STAYING (AS)
SAFE
(AS YOU CAN)

Dorothea Salo

What we've done so far

- Identified (some of) the metadata out there about you that you want to protect ("information assets").
- Identified (some of) the entities who want that metadata and might use it against you ("information adversaries")
- Gauged adversaries' ability to get that metadata ("capabilities") and how bad it would be for you if they did ("risk").

What we're doing today

- Figuring out what you can—and are willing to—do to protect your metadata.

Some caveats, first

- We can't stop all surveillance efforts.
  - It's not like we're going to deep-sea-dive to prevent data from being lifted off overseas fiber!
  - Interdependence is the nature of the Internet; we don't have much choice but to trust some possibly-untrustworthy actors.
    - It's NOT YOUR FAULT security is hard and sometimes fails.
- We can't always stop one another from compromising our own privacy and security, sometimes in really amazingly thoughtless ways.
  - You have my blessing not to fix all the things!
- I don't think that's license to throw up our hands and do nothing. I hope you agree. We don't have to make it EASY!

Questions to ask about available strategies

- What/whom does this protect against?
- How much will this disrupt your experience?
  - The ideal: you don't even notice, but everybody is safer.
- How much care and feeding does this take?
  - Installation and upgrading
  - Support
  - For some strategies, bandwidth
- Can you turn this off if you need to?
  - The correct answer is ideally "yes, but you won't want to."

A word about adversaries

- For some people, the NSA or a data-broker like Acxiom seems like a really remote adversary.
  - This damages motivation to improve personal privacy and security.
- If it helps, imagine non-remote adversaries!
  - Me (I don't mind!), and other UW-Madison authority figures
  - Bosses
  - Family members, "friends," coworkers who are either generally nosy/gossipy, or who dislike you and would enjoy getting you in trouble
  - Ex-significant-others
- What protects you against these will usually also help protect you against the more remote risks.

EMAIL IS NEVER SECURE.

- Repeat after me, three times: EMAIL IS NEVER SECURE. EMAIL IS NEVER PRIVATE. EMAIL IS NEITHER SECURE NOR PRIVATE.
  - Not legally, not technologically
- Watch what you email. Avoid email altogether for private communication, gossip, anything that could come back to haunt you.
  - Workplace tip: Your boss can read your email. So can company IT. IT'S NOT EVEN HARD, okay?
- Google is data-mining your GMail. If you can get off GMail, do.
  - GMail is also a Big Fat Target for the likes of the NSA.
  - Other options: your webhost, Lavabit, ProtonMail

Stay away from the Internet of Things.

- It is HOPELESSLY insecure and unprivate.
- Avoid Siri, Alexa, Echo, Nest, "smart" lightbulbs and appliances, fitness trackers, toys, all of it.
  - Fitness trackers: Bosses and universities are already trying to use these to mess with your (and everybody's) health insurance. Don't share.
- One Thing you will have to deal with: your router/gateway
  - Change its default administrative password!!!!!!!!!
  - Turn off PING, Telnet, SSH, UPnP, HNAP, Wi-Fi Protected Setup; turn off "cloud management" and "remote administrative access" if you can.
  - Keep its firmware updated.

If you're at serious risk…

- (and it's quite likely someone in this class is!)
- What I'm about to show you is useful but insufficient. You need to go hardcore.
- Resources that can help you do that:
  - EFF, Surveillance Self-Defense: https://ssd.eff.org/
  - Zen and the art of making tech work for you: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
  - The Smart Girl's Guide to Privacy (book by Violet Blue; the iSchool library has it)

Start good habits now.

- You won't suddenly have to change your behavior in a stressful situation.
- You'll be less likely to end up in a stressful situation to begin with, and if you do, it's likely to be less severe.
- You'll be in better shape to help friends and family be more secure.
  - Not least because you can say "I use X and it's great!"

PASSIVE STRATEGIES

no special software required

Software minimization

- Works both on mobile and laptop/desktop.
- If you don't use an application, get rid of it.
- Nobody can hack you via software your machine doesn't even have. Plus, more disk space!

