An Activist's Guide to Operational Security (OpSec)

Updated 5FEB2025

Part 1: Overview and Planning

Who is this guide for?

This guide is for activists and resistors that are engaging in lawful, peaceful actions. If you're speaking out against governments, oligarchs, capitalism, or other powerful entities, you should spend time thinking about OpSec. As the saying goes: "Luck favors the prepared"

What's not covered here?

If you expect to be in environments where rubber bullets, tear gas, LRAD, or other crowd suppression measures are expected, the Information Security (InfoSec) portion of this guide might still be useful, but you should look to more advanced guides for proper gear and more advanced techniques.

Why should I care about OpSec?

Unless you share your SSN and bank account numbers on social media, you're already thinking about OpSec to some degree. The rise of fascism in the US is forcing us to pay close attention to the digital tools we use and the ways in which we communicate.

With the Government labeling Antifa as a domestic terrorism organization, Organizers need to be particularly careful. People that communicate with Organizers need to be careful to not expose them or other activists to unnecessary risk. "A chain is only as strong as its weakest link."

Is this the only time I need to think about OpSec?

Sorry, no. You'll want to revisit this content from time to time. The best practices we have here will evolve, and we'll pledge to keep things up to date. More importantly, your activism style will evolve with time, too, and you may start working with different groups than you were the first time that you read this guide. It's worth a periodic check-up to ensure that your situation hasn't shifted to the point that additional care is required.

This sounds hard. Where do I start?

This won't be hard. Start with these three steps:

1) Assess your Activism Activity Risk (the riskiest activities that you participate in)
2) Think about your own Personal Risk Tolerance
3) Talk with your protest group(s) about each person's Personal Risk Tolerance

Activism Activity Risk (Spiciness Scale)

Each activity has a certain level of intrinsic risk, and certain factors may increase that risk.

Bell Pepper (mild)	**Jalapeño (medium)**	**Ghost Pepper (hot)**
Attending an overpass protest during the day	Marching on the Streets	Observing or recording law enforcement or ICE
Making protest signs and/or displaying political art	Organizing peaceful protests	Organizing anti-ICE or pro-Palestine protests
Posting anti-administration or anti-Trump content on social media	Participating in anti-ICE or pro-Palestine actions	Staying at protests after curfew or at night
Writing postcards and/or calling Political Representatives	Protesting alone or in majority red areas	Using defensive gear (shields, goggles) or shouting at LEOs.
Emailing companies or individuals to advocate for politicized policy change		

Personal Risk Tolerance (Gnarly Scale)

People will engage in more or less risky behavior depending on their specific situation.

Pickleball (low)	**Mountain Biking (medium)**	**Bungee Jumping (high)**
Public-facing job	Stable job or progressive employer	Self employed or retired
Missing work would be a financial strain	Secondary income provider	Can easily afford an attorney
Primary income provider or caregiver		No dependents

Less privelege		Lots of privelege

It might seem logical to combine the Spicy Scale and the Gnarly Scale into an awesome measurement of OpSec rigor. Surprise! That's not how this works.

We're all in this together, so we must assume that other folks in our cohort(s) will have a lower Risk Tolerance than we do. As a result, the only thing that drives how vigilant we should be about OpSec is the Spicy Scale – it all comes down to the activity.

This guide will use different shades of purple to steer each person to the level of OpSec rigor that is appropriate for their planned activities.

Now we get to the good stuff!

Part 2: Where the Rubber Meets the Road

Phones - we've all got one

- Phones are powerful tools for fighting corruption, but they can also be used by the bad guys to track troublemakers
- The items in this list might be the hardest, simply because we're so used to having our phones with us all the time.

☐	Turn off biometric (fingerprint or face) unlocking when at events. Use a passcode instead that is at least 6 digits long.
☐	Don't use Google maps to navigate to/from protests. Use Apple Maps or Magic Earth.
☐	Don't use the default Android web browser. Use DuckDuckGo or Brave.
☐	Enable Two-Factor-Authentication (2FA) on any apps related to activism.
☐	Don't use texting, FB messenger, or WhatsApp for messaging. Use Signal.
☐	Leave your phone at home. (Take pictures with a digital camera) Note that you won't be able to call 911 in an emergency.
☐	Put your phone in airplane mode and store it in a Faraday bag before leaving home for events (blocks all radio signals). Only take it out of the bag in an emergency.
☐	Use a VPN from a reputable paid provider
☐	Disable your Advertising ID (Android only - this is the default on iPhone)
☐	When meeting in person to organize and plan, leave your phone at home or use a Faraday bag. Having your phone at the same location+same time as other organizers increases risk for everyone.
☐	Buy a burner phone and prepaid SIM card with cash. Leave your regular phone at home. Only turn on the burner phone when you are away from your home/work, and turn it off before you return home.

PC/Laptop

☐	Don't use Chrome browser – use DuckDuckGo or Brave
☐	Enable Two-Factor-Authentication (2FA) on any websites related to activism.
☐	Use unique passwords for each website. Use a reputable password manager.
☐	Use a paid and reputable VPN provider
☐	Use a VPN provider that has protected overseas servers - "secure core" or similar

Signal – it's a tool, not a shield

- Don't send anything that you wouldn't want read back to you in court
- Unless you know everyone in a group chat, assume that it's not secure
- There are no known instances of Signal being hacked. All of the Signal leaks have been due to human error or carelessness.
- If a group member is arrested or has their phone confiscated, notify the group admin ASAP.
- Delete sensitive messages for everyone. Must be done within the first 24 hours after posting.
- Some Signal settings are shared across all your devices, and some are specific to one device. Be aware of which settings need to be made on each device.

