

Protecting Data and Yourself in an Uncertain World

Risk is the likelihood that a particular threat will actually occur. It goes hand-in-hand with capability. You COULD get caught in an earthquake, but it is way more likely to happen in Los Angeles than it is in Chicago. There are a LOT of potential risks out there, but how likely are they to happen, and what are the repercussions if it does?

Trying to keep up with every potential risk and protect yourself from every potential vector is impossible and impractical. But there are ways to evaluate your risks and create a plan that has a balance between “hassle” and safety. This begins with evaluating the threats you face and planning how to counter those threats.

Improving your privacy is an ongoing process, if you try to do everything at once it may feel overwhelming.

Evaluating Risk

What do I need to protect?

- Your phone calls
- Your social media
- Your personal messages
- Your activities and locations
- Your writing/blog/articles
- Your email

How much do they want that information, and how easy is it for them to get it?

- How confidential should your communications and data be?
- Where is your data stored, how secure is it there?

Who do I need to protect it from?

- Law Enforcement
- Government
- Online attackers (Doxxing)
- Counter Protesters/Activists
- Family/Social Circle

What if that data is not protected? Who else is at risk if the data is exposed?

- Does your data expose other people?
- If you get exposed, who else is at risk?
- What is your personal risk if the data is made public or available to one of your threats?

Passwords

The most accessible and simplest thing to do is improve your passwords. To make this easier use a password vault application. There are a lot of them out there, ProtonPass (<https://proton.me/pass>) and Bitwarden (<https://bitwarden.com/>) both have free options and are highly recommended. Password suggestions:

- Minimum 12 Characters
- Multiple character types included (numbers, letters, special characters etc)
- Random or pseudo random
- Use an obscure phrase or phrase acronym
- DO NOT use anything that can be associated with you. You are easy to research.

Do NOT reuse passwords. Passwords get hacked and leaked all the time. If your password on one site is exposed, an attacker may attempt to use it on other popular sites.

Other relatively easy changes:

- Switching to a more privacy-focused browser on your computer and mobile devices. Tor, Brave and Firefox are a few options.
- Using a privacy-focused search engine. (such as DuckDuckGo instead of Bing or Google).
- Trying to use services that minimize data collection (for instance, messaging app Signal doesn't collect user data and is the gold standard of end-to-end encryption).
- Use Multi-factor Authentication (2FA) for sites and services that offer it.

Widening the Scope

After making sure your passwords are secure and taking some of the above small changes. It's time to expand your scope and think about your data. What information have you shared about yourself, what have you said about your personal politics, what do you say in your personal chats, message boards etc and who has access to that information?

If your data is being held by an online service, check their security policies. Ideally your data is encrypted "at rest and in motion". Which means that it is encrypted while it is stored, and while it is transferred.

Here is a list of services you **may** use (note this is not comprehensive):

- Email Services - e.g. Gmail, Apple mail, work email, hotmail, aol etc
- SMS - text messages, note security can be different between platforms (Apple to android, or the reverse)
- Chat/Messaging Apps - Facebook Messenger, WhatsApp, Instagram, Signal, Snapchat, Slack, Discord
- TikTok - Videos, comments and personal messaging
- Public Post based social media - Facebook, Instagram, Bluesky, Threads, Xitter

Can you think of other similar services you use?

Many of these services collect your data and use it to serve you content. Every time you react to, read a post or watch a video some applications track that, and collect that data together to create a profile of who you are. Be mindful of the data that you are giving away for free when you use these apps and what a company that becomes a bad actor might know about you.

Safe Tools

- Note this isn't a definitive list, just some recommendations
- Password Safes
 - Bitwarden
 - ProtonPass
- Safe Search Engine
 - DuckDuck Go
 - Start page
 - Brave Search
- Safe Browser
 - Tor
 - Brave
 - Firefox
- Web Meetings
 - Jitsi.org
- Email Service
 - Proton Mail
 - Tuta Mail
 - StartMail
- VPN
 - ProtonVPN
 - ExpressVPN
 - NordVPN
- Messaging
 - Signal

The logic of these tools is simple – avoid tools that collect your information, store it outside of your control, or leave it publicly exposed.

Action Security

Actions (protests, rallies, demonstrations etc) bring their own set of unique security concerns. If things go badly, both being involved in organizing an event as well as attending an event could end up targeting you for future problems. This means you want to make sure that your whole chain of activities is secure.

Attending

Before the event:

- Depending on the nature of the event don't broadcast to the public you are attending. Consider more personal communications, and use a secure messaging application to coordinate.
- If you need to search the internet for any information relating to the protest, use DuckDuckGo and private browsing sessions.
- **If you are planning on bringing a mobile device:**
 - Set up a Signal account. If you don't want to use your personal phone number, you can create a new phone number with Google Voice and register that with Signal.
 - Use signal to coordinate with your protest buddies.
 - Make sure your phone and your applications are fully up to date.

At the event:

- **1st Rule:** if you can leave your mobile device at home. **Do it.** There are 100s of ways for you to be tracked by your cell phone and the applications on it and it is difficult to turn them all off. Something as simple as your phone connecting to a local cell tower can tell authorities if you were in the area of the protest.
- If you NEED a cell phone on site, and can afford it, get a burner phone that you keep minimal data on. If you have an old cell phone hanging around that still works this might be a good use for it.
- Write down protest details and important security phone numbers on a piece of paper or your arm. Have phone numbers for local legal aid and/or emergency contacts.
- Do not use mapping applications to get yourself to the protest.
- If you need a mapping application try Apple Maps and DuckDuckGo Maps
- **If you are bringing a mobile device:**
 - Lock it with a passcode and disable biometrics. Use at least 8 characters in your passcode.
 - Currently law enforcement CANNOT force you to put in a passcode/pin but can and will use your face or fingerprint to access your device.
 - Turn off internet access and bluetooth unless you need it.
- Have a protest buddy.
 - Confirm meetup plans with your protest buddies before leaving for the event.

