Table of Contents

Why Does Security and Privacy Matter in the Digital Age?

> Why "If you don't have anything to hide, you shouldn't worry", or "If you aren't doing anything illegal, why would you care if someone is watching you?" is bullshit.

Most of us go about our daily lives without considering whether anyone is watching us – and definitely not being actively worried about it. So why should you care about privacy if you're just an average person?

The best argument for privacy is that the government gets to define what's wrong (aka illegal), and you have no way of knowing when that is going to change. Something that seems totally safe to do right now (for instance, smoking weed in Colorado where it is currently legalized) could easily become dangerous with a few changes to the law. The thing to remember is: if you watch anyone long enough, it will always be possible to find something with which to arrest them. Perfect knowledge gives the government unlimited power to take action against you. The truth is, the world has been steadily moving towards a surveillance state for years, which means the government has all the tools it needs to watch you. And with the COVID-19 pandemic, governments now have a plausible excuse for utilizing surveillance tools for "social good".

It's also good to remember that we're not just worried about the government here – data thieves, ransomware makers, and fringe groups frequently use personal information to make someone's life a nightmare. We talk about these groups more in a couple sections below.

Also, there is a bunch of research that shows that just wondering if you are being watched is enough to make people modify their behavior and self-censor. A place where people start thinking how they are talking and who could be listening is a very scary place to live … and maybe we are already there. It's really important to protect your privacy so you don't end up descending even deeper into a paranoid 1984 existence!

Put another way, this is what Bruce Schneier, one of the country's most well-known security experts and advocates, has to say on the subject:

> *Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without*

> *intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide.*

Important Disclosure

Just as with sexual activity, nothing you can do when it comes to the internet/digital communications is 100% safe. This document is designed to help you practice "safer security" not "safe security". The world of surveillance and security is ever-shifting. New solutions come out just as new vulnerabilities are discovered. So take all that follows as an awesome guide to safety, a "condom" if you will on the imperfect reality in which we live.

It's also important to note that this document is not designed to scare you, make you paranoid, or cause you to build a Luddite bubble from which you can live without the concerns of the internet or technology. For most of what follows, once you set it up you really don't have to think about it again – or at least not until a better version comes out. And when that happens, you can just check out the updated version of this guide!

Encryption 101 – Not Just Spy Stuff

According to Wikipedia:

> *Encryption is the process of encoding messages or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies intelligible content to a would-be interceptor.*

So basically, encryption is like speaking in a made-up language to your best childhood friend (before he started ignoring you for the cool kids).

Want to know more? Here is a great nerdy resource. Many of the resources shared below are encrypted, which means they protect your content from being easily viewable by those who would like to get into your stuff but who you didn't send it to on purpose.

Assess Your Risk – Who Are You Worried About and What Are Your Assets?

Risk / Threat assessment is important because any time you bolster your security measures, there is a trade-off in convenience. It's important to implement things you will actually follow through with (because if you don't use it, it won't work!), so take some time and consider what risk you're actually worried about. Higher risk = more effort to protect yourself.

Surveillance Types – Dragnet and Targeted

The two general types of surveillance are **dragnet surveillance** and **targeted surveillance**.

Dragnet surveillance is when the NSA, data thieves, or ransomware hackers intercept all internet traffic and scans/flags/stores it. So as long as you're doing things on the internet, you're dragged into the proverbial net no matter who you are or what you're up to. This is the lowest hanging fruit, so if you have low security practices, you could easily get caught up in this type of surveillance.

Targeted surveillance is when the government, ransomware hackers, or fringe groups are following you personally because you've already been flagged due to who you are or what you're up to (e.g., activist, drug dealer, rich person).

Are you generally concerned about being swept up in dragnet surveillance or are you concerned your activities could make you the target of specific governmental or 3rd party surveillance? This is how you assess your risk. This is important because depending on what type of surveillance you're concerned with, you may want to implement different security measures (described below).

Surveillance Types – Physical and Remote

Your data can be surveilled via physical access to your device (as when a police officer asks you to unlock your phone so they can see what's on it) or remote access (via the internet).

Malicious Actors and Their Nefarious Tactics

So … who are we worried about?

Law Enforcement

Law enforcement includes the police, FBI, Secret Service, DEA, ICE, ATF, and Customs. These are the people you should be worried about **physically** accessing your devices (don't touch my stuff!). For example, if you cross a border with your laptop, Customs can force you to give up your passwords to your devices, and is allowed to hold your laptop for an undefined period (while they try to get into it) and can copy whatever they discover on it. Protesters who are arrested can get their phones seized by the police, who then can try to access the phone's information. The FBI can hack **remotely** into online accounts including email. According to this new-ish law, the NSA has the right to pass any illegal activity they discover through **dragnet surveillance** to law enforcement for prosecution. Also did you know that in the United States, the "border" actually stretches 100 miles from the literal border? This means that a majority of Americans actually live under border control laws and so these Custom laws apply.

