional measure of security, you can recommend using something like a Yubikey, which is a commercial encryption device that can store up to two strong passwords when in static mode. You insert it in your USB drive and it acts as a keyboard, so pressing the button on the device will enter your password (short press for the first, long press for the second). That means you also avoid the risk of password keylogging. I have included links to Yubikey and the static password mode instructions in the list of links. I wrote a little more about this password strategy for ALA's Choose Privacy Week: <https://chooseprivacyweek.org/choose-privacy-week-2015-strong-passphrases-for-privacy-and-security/>
- Make sure to tell your students to back up all of their master passwords, whether they use the xkcd method or a Yubikey (especially for the latter!). Writing it on a piece of paper and storing it in a safe is a fine method.

Tools in this slide: KeePassX or KeePass(2), LastPass, KeePass, diceware list and die, Yubikey, Yubikey static password mode instructions

Yes, this section is about exactly what it sounds like!



- who owns your browser?
- what is a browser extension?
- Firefox and Tor
- Firefox privacy settings
- Firefox extensions menu

This is a great place to circle back to FOSS and proprietary software.

- Ask the first question in the slide and get the class to identify whether or not their browser is FOSS or proprietary. An easy way to define an extension is “a browser component that adds a specific feature” .
- Firefox is obviously the recommendation here (owned by nonprofit Mozilla and also FOSS), but

take a moment to talk about why Firefox and Tor are different, because you'll be introducing Tor soon.

- You don't have to review the Firefox privacy settings completely, but at least point the class to the settings link. It's easy enough for a user to follow on their own, and will help them set up defaults for not saving information in forms, denying certain cookies, etc.
- You also should absolutely should point out where the Firefox extensions menu is (menu → add-ons) and show how to remove or disable them. You should also show how to start Firefox in safe mode with all add-ons disabled (menu → ? → restart with add-ons disabled).

Tools in this slide: Firefox, Firefox privacy settings, Firefox extensions menu

In my experience, most users are at least somewhat familiar with third-party tracking and behavioral advertising, and it's useful to engage them about their experiences with this. They've all seen sponsored ads based on things they've searched for or websites they've visited.

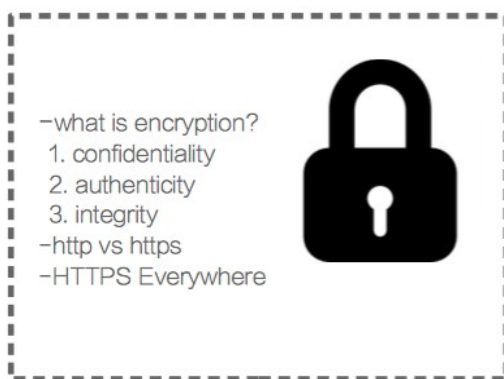
- Explain how some of those trackers function and what they do, how you interact with them, how they can follow you across websites – and give definitions of each (cookies, analytics, etc).
- Then after you introduce and download Privacy Badger, show how it works on a popular website (I usually use salon.com or nytimes.com). There are other extensions that work similarly to Privacy Badger, so here is an explainer of how it's different: https://www.eff.org/privacybadger#how_is_it_different. The other one I like is Disconnect.me.
- Ditto for uBlock Origin. I use them both together because they get at different blacklists, and also because uBlock Origin blocks ads from displaying. Make sure to clarify that uBlock Origin and uBlock are not the same.
- Then talk about search engines: all the major search engines collect and store



everything you type into them. Google, for example, stores searches for at least 18 months.

- There are a few search engines that don't do this, and the one I recommend to students is DuckDuckGo.
- The Don't Track Us (<http://donttrack.us/>) site, created by DDG, has some more helpful talking points about search tracking.
- DDG does support ads, but the ads only appear within the search results based on what you **just** searched for. They do not follow you to other sites or create a profile based on your preferences.

Tools in this slide: Privacy Badger, uBlock Origin, DuckDuckGo search engine



Time to talk encryption!