- Once you meet up, agree on a fallback location in case you get separated.
- Keep an eye out for designated event marshalls and follow their guidelines for a safe event.
- Remember that at some events there may be undercover police officers or agitators.
- Don't take pictures of people without permission.

After the event:

- Leave and delete Signal groups set up for that protest.
- Don't post pictures of people without their permission.

Other

These tips don't just protect you, but protect the safety and privacy of others as well!

- Think carefully about who you can safely share your involvement in activism with.
- Don't use email for protest related conversation.
- Google your full name occasionally and see what comes up.
- Do not "check in" to a protest on Facebook or any other service. You don't want to give third parties evidence that you were there. Police use subpoenas to get user information from Facebook and other social media companies all the time.
- If you take any photos, don't post them on social media. Images have extra information hidden in them that includes the time and place they were taken. If you send photos or videos out at all, only send them to people you trust, over secure means, long after and far away from the protest.
- When using Signal, enable "Disappearing Messages" for any sensitive conversations.
- Take extra care when accessing organisational information over public wifi - if you need to do this regularly then invest in a VPN.
- For groups and people that have more acute security concerns, a factory reset of mobile devices is recommended every few months to make sure any malicious tracking is wiped out (but this presents the inconvenience of re-configuring devices). You can also use iVerify to check for certain spyware.

Phone Data and Backups

Your phone is a data goldmine, full of tracking and identifying information. This includes where you have been, what you have said, and with whom you have communicated.

Assume that any messages you send, phone calls you make, or anything else you send or receive can be logged and recorded by the police. If your information is strongly encrypted, they may still have access to it, but they won't be able to decrypt it. Be sure to update your phone to the latest supported operating system (OS) well before an action.

Keeping backups of your important data is always a good idea, but the built-in cloud backups of iOS and Android pose a problem for activists. Backups made with iCloud are encrypted in such a way that employees at Apple can access them. This weakness is attributed to pressure from the FBI. Anything in the backup, which may include photos, contacts, unencrypted messages, and more, can be handed over to law enforcement. Keys to unlock the phone's full-disk encryption are also stored in the iCloud backup. This arrangement allows law enforcement to request the backup data from Apple and use the key to unlock the entire phone. It also offers a convenience, where if the user forgets their unlock code, Apple can still recover the device. For activists, the risk posed by your unlock keys being accessible to law enforcement is potentially greater than the benefits of that convenience. We do not recommend using iCloud backups.

Android leverages Google Drive for data backup, which does not generally contain unlock keys, but does automatically include app data, call data, contacts, calendar events, videos, and photos. Starting with Android version 9 (released in 2018), Google has offered end-to-end encrypted backups that even they cannot open without the user's passcode. If your phone uses version 9 or newer, this feature is automatically active as long as you have a lock screen protected with a PIN, pattern, or passcode. Do not use Android cloud backups prior to version 9.

If you have privacy concerns and your phone is no longer receiving software updates, consider not bringing it. If you are attending a protest without a phone, don't go alone. Arrange times and places where you can meet up with your buddies before you go to the protest.

References:

- <https://activistchecklist.org/>
- <https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442>
- <https://www.cnbc.com/2019/05/17/google-gmail-tracks-purchase-history-how-to-delete-it.html>
- <https://infosecforactivists.org/> - like everything here read it, know it
- <https://www.youtube.com/watch?v=nWEpW6KOZDs>
- <https://activisthandbook.org/tools/security>
- <https://ssd.eff.org/>
- <https://ssd.eff.org/module-categories/security-scenarios>
- <https://www.businessinsider.com/fbi-uses-instagram-etsy-linkedin-to-find-george-floyd-protester-2020-6>
- <https://thenextweb.com/news/both-yahoo-and-aol-are-scanning-customer-emails-to-attract-advertisers>

Worksheet - Building a Security Plan

When building a security plan, start by answering these six questions:

What do I want to protect?

Look at all of the rest of this packet and think about what kind of data risks you have

Who do I want to protect it from? Who are my adversaries?

Your list may include individuals, a government agency, or corporations. Depending on who your adversaries are, under some circumstances this list might be something you want to destroy after you're done security planning.

How bad are the consequences if I fail?

Will you get arrested, doxxed, harassed? Will there be employment repercussions?

How likely is it that I will need to protect it?

Are your adversaries likely to target you for surveillance? Are you likely to be harassed for your online speech?

How much trouble am I willing to go through to try to prevent potential consequences?

What changes are you willing to make to reduce your risk and your opponents capability?

Who are my allies? Who else does my data put at risk?

It is important to distinguish between what might happen and the probability it may happen. For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in Stockholm (where they are not).

If there are tools you are not ready to give up, we encourage you to research their privacy policies and what you can do to protect your data.

Assessing risks is both a personal and a subjective process. Many people find certain threats unacceptable no matter the likelihood they will occur because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

Create your own security plan based on your own unique situation. Then mark your calendar for a date in the future. This will prompt you to review your plan and check back in to determine whether it's still relevant to your situation.