Intelligence Agencies

Intelligence Agencies include the CIA, NSA, and every international agency (including those in the Five Eyes Treaty: United States, United Kingdom, Canada, Australia, New Zealand). These agencies have the ability to perform mass-scale **remote** surveillance – **both dragnet and targeted**.

Data Thieves

Data thieves are people who steal your person data to either sell it on black markets or use it themselves to do things like open up new lines of credit or buy expensive gear. There are places online where you can buy a person's personal data for as little as $1USD. This is why people hack corporate or governmental databases – so they can sell massive datasets. Data thieves mostly engage in **remote dragnet surveillance**. There are now cases of people stealing laptops to wipe and resell, but finding your nudes or other potentially valuable content which they now have. This is a different type of data thievery. We could call this incidental data thievery.

Ransomware Hackers

Ransomware makers hijack people's systems or data and hold them ransom for money. When they do this to governments it can look like "I just shut down your traffic light system and will keep doing it unless you give me X amount of money". For individuals, this can look like "I just wiped your computer and backups and I have your dissertation drafts and research, give me money and I'll give you the backup I made". Ransomware hackers tend to engage in **remote targeted surveillance** because they will be looking to target people who have money, but they also could cast a wide net through **remote dragnet surveillance** to see if they can stumble on something valuable.

Fringe Hackers

Fringe groups hack computers to personally threaten activists, journalists, researchers, scientists … you name it. With fringe hackers, you're worried about remote hacking – similar to intelligence agencies. Their tactics are mostly focused on identity theft, blackmail, and harassment (including doxing, which is when hackers research and then share private information about an individual which opens you up to mob harassment, and swatting, which is when someone calls in a 911 armed assailant report to an address such that the swat team shows up and kicks down your door). See Gamergate for examples of both doxing and swatting that have targeted women. This is **remote targeted surveillance**.

Distrust…and Verify

The fundamental premise behind digital security is distrust – that you cannot trust 3rd parties. When you use email, don't assume that the service provider (Gmail, Facebook, any website) is being responsible and confidential with your data. In fact, we are always learning how much we *should not* trust these companies – that they are using our data ethically and that our data is secure. What you have to ask yourself is: when a company claims your data is encrypted, what does that mean? Have they opened their software up to security audits by 3rd party experts? Is the software open-source?

Use Open-Source Applications Whenever Possible

Why is open-source software good to use? Open-source means that the source code is open for viewing and modification by the public. This means that open-source software can get vetted by unlimited experts (outside of the people who made the software/are selling it) to make sure that a

service is as secure as it claims to be. It also makes it harder for governments to install unnoticed backdoors – they can still try, but software designers are more likely to notice and take action.

Whenever possible, use open-source options. It is going to be more secure – this means: Linux over Windows/OS X, Firefox vs. Google Chrome, Keypass vs. Lastpass, etc.

The level of distrust and verification depends on your threat modeling. If you are worried only about dragnet surveillance, you may feel secure using a service that says it is encrypted, even if it's not open-source so you can't 100% verify that they aren't sharing your data with 3rd parties (which could be advertisers or could be the government). If you're worried about targeted surveillance, you will likely want to take additional steps to avoid handing services as little of your data as possible. We will discuss this in excessive detail below, don't worry!

Now for The Nitty Gritty: What Do You Actually Need to Do?

DISCUSSION: What security practices do you currently use?

1. Actually Deal with Your Account Security

Turn on Two-Factor Authorization

Two-Factor Authorization requires that you provide not only your account password but also a unique one-time code to be entered in order to get into your account from a new device.

Justification

Password databases get cracked/leaked all the time, and there are many ways for your password to get intercepted. Two-Factor Authorization makes it necessary for a 3rd party to have your account information and phone to hijack an account or steal personal information – see the last episode of Season 1 of Mr. Robot for a fun example of this.

Two-Factor Authentication works like this: after you sign in, the website/service requires a code that you receive either through an app (Authy or Authenticator) or via SMS/text/email. You need to input this code into the website/service before you can access it. Always use Authenticator or Authy whenever possible, as someone could intercept the SMS or email code.

Supported Services

Here is a list of all sites that support Two-Factor Authorization: https://twofactorauth.org/.
Google search "service name + two factor authorization", and follow instructions to set up.

Protections

Targeted online account hacking

Action Items

- ✓ Download Google Authenticator or Authy
- ✓ Set up Two-factor Authentication on all sites you use that allow for it

Create Passwords that are Unique and Unmemorable

It's important for your password to be unique (not something obvious someone else can guess) and unmemorable (if a password is strong and secure, you won't be able to remember it because it will be too complex and random).