☐

Identity (any device):

- Don't use your real name or photo in your Signal profile. Use an alias.
- Hide your phone number: Settings > Privacy > Phone Number > Under "Who Can See My Number" > Select "Nobody".
- When connecting with others on Signal, don't share your phone number. Use a QR code or link. It's super easy.
- Enable Registration Lock. This prevents anyone from using your phone number to register a Signal account on a new device without your PIN. Note that if you turn this on and then forget your PIN, you won't ever be able to access your Signal account on a future device. Settings > Account > Registration Lock (turn on)

Notifications (each device):

- Disable notifications with sensitive info (so that it doesn't show on your lock screen): Settings > Notifications > Notification Content > Select "No Name or Content"

Disasppearing Messages (any device):

- Set the default disappearing message time: Settings > Privacy > Disappearing Messages: 1 week

Misc (each device):

- Make sure that you use a complex password for your signal account, and ensure that the password isn't used for anything other than Signal.
- Make sure that any device that is portable (phone, tablet, laptop) locks automatically after a certain period of inactivity and requires a password/passcode/fingerprint/face to unlock it. Disable biometric (face/fingerprint) unlocking before attending an event.
- Enable "screen lock": Settings > Privacy > Enable "Screen Lock". Set Screen Lock timeout to 5 minutes or less.
- Enable "hide in app switcher": Settings > Privacy > Enable "Screen Lock" then enable "Hide Screen in App Switcher." (iPhone) or "Screen Security" (Android)
- Disable link previews: Settings > Chats > Disable "Generate Link Previews"
- Incognito Keyboard: ON (Android only)

	Environment (each device): Be aware of your surroundings when using Signal. The best technology is no match for simple evesdropping or snooping. Try to position yourself so that nobody else can see your screen. If in public, be aware of where security cameras are facing. When joining video/voice calls, use earbuds/headphones so that nobody else can hear what others are saying.
☐	Signal Chat Admins: • Use a QR code to invite new members to Signal; don't ask them to share their name or phone number with you for the purposes of sign up. • Change the disappearing message time on existing DMs or Group Chats: Open the message thread you want to change > Click on the person's name (or group name) at the top of the screen > Disappearing Messages > Set to a short window. Note that disappearing message time is NOT retroactive. This means that if you had a running DM or GC with someone with no disappearing message time set, and then you set a disappearing message time, only NEW messages will dissappear after that time. It's necessary to delete old messages manually if they were sent without a disappearing message time set. It might be tempting to delete a whole DM from your device, but this won't delete the messages on the other person's device.
☐	Set the default disappearing message time: 1 day
☐	Set the default disappearing message time: 2 hours

Social media

- Your social media footprint is the most accessible part of your digital footprint by those that are building profiles of troublemakers. Now more than ever, think before you post.
- Boycotting social media platforms isn't part of OpSec, but think seriously about deleting: Xitter, TikTok, Facebook, and Instagram. They are all fascist-controlled.

☐	Assume that anything you post, even if anonymous, can be connected back to you.
☐	Disable location access for any social media app that you use on your phone (under App Settings).
☐	Do not post activist content on any social network where you are not anonymous.
☐	Never use social media for planning or organizing activism

Cloud file sharing

- Most big tech companies are friendly with the current administration.
- Don't use Google or Meta for file sharing.

☐	Use Dropbox (with encryption), Proton Drive or CryptPad. If using Dropbox, use the Public folder so that file recipiends don't need to log into Dropbox.
☐	Use Proton Drive or CryptPad.
☐	Use expiring or single-use links to content

email

- Certain tech companies make money letting computers read your emails.
- Most big tech companies are friendly with the current administration.

☐	Make a burner email account that isn't connected to you. Access it via VPN.
☐	Make an email account with a company that is EU-based (making it harder for the administration to access your content).
☐	Use a secure email service like ProtonMail, posteo.de, etc.

Video Conferencing

☐	Be aware of who is on the call. Be cautious if you don't recognize everyone.
☐	Be aware of who around you could overhear or see the call.
☐	Use Signal for audio and video conference calling (works really well).

In Real Life (IRL)

☐	At protests, be situationally aware. Watch for counterprotesters. Watch for fellow protesters that might need medical aid.
☐	Know in advance a safe direction to move if trouble breaks out.
☐	Take de-escalation training to more safely interact with counterprotestors.
☐	Take first aid classes. Bring water and basic first aid supplies with you to events.
☐	If driving to an event, use a route that avoids Automated License Plate Readers (ALPRs) like Flock. dontgetflocked.com does map routing around known ALPRs.

Part 3: Epilogue

We find ourselves at a very unsettling time in our country's history. Rights previously protected by the US Constitution are increasingly under attack. Peaceful protesters are being painted as extremists. Those outwardly critical of the current administration are being retalliated against, sometimes brutally.

For those of us brave enough to peacefully take a stand, this isn't a business-as-usual environment. Extra caution is warranted at this time, particularly if our goal is to continue to resist for as long as it takes. Now more than ever, it's important that we think about our fellow resistors and take steps to ensure that our own actions don't put others at increased risk.

This content is provided by the Ventura County, CA chapter of 50501, a nonpartisan, grassroots, volunteer-led movement dedicated to defending democracy, protecting constitutional liberties, and holding those in power accountable. We build community through peaceful action, civic engagement, and mutual aid. We organize for justice, inclusion, and transparent, accountable governance locally in Ventura County and upward to the state and federal levels. Our movement demonstrates that people-powered efforts can drive meaningful change now and for the future.

Part 4: Further Reading

Want to dig even deeper? Try these excellent resources:

https://activistchecklist.org