Patching and upgrades

- I know it's annoying. I know it's expensive. I know it's time-consuming, including the time to learn the new version.
- Do it anyway. Including for any browser plugins you install.
- Black hats love to hack older software.
- So do spooks.
- People who don't like you rely on techniques from black hats and spooks to get you in trouble.
- Red alert: if you're using any software that's gone past its last support date. This is hideously dangerous. Don't do it!

Operating systems

- You don't have to upgrade to the latest MAJOR version (e.g. Win8 to Win10, or Sierra to High Sierra) right away.
  - I skip major OS X versions myself... and I wait until .1 (which was especially wise for the amazingly bugridden High Sierra).
- You DO have to upgrade when the major version you're on STOPS GETTING SECURITY UPDATES.
- You DO have to upgrade to new MINOR versions ("service packs" on Windows, .1 to .2 on Mac) RIGHT AWAY.

Other software

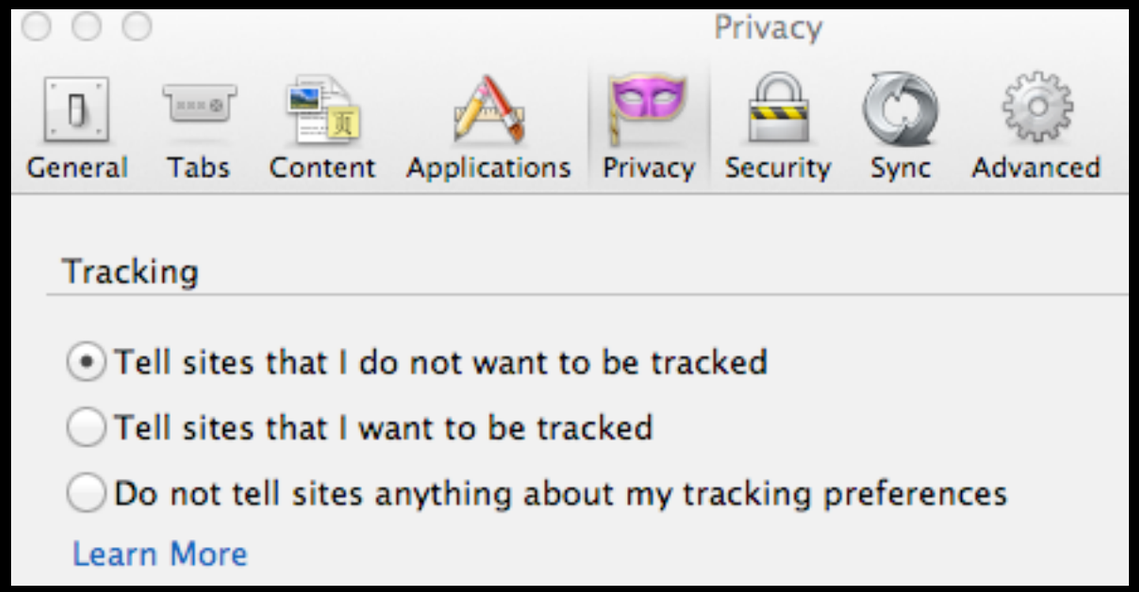
- Microsoft Office: treat like your operating system
- Anything else (especially your web browser!!!!!!!!): UPGRADE. JUST DO IT.
  - Firefox tip: If it should be updating and it's not, go to the About Firefox... screen. That should trigger the update.

Settings

- Go into your gadget's main settings/preferences.
- Turn off everything you can!
  - If you're worried something will break, turn things off one at a time, use the gadget for a few days, rinse, repeat.
- Turnoff candidates:
  - Bluetooth
  - WiFi
  - Location services
  - "Sharing" (e.g. file sharing, connection sharing)
  - Anything that turns your gadget into a hotspot or server
- Most of this stuff is checkboxes. If you need it, you can turn it back on, no big deal.
  - When I rent a car, I turn Bluetooth on just to play music. Done? Bluetooth goes back off.

“Do Not Track” browser setting

- It’s pretty much useless.
- Set it in your default/neutral browser configuration anyway.