- Start with the basic definition of what it is, how it is different than plain text, and how it protects your data (confidentiality, authenticity, integrity). Here's a brief explainer on encryption in general:
- <http://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works>.
- Next, explain how encryption works as a layer on top of http(s). This article is a great explanation of it

and why it's necessary for privacy and security:

<https://firstlook.org/theintercept/2014/08/15/cat-video-hack/>. I've also written about it for library websites here: <http://litablog.org/2015/01/why-we-need-to-encrypt-the-whole-web-library-websites-too/>.

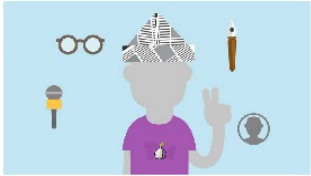
- After you talk about the importance of https generally, you can show the HTTPS Everywhere extension. This extension forces https to work by default on sites that have a TLS/SSL certificate installed, which means that even if you type <http://example.com> in your browser, you'll always get <https://example.com>. Not forcing https by default is a common problem on TLS/SSL-enabled websites. You don't really have to demonstrate how this extension works on a compatible website, since it's a bit more invisible than the other extensions. Here's an FAQ from the Electronic Frontier Foundation on HTTPS Everywhere: <https://www.eff.org/https-everywhere/faq>

Tools in this slide: HTTPS Everywhere



Yup!!!!

Tor is the most secure browser available.



-Tor vs. Firefox
-Tor extensions: HTTPS Everywhere and NoScript
-Tor best practices
-more with Tor (mobile, proxies)

Before teaching about Tor Browser, I strongly recommend reading the overview of Tor <https://www.torproject.org/about/overview.html.en> as well as the best practices on the Tor Browser downloads page: <https://www.torproject.org/download/download-easy.html.en>. If you really want to know everything about Tor, read this: <https://ritter.vg/p/tor-v1.3.pdf>. I try to sum up as much as possible about how the network works and what it protects you against, because there is so much to say about Tor Browser and it's all pretty

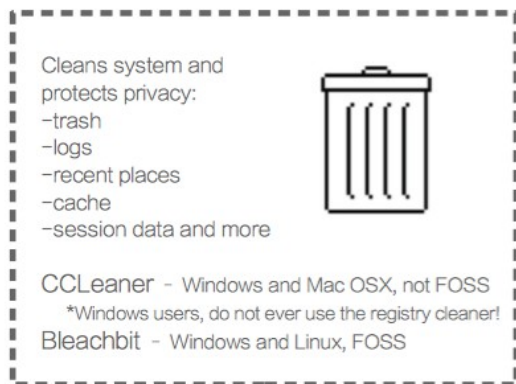
important for the user to know.

- At the very least, you should say that Tor Browser protects privacy by obscuring your location and browsing data, making it difficult for an attacker to learn your location or information about what you're doing online.
- Be sure to help your students understand how it's different from Firefox; if you want, you can explain that Tor Browser is built from an Extended Support Release of Firefox and that's why their interfaces are similar.
- Explain that it comes with HTTPS Everywhere (already illustrated in an earlier slide) and NoScript for further privacy. NoScript's website has some useful info on how it works <https://noscript.net/>, but in brief, you can explain what scripts are and how untrusted scripts can deanonymize you.
- Some of the Tor best practices that I make sure to cover: don't log in to identifying accounts, unless you create them using Tor, disconnect from the internet before opening downloaded files, and don't install more extensions.
- If you have time and your audience seems like they'll find it useful, you can get into "more with Tor" by explaining how you can use Tor as a SOCKS proxy for other applications: <https://www.torproject.org/docs/faq.html.en>. However, this is a bit more advanced than your class may be ready for.

Tools in this slide: Tor Browser, No Script

Onward!

LOCAL FILE MAINTENANCE



- These applications - CCleaner or BleachBit - will shred all kinds of unneeded files from your system so that they can't be discovered and compromised later.
- CCleaner is not FOSS, but BleachBit doesn't work with OSX.
- CCleaner settings also need to be changed to "secure deletion" (you'll see it in the settings menu).
- I usually recommend running these programs

about once a month. They're also just good system maintenance tools - users will probably find that things run a bit faster.

- CCleaner Windows users should absolutely never check the "registry cleaner" option. The registry is not a thing that ever needs cleaning!!!

Tools in this slide: CCleaner and BleachBit

okay!