Justification

Many passwords are the same, and you don't want your account to be the low-hanging fruit for brute force hacking (which is when a hacker tries many, many attempts to guess your password. This isn't like a movie where a human "guesses", they use software to test millions of passwords per minute). For mathematic reasons, you want your password to be highly complex for when an entire database of encrypted passwords gets stolen (which we now know happens all the time). Given enough time, any password database can be decrypted. You can check out Firefox Monitor to see just how many of your accounts have been compromised (that we know about). You can also sign into Firefox Monitor to have the system automatically alert you if a database containing information leaked to the email address you input is leaked. Pro tip: Do not set your password manager's password to be a password you've used elsewhere. It should be unique.

Supported Services

Anything that has a password

Protections

Both dragnet and targeted surveillance – it protects against you being the low-hanging fruit in large-scale hacks, and makes it more difficult for the government/other targeted hackers to guess your password (or have their high-speed computer guess it for them)

Action Items

- ✓ Download Keypass (Windows) or KeypassXC (Mac) to have a free, open-source password manager/generator. This service creates strong passwords and keeps them all in a single encrypted place so you don't have to remember them – you just need to create and remember one solid password that gives you access to this service. You can save this list on your desktop, in a secure cloud service like Dropbox, Box, or Google Drive, and/or on a USB stick – which you can keep on your keychain.
- ✓ Download Keypad Touch (iOS) or Keypass2Android (Android) to have a version of Keypass on your phone, so you can access your passwords when you're away from your computer or laptop.

- ✓ Here's how you set up Keypass Touch (iOS):
  - Download Keypass Touch.
  - Open the app.
  - Click the option to sync it with Dropbox.
  - Enter your Dropbox credentials (user name and password). You can use the Dropbox app or just navigate to it online if you don't want to have another app on your phone.
  - Navigate to the folder your Keypass file is in and click it to open. It should be named DATABASENAME.kdb. Click it to open your Keypass!
  - Make sure to make the Keypass document available offline – it's a function on Dropbox. That way you will be able to access it when you don't have internet access on your phone.
- ✓ Here's how you set up Keepass2Android (Android):
  - Download Keepass2Android.
  - Click the app → Click Open File → Dropbox → Allow → Navigate to .kpx file
  - Enter your Dropbox credentials (user name and password).
  - Navigate to the folder your Keypass file is in and click it to open. It should be named DATABASENAME.kdb. Click it to open your Keypass!

Change Your Passwords Regularly

It's important for your password to be changed regularly - every 6 months is optimal, once a year at minimum.

Justification

If an entire database of encrypted passwords gets stolen, it's only a matter of time until the thief decrypts it. You want to protect your information for when that happens (and companies won't necessarily tell you when they are hacked, although they will usually know) by having a different password by then.

Supported Services

Anything that has a password

Protections

Both dragnet and targeted surveillance – it protects against you being the low-hanging fruit in large-scale hacks and in targeted attempts to guess your password because by the time the hacker gets around to decrypting your password, it will have changed and their stolen information will be outdated.

Action Items

- ✓ If you are using Keypass, set your passwords to automatically expire after a certain amount of time – every 6 months is best practice, a year is better than nothing. You will still have to manually change the password on the source site, but you will have a reminder to do so!

- ✓ If you are not using Keypass, set an alarm on your phone/calendar to remind yourself to change your passwords every 6-12 months.

Lie on Your Security Question Responses (But Remember Your Falsehoods!)

It's important to have security question answers that people can't find the answers to easily on the internet.

Justification

Security questions are a common way to reset a password, and the question prompts are often similar or the same (e.g., what's your mother's maiden name, what town were you born in). Many of these responses are really easy to find through a simple Internet search (seriously, try looking up your name and see how long it takes to get to the answers to these questions). Whenever possible, answer questions that can't be found in this way (for example, some sites have options like what was your favorite band in high school, what was the name of your first pet) but if there are only very simple options – lie. If you're worried you might not remember your fake responses, swap responses with a friend you know very well.

Supported Services

Anything that has a password

Protections

This is really only relevant for targeted surveillance because it assumes someone is trying to sign into a service as you and they don't have your password so they are trying to reset it.

Action Items

- ✓ If you have existing security questions already set up, see if you can change them to topics less possible for someone to find just by searching your name on Google.
- ✓ Pair up with a buddy and set your responses together – using each other's information.

2. Be Real About Your Communications

Use Encrypted Messaging Services

Encrypted messaging apps.

Justification

All messages can be (and already are) intercepted by 3rd parties, including the government (NSA). If you don't want your texts to be read, stop using SMS and iMessage – these messaging services are unencrypted and therefore easy to read (they are actually called "plaintext").