Other browser settings

- Do not let the browser keep passwords.
  - Use a password manager instead (hold that thought).
- Turn off third-party cookies.
- Do not let your browser share location information (geotagging!) without telling you about it.
  - When it tells you, tell it "no" unless something will break. No, Home Depot, you do not need to know where I live!
- Consider not letting the browser keep history or cache pages.
  - Wiping at the end of a session is fine.

“Private” or “incognito” mode does not make you private!

- It only prevents **your browser** from storing information about your browsing.
- It **DOESN’T** prevent **websites you visit** from storing information about your browsing.
- It **DOESN’T** prevent **third-party trackers** on websites from storing information about your browsing.
- It **DOESN’T** prevent your **Internet Service Provider** (ISP) from storing information about your browsing.
- Long story short: it helps a little, but really not much. You need to do more to protect yourself.

Change default search engine

- Google tracks everything. Don't default to it!
  - Browser preferences let you change the default site searched with the browser search bar, or via the URL bar.
- Better option: DuckDuckGo
- Results no good? You can always pop over to Google for that one quick search.
  - I find that DDG has improved a lot!
- Bonus: you don't get filter-bubbled, overly-ad-influenced, or geographically-limited (all this is what search engines call "personalized") results.

If you MUST use Google…

- You can turn off a boatload of tracking.
- While logged in, go to myaccount.google.com.
  - Go through EVERY SINGLE LINK and do what will maximize your security and minimize Google tracking you. Usually that's pretty obvious.
  - Turn off ad personalization.

On mobile

- Leave WiFi off unless you're actively using it.
  - Yes, this means ditching push notifications. I'm guessing you won't miss them as much as you think you might.
  - The process of seeking a wifi connection leaks ridiculous amounts of information. If your mobile device's wifi is turned on, it is constantly seeking a connection!
    - Bonus: turning wifi off helps conserve battery.
- Turn geolocation of photos off.
  - This adds location metadata into your photos. Bad idea.
- Leave location services off unless you need them.
  - I only turn them on when I'm traveling...
- Prefer iOS to Android, if possible.
- Stay in "airplane mode" as much as you can.

Mobile apps

- Check their permissions—what other data on your device they have access to.
- Turn off everything you can.
- Android apps are absolutely notorious for over-harvesting data. Google doesn't police this.

Password manager: get one!

- Makes and stores strong passwords that you don't have to remember. You just have to remember your password manager's password!
- Some let you store your password cache (encrypted, of course) in the cloud to use it across devices (including mobile).
  - I don't, but... you might?
- Solid choices:
  - LastPass (Win, Mac, Linux, iOS, WinMobile, Android, BlackBerry)
  - 1Password (Win, Mac, iOS, Android)
  - KeePass Password Safe (open-source, cross-platform)

Passwords and secret questions

- Use your password manager as much as you can. If you're like me, though, a few passwords you'll want to create yourself.
- There's lots of guidance for this (some of it contradictory). Here's what I do:
  - Come up with a NONSENSE PHRASE, 3-5 words long. Not in English if possible.
  - Put a couple of special characters and a number in it.
  - Need a new unique memorable password? Add part of the website name to the phrase!
- Secret questions
  - Do not give correct answers, ESPECIALLY if the answer is researchable. (Mother's maiden name? High school? Street you grew up on? Come on. And yes, lots of people have had accounts hacked this way.)
  - Make another nonsense catchphrase. Use it every time. (Special characters less important here.)
- In password or secret-question hints, put a word you're adding to the catchphrase. Bonus points if it misleads an attacker!

Online accounts, including social media

- Turn two-factor authentication on, for any site that offers it.
- Turn geolocation OFF for social-media sites.
- Do not let websites save your credit-card info, if you can avoid that. Type it every time.
- Don't give sites your real birth date when you can avoid it.
- Avoid social-media add-in "apps" (like games, quizzes, and such). Most track you. Some are actual malware.
- Avoid social-media mobile apps. They overharvest personal data.
- Get off Facebook if you can.