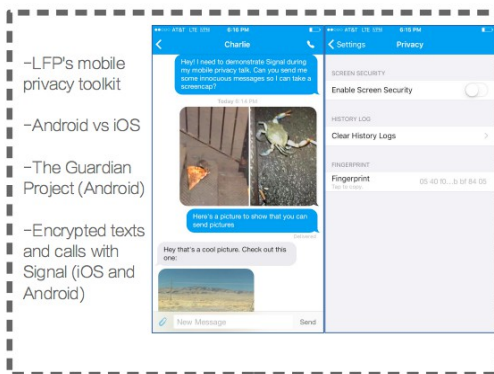
DISK ENCRYPTION



- Remind folks again what encryption is and what it does for privacy
- Explain how full disk encryption can protect data in case your laptop is stolen
- It's easy to set up each of the disk encryption tools that comes in the operating system - just show folks how to navigate to it and turn it on.
- For Veracrypt, you might want to demonstrate how to encrypt a volume or individual file.
- Make sure to mention that Veracrypt has not been fully audited (as of November 16, 2015 - check to see if this is still true when you use this guide!)

Mobile!

MOBILE DEVICES



Mobile stuff is really its own class, but it's worth a mention if only because folks will be thinking about it.

- A full mobile privacy toolkit is here: <https://libraryfreedomproject.org/mobileprivacytoolkit/>
- Usually I talk briefly about the inherent privacy and security problems with mobile devices: I like the “iOS is a walled garden and Android is an open sewer” analogy most. That is to say, iOS is secure if you trust

Apple with your data, but you can't get many privacy apps because they haven't been Apple-approved. Android, on the other hand, seems to have been designed to BE insecure.

- The Guardian Project's suite of apps offer a great range of tools to help harden Android phones, including Tor Browser for Android (Orbot).
- Signal (for iOS or Android, screenshots here) is an excellent app for encrypted texts and calls. It's also really easy to use. Talk about the settings, how to use the fingerprint, and how to delete all data on the spot.

Moving along!

VIRUSES AND MALWARE

DON'T GET SCAMMED! BE SAFE!

- phishing, script kiddies, malicious links, malicious attachments, and other scams
- differences between viruses and malware
- relationship to privacy
- good practices

antivirus: ClamAV
antimalware: MalwareBytes (Windows only, free vs pro)

Just like behavioral advertising earlier, most users are reasonably familiar with malware and viruses and how they compromise privacy, but a quick review is useful.

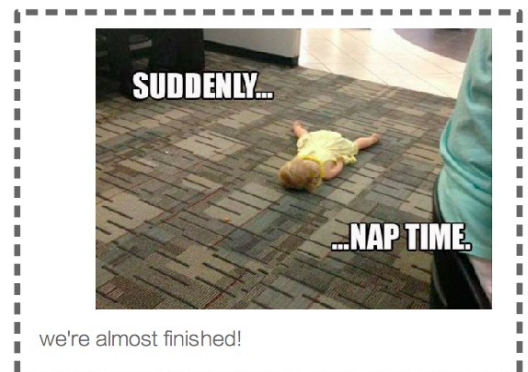
- Talk about common ways that users can inadvertently download malicious programs - untrusted download sources with malicious software bundles, email scams, advertising scams, and so on.
- I encourage patrons to make sure they're always on the https version of the correct site

for downloading software (eg <https://www.torproject.org>).

- Remind them of what encryption does to protect the integrity of their data, and relate this to the integrity of software downloads (nothing injected in the download, no MitM attacks).
- If students in your class already have an antivirus program, there is probably no reason to change it. They should make sure that it's functioning and up-to-date.
- If they don't have one, ClamAV is a FOSS antivirus program they can download.
- They should never have more than one antivirus program running on their computer at once.
- MalwareBytes (not FOSS) will handle malware blocking on Windows machines (I recommend the pro version, which will scan and prevent malware from being downloaded, rather than the free version, which will only clean up after an attack).
- OSX users have native malware protection (information on this is linked in the privacy links).

Tools in this slide: ClamAV, MalwareBytes, OSX native malware protection

Take a break here if you need to!





time for some difficult stuff!