A number of encrypted messaging services exist, which protect your messages from being easily read by anyone intercepting them. Encrypted messages might always be unencrypted, although it can take a lot of computer time.

It's a good idea to use encrypted messaging systems even if you're not discussing anything activism-focused or illicit – this makes it more expensive for the NSA to store all the messages (they have disclosed they are storing all encrypted messages) and also provides "herd immunity" wherein the mere use of encrypted messaging doesn't mean much (as in, using a certain system doesn't automatically flag you as an activist, etc.).

Supported Services

You can use encrypted messaging services on your laptop, phone, or desktop. Signal is the strongest messaging app with built in end-to-end encryption right now. WhatsApp is fine if you're only worried about dragnet surveillance but records the metadata of the communication (who you speak to, when you speak to them, potentially where you're speaking from if your GPS is on) and reserves the right to give this metadata to the government if requested. Did you know that WhatsApp is owned by Facebook? It is not open-source.

Protections

Dragnet, and targeted surveillance to a large but unverifiable degree – the problem with all encryption platforms is that you are trusting that the software generates an encryption key just for you and doesn't also send it anywhere else, where someone else could potentially view it (including the government, employees, etc.). If you're worried about targeted surveillance, read on – we'll be talking more below about how you can set up further protections for your messages.

Action Items

- ✓ Download Signal (if you're on iPhone, you'll need to turn on notifications for Signal inside System Preferences / Settings → Notifications → Signal)

Use Encrypted Video Services

Encrypted video chat apps or services.

Justification

There are many video chat services people use to stay in touch. These include: Zoom, Google Hangout, FaceTime, Slack, WhatsApp, Discord, and Signal. Particularly now, with shelter-in-place requirements as a result of the COVID-19 pandemic, video chat and group video chat are becoming increasingly part of our lives. All of these offerings (except for Signal and WhatsApp) have link encryption, which means that the data is encrypted while it is being transmitted from your device to the company server, but is not encrypted on the company server. This means that your data is protected from non-governmental 3rd party actors trying to intercept your communication, but the company has access. This means the government potentially has access if they request it from the

company and the company acquiesces, and further that anyone hacking the company (or government) could gain access to your content.

WhatsApp and Signal have end-to-end encryption, which means not only is your communication encrypted during transmission, but the company cannot see your content on their end either. This means your data can be stored but not seen without being decrypted. However, as we discussed in the last section, WhatsApp does store and share your calls' metadata. Further, WhatsApp and Signal don't support group chat.

Supported Services

Signal is the strongest video app with built in end-to-end encryption right now. It currently only allows you to video chat with one person at a time.

There are some things you can do to improve your security on link encrypted services, which are all the group video chat offerings right now. These only protect you against 3rd party aggressors. These include:

- Keep your room meeting code private (i.e., only give it to people you actually want to chat with)
- Add a password to your chats (you can do this for Zoom; here's how).
- Enable a "waiting room" so you can let people into your chat manually (this is currently only a Zoom feature; here's how to enable it)

Protections

Dragnet, and targeted surveillance to a large but unverifiable degree – the problem with all encryption platforms is that you are trusting that the software generates an encryption key just for you and doesn't also send it anywhere else, where someone else could potentially view it (including the government, employees, etc.). If you're worried about targeted surveillance, read on – we'll be talking more below about how you can set up further protections for your video messages.

Action Items

- ✓ Download Signal (if you're on iPhone, you'll need to turn on notifications for Signal inside System Preferences / Settings → Notifications → Signal) for one-on-one encrypted video chat (for your nudes!)

3. Pay Attention to Your Hardware

Encrypt Your Devices' Physical Storage

Encrypt laptop hard drive, phone

Justification

If a 3rd party steals your device (or the government seizes it) it's easy for them to access any unencrypted data. Device-level encryption makes this much more expensive/difficult because they have to find a way to hack or decrypt it. Think of the San Bernardino iPhone case.

Be aware that full disk encryption (where you encrypt your complete device) is only fully secure when the device is turned off. If you get caught with your device powered on, the level of protection is much lower because you are always going to have unencrypted things in your memory – your computer has to decrypt files for you to be able to use them. It's always a good idea to turn off your devices before going through Customs at national borders, or if you bring your devices to a protest or sensitive meeting (anywhere you might get arrested).

Supported Services
Laptop, desktop, phone

Protections
This is mostly relevant for targeted surveillance, where you're worried that law enforcement will physically take your computer to read its contents, but is also relevant for dragnet surveillance if you are traveling across borders.