Social media

- Check your default visibility/sharing settings. Be conscious of who can see what you post.
  - "Friend of a friend" (as on Facebook) is a LOT OF PEOPLE.
  - If you have a private or semi-private account, check who has access every once in a while.
- Keep an eye on the news for platforms you use. Whenever they announce new functionality, RECHECK YOUR SETTINGS.
  - Both Facebook and Twitter are notorious for using new features as an excuse to damage users' privacy.
- Consider periodically deleting old stuff.
  - I do this on Twitter. Platforms don't always make this easy, but it can usually be done, somehow or other.
- Don't stay logged in all the time.

BLOCKING STRATEGIES

...in rough order
from least intrusive to most

Tracker-blocking browser plugins

- Typically block trackers, tracking cookies, marketing/social media "web bugs." May block *coin-harvesting code.
  - They do not block ads just because they're ads!
  - They do help keep ads from damaging privacy. Sometimes this does mean blocking the ad.
- Several available, but the one I recommend for desktop/laptop browsers is Privacy Badger (yes!) from the Electronic Frontier Foundation.
  - Learn how to tweak and disable it, just in case.
- Mobile: no equivalent that I'm aware; you'll have to go to an ad blocker.

Ad blockers

- Adblock is popular, and fine if it's what you have.
  - Add EasyList for automatic blocking of many ads.
  - Dig into the preferences to disable Adblock's payola-based unblocker.
- If you don't have one yet, try UBlock Origin instead.
  - Be careful to ensure you have the right plugin! Jerk malware creators disguise malware as UBlock Origin lookalikes.
- Suggest installing an adblocker in the browser of an Internet-naïve or otherwise scam-vulnerable person.
- Ads are carrying malware these days. This is another fine reason to install an ad blocker!

Other browser add-ons

- Be REALLY CAREFUL about these in Chrome.
- Google isn't assessing Chrome add-ons for whether they track you unnecessarily. A lot of them do, it turns out.
- Whatever browser you use, it's wise to go through your extensions once or twice a year to disable unneeded ones and update all of them.

Flash

- Dying, but still a malware and tracking vector.
- Change your browser settings (or add a browser plugin) to make you click on Flash objects for them to work.
  - Firefox: type about:addons in your URL bar, go to Plugins tab, pick “Ask to Activate” for Shockwave Flash.
- You will be AMAZED and HORRIFIED at how much Flash there is that doesn’t do anything useful.
  - (A lot of it is ONLY THERE TO TRACK YOU.)

*coin harvesting code

- Bitcoin etc. I'm not even going to get into how blockchain currencies work.
- What you need to know: some people add currency-mining code to their websites to leech off your machine's processing power.
- Right now (2018), you'll need a specific coin-blocking plugin. I have hopes regular ad-blockers will add this soon, however.

ENCRYPTION STRATEGIES

Consider…

- … encrypting your hard drive. Your operating system makes this an option.
- … encrypting your PHONE, especially since you're so much more likely to lose it or have it stolen.
  - Security apps are a good idea too.
- … phone passcodes! Use them, even if you have TouchID or similar. Make them as long as the system allows!
  - Legal weirdness: law enforcement can compel you to use your finger more easily than it can compel you to reveal a password or passcode.

Backups: a security must

- Not just for computer breakdowns any more!
- "**Ransomware**:" when somebody ELSE encrypts (locks up) the data on your computer, then demands money to decrypt (unlock) it.
- If you have a good backup, you can flip the criminals off, wipe your computer clean, and restore your data.
- If you don't have a backup... you're hosed.
- That raises a question, though: secure backups?

(More) secure backups

- A hard drive in your home or office, kept offline, is pretty secure as these things go.
  - Risk: you're connected while malware/ransomware ends up on your hard drive, such that it too is backed up, and it reinfects your computer. This isn't super-common, though.
  - Risk: you don't back up often enough. THIS is VERY common. Make your computer back itself up on a schedule if at all possible!
- Cloud storage: mostly not terribly secure, sorry.