Unless you're teaching an all-day class, you likely won't have time to fully demonstrate the last few tools. Try to at least get your students to understand what they are and possibly try them on their own, and if your library offers one-on-one tech help sessions, that would be a great way to help those students who need further assistance with these more difficult tools.

I know, you're probably thinking “this is far too complex to cover in a basic class” and that's probably true, however, you will get asked about email, I promise. So you should at least get into the basics.

EMAIL



who can read your email?

- your email service provider
- operators of intermediate network connections
- your intended recipient's email service provider
- anyone who accesses those servers

- You at least want to convey to your class that most email is not secure or private. Google, for example, inspects all Gmail content as a matter of course, again for behavioral advertising purposes.
- Get your students to think about email in terms of the provider storing your content on their servers, and also in terms of the security of those connections (another good time to talk about TLS/SSL and encryption in general).

- Explain to your students that the only way to achieve real email privacy is through true end-to-end encryption

PGP encryption

- email self-defense from FSF

email providers

- pobox.com
- alumni email
- a server you trust



with PGP.

- Explain briefly what this is and how it works – the key exchange, the encryption and decryption processes, and how both users have to be using PGP for it to work.
- The email self-defense guide from the FSF is the simplest tutorial for setting up PGP encryption, so you can point students to that and maybe briefly cover it, encouraging them to check it out on their own time (it's in the list of privacy links).
- You won't have time to cover PGP unless this class is an all-day workshop, and besides, I've had more success teaching this to people one-on-one. So encourage them to contact you to schedule an appointment.
- Switching to a trusted email service provider is a fairly simple step, so your students might want to start there.
- I've listed a few options here – alumni email is the free option, however, alumni email is not private by definition! Especially since many schools are switching to Google Apps. Tell your students that they can find out more about the privacy/security of their alumni email by contacting the IT department of their former school and asking about their server security, data retention, and how they deal with requests from law enforcement.

Tools in this slide: Email self-defense from FSF/PGP, safer email provider options

yeah!

VPN

- what is a VPN?
- what to look for in a VPN
- some options
 - Bitmask (Android and Linux)
 - Private Internet Access (iOS, OS X, Windows)

Some of your students may be familiar with VPNs that they've used at work.

- Explain in a broader sense how VPN tunneling encrypts your traffic (confidentiality, authenticity, integrity again) and how you can use a VPN for more private internet access.
- I have a couple of VPN options that are simple to use: Bitmask for Android and GNU/Linux, which is FOSS, and Private Internet Access for all

other OSes, which is not FOSS.

- There are many other commercial VPNs available that are simpler for basic users to set up, and that link in the list of privacy links asks commercial VPN providers **all** the right questions – how do they respond to law enforcement requests and DMCA notices, what their data retention policies are, and so forth.
- I would review those questions for the “what to look for when choosing a VPN” bulletpoint.

Tools in this slide: Bitmask, Private Internet Access, link to list of other commercial VPNs

Some extra tools for people who want to go even further:

- PRISM Break: a list of FOSS alternatives to all kinds of software. Includes a lot more mobile stuff.
- Surveillance Self-Defense: a set of playlists with recommended privacy tools for different threat models (eg LGBTQ youth, political activists, etc).
- Bruce Schneier's blog is a great resource for things happening in the privacy/security world, and it's easy to absorb even for nontechnical people.
- The Cryptoparty website includes upcoming events and resources. Folks might want to go further by attending one of those more in-depth sessions in their community.
- Lastly, you can always point your students to the resources on Library Freedom Project's site. We are adding more all the time.

EXTRA CREDIT

- PRISM Break
- Surveillance Self-Defense (EFF)
- Schneier's blog
- Cryptoparties
- LFP resources



alison@libraryfreedomproject.org

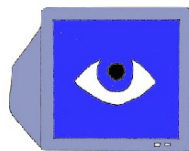
@flexlibris

@libraryfreedom

libraryfreedomproject.org



Attribution-ShareAlike 4.0 International
www.creativecommons.org



And that's it! Please feel free to modify and redistribute this as you wish, as long as you follow Creative Commons' CC-BY-SA guidelines: <https://creativecommons.org/tag/cc-by-sa>. For questions or feedback, please contact me at the address on this slide.