Action Items

- ✓ For Windows: go to Control Panel → System & Security → BitLocker Drive Encryption → Turn on BitLocker for Operating System drive. And you're encrypted!
- ✓ For Mac: go to System Preferences → Security & Privacy → FileVault → Click "Turn On FileVault". And you're encrypted!
- ✓ For Android: Settings → Security → click "Encrypt Phone" → Click "Require screen lock to decrypt data when phone turns on". Note: this will vary based on your system version. And you're encrypted!
- ✓ For iPhone: go to Settings → Passcode → Set Passcode. Once you've set a passcode, you should see "Data protection is enabled" at the bottom of your screen. And you're encrypted!

Tape Over Your Webcams

Obscure internet-connected cameras.

Justification
Any camera that is connected to the internet can be remotely activated by other people (without you even knowing). For instance, Apple used to claim that the light on their camera was hardware-forced to turn on when it was activated; however, a hack later showed that was not actually true. Webcam activation is useful for blackmail, surveillance/tracking, home robbery...etc. To protect yourself, put tape over the camera on your laptop, or buy a sliding webcam cover. You can also put tape or a sliding cover over the front-facing camera on your phone (if you don't use it much), and then you can place your phone face-up and not have an active useable camera for spying. If you are always taking selfies,

you can still put a sticker on the front of your camera and just remember to remove it before taking your pics.

Supported Services
Gaff tape, stickers

Protections
This is relevant for both dragnet and targeted surveillance – if someone wants to watch you in particular, this is a really simple way for them to do so, but also remember that you can probably be caught doing something illegal/suspect if someone is watching you all the time.

Action Items
- ✓ Put a piece of gaff tape/removable tape over your computer camera and/or phone, or buy a sliding webcam cover for your computer and/or phone.

Silence Your Microphone

Use a dummy microphone plug.

Justification
Microphones are passive devices – this means they are always working, always listening. All someone has to do is decide to listen to you on your device and the data is there for the taking. You wouldn't know if someone was listening to you. By plugging in something into the microphone jack on your computer or the headphone jack on your phone, your device detects that and ignores the data being collected from the microphone – because you're listening to something! This method only blocks dragnet surveillance because it tricks the software, but someone could code software to override that and keep listening. Note: this trick doesn't work for new iPhones, because they don't have a headphone jack.

Supported Services
Old headphones with a built-in you don't mind mutilating, mic-lock

Protections
This is relevant for dragnet – you can probably be caught doing something illegal/suspect if someone is listening to you all the time.

Action Items
- ✓ Cut the plug end off of an old pair of headphones that have a microphone in them (it will have three rings on the jack; headphones without microphones just have two rings).
- ✓ Put that in your computer microphone port and/or phone headphone jack.
- ✓ Alternately, you can buy a mic-lock which is essentially the same thing.

Make Sure Your Operating Systems Are Updated

Keep devices as up to date as possible.

Justification

You know how your phone and computer periodically make you download updates? That's because developers are always thinking of ways to make your systems run better. These security patches are really important because they close holes in your operating system. Devices with widely known unpatched security holes are low-hanging fruit for hackers and government agencies. Either make a habit of checking the update page app for whatever device you are using, or set it up for automatic update download and install.

Supported Services

All operating systems, apps

Protections

This is relevant for both dragnet and targeted surveillance – you never want to be the low-hanging fruit for hackers, whether they are specifically trying to get your information or just any information they can.

Action Items

- ✓ For Windows computers, go to Control Panel → Windows Update.
- ✓ For Mac computers, go to the App store → Updates tab. Download any updates.
- ✓ For Android devices, go to Settings → System Updates for Operating System updates. Application updates are in the Play Store → My Apps and Games → Update individually/all as you see fit.
- ✓ For iPhone devices, go to the App Store → Updates. Download any updates.

Encrypt Your Back-Ups

Encrypt your backup storage.

Justification

If you're using a cloud service backup, you should make sure it's an encrypted one because otherwise all your backups are just wide open for anyone looking to be able to read them easily. The same goes for local backup tools (like TimeMachine). This is a big deal. In January 2020, Apple abandoned its plans to create an end-to-end encrypted cloud service due to FBI complaints that this service would make it more difficult for the FBI to gain access to people's data.

Supported Services

Spideroak is ranked the best, Crashplan second, and everything else follows (TimeMachine is also a good option). Unfortunately, there is no open-source encrypted backup solution available right now, and there has been no 3rd party audit of these offerings, so it's unclear how secure these options are.

Protections

Encrypted backup services will help protect you against dragnet surveillance (because you won't be the low-hanging fruit for hackers). However, if you are being targeted by the government there's no guarantee. This is because there is no open-source encrypted backup solution, so we simply don't know how secure they are. Something you could do is to encrypt your files before you back them up, that way they will be encrypted in the cloud backup system.

If you're using a local backup tool like TimeMachine, encrypting your backup drive is mostly important if you're worried about targeted surveillance as in the case of a police raid – if your laptop is encrypted but your TimeMachine drive is not, all the police have to do is go through your TimeMachine drive to get the full contents of your laptop.