Encrypted cloud storage

- Cloud storage: Look for the phrase "zero knowledge" or "no knowledge." Just saying "encrypted" is NOT GOOD ENOUGH.
  - (The question is who's holding the encryption key: you or them.)
  - Providers worth looking at: SpiderOak, Tresorit
- DROPBOX IS NOT SECURE. DO NOT USE IT AS THOUGH IT WERE.
  - Documented cases of employees snooping, mass account hacks, spooks allowed behind the scenes.
  - If you must: encrypt files first, then send to Dropbox.
  - I think it's way easier to use a zero-knowledge provider to begin with.
- GOOGLE APPS/DRIVE ARE NOT SECURE plus Google surveils everything anyway.

HTTPS Everywhere

- EVERYONE SHOULD INSTALL THIS EVERYWHERE IT WILL WORK.
- Browser plugin (Firefox, Chrome, Opera, Firefox/Android) that automatically sends you to the secure (encrypted) version of any website that has one
- Almost entirely unobtrusive; you won't even know it's there.
  - Like, once or twice a YEAR I run into a site that this breaks?
- https://www.eff.org/https-everywhere

Off the Record (OTR)

- Encryption for instant messaging/chat.
- Works with quite a few chat protocols.
- You may need to use a different chat client. It's worth it!
- Alternately...

Signal

- Signal is the most private chat/messaging service available today.
  - They even scrub metadata! We know this because they've been NSAed!
- Move yourself, move your friends.
- https://whispersystems.org/

Wired computer connections

- Whenever possible, use an Ethernet cable instead of wifi.
- All else being equal, wired is more secure than wireless.
- Mobile: keep your wifi turned OFF until you actually need it.

Wireless encryption

- Snooping unencrypted wireless traffic is TRIVIAL.
- ENCRYPT YOUR HOME WIRELESS. Talk to your nerds about this.
- WPA2 is better than WPA, which is better than WEP, which is (marginally) better than nothing.
  - ... they're all kind of bad, honestly. But it's what we have.
- WPA3 is coming! When it arrives, move to it.

Virtual Private Networks (VPNs)

- Like a wired connection, only over wireless.
  - The initial setup is annoying, but once it's set up, it's easy to turn on.
- UW-Madison has a VPN that you may use.
  - You will have to install some software and/or fiddle with networking connections... but once that's all set, connecting to the VPN is easy.
  - Interested? Go to http://kb.wisc.edu and search for "GlobalProtect" then find installation instructions for your operating system. Or go to one of the DoIT helpdesks, and they'll help you!
  - Works on mobile too!
- You can also pay for a VPN provider.
- ESPECIALLY useful if you use airport or coffeehouse wifi.

Will any VPN do?

- No, unfortunately.
- Using a VPN moves your trackable browsing habits from your (probably untrustworthy) ISP to your VPN...
- ... but that assumes your VPN can be trusted not to log you and/or sell you out! Not all VPNs are trustworthy!
- As yet there's no way to prove (or even test) a VPN's privacy assertions. I hope and believe this will change.
- Look for VPNs recommended by technical folks.

The Onion Router (TOR)

- Foils attacks based on analyzing network traffic
- Routes bits and bytes through a labyrinth
- Hides your physical location
- Will slow down browsing appreciably!
- Does help create “herd immunity” to surveillance, however.
- Not quite the nuclear option, but... rocket-launcher option, maybe?

TOR options

- TOR Browser (Firefox + Tor)
- Orbot (TOR browser for Android; highly recommended!)
- The completely nuclear option: Tails operating system
  - An OS-on-a-stick that you can boot your computer from.
  - Designed to remember absolutely nothing.
- If you're nerdy and you know it: please consider running a TOR exit node.

“OPSEC”

“operational security”

Things not to do

- Do not EVER EVER EVER click on a link in an email. DO NOT DO THIS. EVER.
  - Copy (or right-click)-and-paste if you must.
  - Scrutinize the URL really carefully first, though!
- Don't log in to a non-Facebook site via Facebook. Same for Google, GitHub, Twitter. Separate your accounts!
  - If you don't, somebody who hacks your Facebook has access to lots more... as demonstrated in the Great Facebook Hack of 2018.
- DON'T GIVE ANYONE YOUR PASSWORDS.
  - Never ASK anyone for them either. Ask to have them reset, instead.
- Don't let your computer or phone auto-login. Type your username and password or passcode every time.

Thanks!

And be careful out there.