Action Items

- ✓ If you're using Spideroak, congratulations! Encryption is built in.
- ✓ If you're using Crashplan, open Crashplan → Settings →Security →Custom Key → Generate → Save they key that appears below somewhere safe → Save.
- ✓ If you're using TimeMachine, click the TimeMachine icon in your system tray (the space next to your date and time on the top right of your computer). Open TimeMachine preferences → Click "Select Disk" → Remove your current disk by clicking "Remove Disk" → Click the disk you were using (which should say TimeMachine) → Click "Encrypt backups" → Click "Use Disk".

Don't Buy Devices with Always on Microphones

All voice-activated devices have microphones that never turn off – even when you have turned it off (or discontinued the service, as in the case of OnStar).

Justification

Any device that can be voice-activated is always listening. ALWAYS. There is an assumption of trust that they are not recording or transmitting when they are not activated, but that is a lot of trust. And they can always be turned on through hacking. Unfortunately, phones are also devices with always-on microphones, which is why we just talked about one way to subvert the microphone software (and if you're really concerned about being listened to, there's more options in the activist section below). For instance, there is proof that Apple was paying contractors to listen to Siri recordings.

Supported Services

Any voice-activated device, including Amazon Alexa and Echo, Google Home, Microsoft Connect, Smart Samsung and LG TVs, OnStar

Protections

This is relevant for both dragnet and targeted surveillance – if someone wants to listen to you in particular, this is a really simple way for them to do so, but also remember that you can probably be caught doing something illegal/suspect if someone is listening to you all the time. These microphones are always sending the data to the server to be analyzed – we don't know how much of this is being kept or what it's being used for.

Action Items

- ✓ Get rid of any voice-activated devices.
- ✓ Or if you don't want to do that, disconnect them from the internet (FYI this isn't possible with many of these devices).

Don't Use Public USB Charging Ports

Don't plug your phone into public USB charging ports. Always bring your own adapter and plug directly into the power outlet.

Justification

USB cables are data cables that also carry electricity, which is why we use them to charge our phones! If there's a malicious software put into the USB port (by a hacker, the government, whomever), someone can be hacking your phone, or introducing a virus into it.

Supported Services

USB ports

Protections

Dragnet – 3rd party hackers and governments have all been caught doing this

Action Items

- ✓ Always bring your USB-to-wall plug adapter ("brick") with you when you want to charge your phone in public.

4. Use Your Internet Wisely

Scrub Personal Information from the Internet

Your personal information, including your name, addresses, phone numbers, emails, date of birth, family member information are all on the internet in many places. Companies save this information (e.g., you sign up for a magazine to be sent to your home) and sell it to others.

Justification

This is mostly an issue if you're worried about online harassment – but it's a good idea to just not have that information out there for popular consumption. It could show up if you Google someone before a first date, for instance. And even if you don't care, a family member of yours might. So it's best to just not be findable in the first place!

Supported Services

Familytreenow.com, among many, many others

Protections

This is mostly a concern for people worried about doxing or other methods of internet harassment that migrate to the physical realm – so when someone finds your personal information on the internet and uses it to go to your house to harass you there, or finds the name of your family so they can be harassed as well.

Action Items

- ✓ Search your full name on multiple search engines (Google, Duck Duck Go, Bing, Ask Jeeves if that still exists) and see what comes up – if you see your personal information on a 3rd party site where you don't want it, unsubscribe.
- ✓ For Family Tree Now, go to www.familytreenow.com → search your name to find your profile → Click the record detail. Make sure it's you → Click "Opt Out" button. You're done!
- ✓ Do this every year to be sure you haven't gotten back on lists.

Do Not Use Public Computers

Computers in internet cafes, libraries, etc.

Justification

Public computers could be (and often are) compromised with viruses and key loggers (software that captures all keystrokes and sends them to a 3rd party, so they can capture your password information, credit card information, etc.). If at all possible, do not use public computers. If you have to use a public computer, use two-factor authentication (discussed above!) for all accounts you sign into, and change any passwords you used afterwards (on a non-public computer of course!).

Supported Services
Internet cafes, computers at hotels or libraries, etc.

Protections
Any viruses or key loggers put onto a public computer will capture information inputted by anyone who uses that computer, so this is mostly a dragnet surveillance issue but could be used to target a specific person or group.

Action Items
- ✓ Change passwords after using public computers.

The Same Goes for Public Wifi

Public, open wifi

Justification
Any unencrypted messages sent over public wifi can be read by the owner of the wifi or anyone who is intentionally listening.

Supported Services
Free wifi

Protections
This is mostly a dragnet issue, since anyone using the public wifi can be spied on. However, if someone being targeted uses a public wifi, they can be listened to intentionally.

Download and Delete Old Emails

Take emails off the server.

Justification
If someone is able to gain access to your email account, they will have every communication you have ever sent. This could include password reset information, bank statements, porn, you name it. To mitigate this, you can download your obsolete emails to your computer and delete them from your account. Bonus, you get space back in your email account! If you're following this instruction, be sure to back up your computer regularly – you don't want to lose everything!

Supported Services
Any web email browser

Protections

This is relevant to dragnet surveillance by non-governmental 3rd parties. If you're emailing sensitive material, then it's something to be particularly concerned with.

Action Items

- ✓ Download Thunderbird – an open-source local email application for your desktop (made by Mozilla, who makes Firefox).
- ✓ Link it to your email account (instructions depend on your provider – go to File → New → Existing Email Account, then add your email account credentials).
- ✓ After it has downloaded all your emails, go to your email account and delete all emails over a certain length of time.
- ✓ Set an alarm to do this a couple times a year.

To Consider … This Stuff Stacks

We have now gone through a number of things you can do to limit how much other people can spy on you. It's important to consider the ways in which you use these different devices and software simultaneously to mitigate your risk. For instance, if you are on public wifi but you're using Signal so all your messages are encrypted, it's less of a big deal if someone's using that free wifi to get information on people. On the other hand, if you are using a public computer, do not have two-factor authentication on, and you use the same or similar password for multiple accounts, someone could really do a lot of damage quickly. This is not to scare you – in some sense, it means you can pick and choose which of this long list of activities work for you. Every step helps get you safer!

We're Stronger Together!

We know that the government is reading all internet and messaging traffic, attempting to decrypt encrypted emails and messages, and storing all encrypted information they have not been able to decrypt yet. We also know that the government is targeting encrypted messages because it's assumed they contain sensitive information. However, this doesn't have to be the case. If everyone encrypts their messaging and email services, we can flood the system with all our conversation – mundane or otherwise. It's assumed that given enough time, anything can be decrypted at some future point. So if the government decrypts a new repository of data and we are all on there, they will have to wade through our party discussions, recipe swaps, and infinite laconic responses of "K" or "C u soon" to get to what they are looking for. It also makes it significantly more expensive for them to store.

If You're a Badass Activist, You Should Also…

Consider Your Use of the Cloud

If a 3rd party steals your device (or the government seizes it) it's easy for them to access any unencrypted data. Device-level encryption makes this much more expensive/difficult because they have to find a way to hack or decrypt it.

Justification

Anything on Dropbox, Google Drive, iCloud, or other cloud services (with the possible exception of Spideroak and Crashplan, possible because they are not open source so we are trusting what they say) can be read by employees of those companies, and also the government or anyone authorized by the company. If you're storing personal/incriminating information on the cloud, encrypt your data using Veracrypt before loading it onto the cloud service.

Supported Services

Anything connected to the cloud

Protections

This is relevant for targeted surveillance if you are worried that someone is going to look through what you have on the cloud.

Action Items

- ✓ Take confidential material off the Cloud.
- ✓ Use VeraCrypt to encrypt any materials before you put them onto the Cloud.

Encrypt Your Emails Containing Sensitive Material

Most email services have transmission encryption but not storage encryption. Using full end-to-end encryption protects you from dragnet and targeted surveillance.

Justification

US-based email services are all subject to US law, which can include the government demanding that they hand over your emails. The providers are then hit with gag orders so they can't tell users that their accounts have been compromised. When hackers break into companies, the companies are often slow to notify users – if they tell you at all.

To bump up your email security, you can use a PGP (which stands for "pretty good protection") encryption tool to set up a public / private key set. How this works is that you share the public key with anyone you want to message you – the public key allows anyone to encrypt a message, which you can then decrypt with the private key. You can have the other user send you their public key so you both

can exchange encrypted messages only the other person can read. Many journalists and security activists have a public key publicly listed on their website, which allows anyone to get in touch with them using an encrypted message.

Note: if you are using public / private encryption, please write your email in Microsoft Word, Textpad, or some other local text application – and not in your email drafts. These are automatically saved to the servers, so it's basically the same as sending the email.

Supported Services

GnuPG – open-source PGP encryption tool

Protections

This is really important for targeted surveillance, particularly journalists and activists.

Action Items

- ✓ Use GnuPG to encrypt email messages before putting them into your email service – content you put into even an email draft can be read by those services.

Leave Phones at Home During Sensitive Discussions

Leave your phone at home, remove your phone battery (if you have a really old phone that still allows you to take the battery out), or put your phone into a sound-insulated faraday cage to block all transmissions.

Justification

Phones can be easily tracked and more importantly, the microphone can be enabled and transmit even when your phone is turned off. Only phones with removable batteries can be securely disabled in this regard. So if you are at an action planning meeting, or discussing anything you don't want the government to be privy to, make sure your phone is not in "earshot". A metal box or pouch that functions as a faraday cage might work to block internet connectivity. Note: faraday cages block internet, they will not stop any already existing audio recording software that has been uploaded to your phone previously, which it then can upload to a server once internet connectivity has been restored. Also to consider: even if you turn off the GPS tracker on your phone, it is always on. That's how 911 calls work to find you if you're in need.

Supported Services

Faraday cage – purchase online or DIY at killyourphone.com

Protections

This is mostly important for targeted surveillance, but should also be considered by doctors and therapists who see patients who might be targeted.

Action Items

- ✓ Purchase or make a sound insulated faraday cage.

Disable the Microphone on your Devices

Unplug the microphones in your phone/laptop/computer.

Justification

As discussed previously, your phone and computer are always listening – just because you turn off the microphone does not mean that someone has not put overriding software on your device to keep listening anyways. If you never want anyone to be able to hear what you are saying when you are within earshot of your device, you can disable the hardware microphones (did you know your phone has multiple microphones?). This means you will only be able to listen to things on your device through headphones, so take that into consideration if you move forward with this. You can do this yourself if you're feeling very techie (this is not an easy maneuver), or you can go to a 3rd party store and ask them to do it for you.

Supported Services

Disabling the microphone hardware on your device(s)

Protections

This is mostly important for targeted surveillance, but should also be considered by doctors and therapists who see patients who might be targeted.

Action Items

- ✓ Disable your device microphones; here is a guide to get you started
- ✓ Pay someone else to disable your device microphones

Use Tor Browsers When Visiting Sensitive Sites

Tor is an internet protocol that allows you to route your internet traffic through multiple servers (called "nodes") such that most of the nodes don't know where your data is going or what it says. You're only truly anonymous when using Tor if you are also using encrypted services. This is because the last node (called the "exit node") that your data takes on its journey from you to your intended recipient can see your data.

Justification

If you are engaged in high-risk work where even the recipient of your communications or the websites you frequent could put you at risk, use of Tor Browsers can mitigate your risk – to some extent. It is not perfect and should not be relied on in isolation. Ideally, you would want to also encrypt your messages and access all sites from a public network (yes, we know we said that public computers can

be risky, but here the more important thing is to make sure your browsing history can't be traced back to *you*).

Supported Services
Tor Browser

Protections
This is mostly relevant to activists or journalists who are worried that their browser history or communication partner(s) could put them at risk.

Action Items
- ✓ Download Tor Browser

Use VPN to Cover Your Tracks

VPN stands for virtual private network. What this actually means is that it creates a high-security, encrypted connection to a server that stands between you and the general internet. You might already use this to access work remotely (or Netflix if you don't live in the US).

Justification
If you're doing high-risk work and are worried about targeted surveillance, a VPN will allow you to make a secure "tunnel" to another server that might not be watched (because it's not yours – it can be anywhere) and that server will pass your internet communications along. Just like Tor, if your data isn't encrypted, the VPN host company can read your data (and share it with the government, if they want). We recommend using VPN companies that do not have agreements with the US government.

Supported Services
Internet with VPN set up

Protections
This is relevant for people worried about targeted surveillance.

Action Items
- ✓ Go to TorrentFreak.com to find the most secure VPN option. This is subject to change – it depends on what you want, where you live, etc.

Get Your Organization to Set Up SecureDrop

Justification
SecureDrop is an open-source encrypted anonymous whistleblower submission system designed to allow organizations to securely accept documents from and communicate with anonymous sources. Think WikiLeaks but without all the complex baggage of Julian Assange.

Supported Services
SecureDrop

Protections
This is really only relevant for journalists and news organizations that deal in content that might be sensitive.

Action Items
- ✓ Have your organization contact the Freedom of the Press Foundation to gain access to SecureDrop
- ✓ Make sure your organization's information is visible online so people know they can send you anonymous tips

Don't Use Biometric Phone Unlock Options

Most smartphones have the capacity to be unlocked by fingerprint or facial recognition (called biometrics).

Justification
Any biometric unlock may seem convenient and safe (because it's your body, after all) but you can be easily forced to put your finger onto a keypad or point your face in a certain direction – and this isn't defined as self-incrimination in the US. This is also an issue in cases when you may be unconscious.

Supported Services
Smart devices, some laptops

Protections
Everyone should disable these features (because why not), but this is particularly important for people who have sensitive information stored on their devices who are worried they might be forced by law enforcement to share that information.

Action Items
- ✓ Discontinue any biometric unlock system on your devices

Use All The Tools In Your Toolbox!

Remember what we said before: all these tools stack to make you as secure from surveillance as possible.