Digital Security for Arrestable Actions

ACTIVIST CHECKLIST

Last updated on **October 30, 2026** Takes about **20 minutes**

This is for pre-planned lower-risk nonviolent civil disobedience actions where some people are risking arrest but the legal consequences are relatively low. Best option: leave your phone at home or hand it to someone who is not risking arrest before deployment.

This guide covers digital security if you need to bring your phone to a nonviolent civil disobedience action (aka direct action) where some folks are planning to risk arrest. It's one part of keeping your crew safe. Your action should also plan for physical safety, have a safety team, and make sure everyone knows their rights. Our safety checklist for action organizers can help with all of these.

> **Assess your risk level**: This guide is for actions where you are taking relatively lower legal risk (example: a sit-in or chaining yourself to a door). If you are planning something where you are striving for anonymity or where the legal consequences are much higher, you should be taking a lot more precautions than this guide offers.

This guide is written for the following situation:

- This is an action that is centrally organized enough that you can set agreements around digital security that everyone will follow.
- You have encouraged most people attending the action to **not bring their phone**
- Some people still need their phones to coordinate your deployment (ie: tactical lead, medics, de-escalation team, etc.)
- The risk of arrest is high, or you are planning to risk arrest.
- You expect the police may try to use phone-cracking tools to access the data on the phones they confiscate.
- You are not concerned with surveillance to and from the action.

If any of these don't apply to your action, you may need to take more precautions. Check out the protest enhanced phone security section or consider bringing a secondary phone (sometimes called a "burner phone").

Tip for organizers: In the lead-up to the action, consider hosting a security party so your crew works through these steps together before the day of.

Why does this matter?

We know social movements have been surveilled, infiltrated, discredited, and obstructed by government agents (local cops, FBI, CIA, NSA, etc) for decades. The rise of technology means we're all being tracked and profiled (even if you've never been arrested).

Even when we are exercising our legal rights to free speech and assembly, there are many government forces that seek to crush dissent and criminalize activists. (See Minnesota 15 case)

But there are actions we can take to protect our movements! This guide offers some simple things we can all do before and during a protest/action to keep ourselves and the most vulnerable folks in our movements safer. Taking these precautions helps protect everyone you organize with (not just you and your data). It isn't a sign or admission of any kind of wrongdoing.

Threats to consider

- **Phone seizure and searching** - If arrested, police can try to break into your phone to access your messages, photos, and other private information to use as evidence
- **Monitoring of communications** - Police can intercept regular SMS texts and calls to gather info about protest plans and participants
- **Subpoena of your account data or cell carrier data** - Cops can get a court order to access your online accounts (like Google or Apple) or your communication/location data from your cell carrier.
- **Informants and undercover agents** - People in your meetings or group chats may be passing what they see and read to the police
- **Mapping activist networks** - By getting data from one person's phone, police can identify entire communities of activists and organizers connected to them

For everyone participating in the action

Important Agree as a crew that anyone risking arrest should hand their phone to a support person (or leave it at home)

Phones that are off and at lower risk of seizure help keep everyone safer.

For lower-risk arrestable actions, it's best to have everyone either A) leave their phone at home or B) **turn off their phones** and leave them with a support person. This is often a person doing jail support. This person should either not attend the action or be in a very low-risk position on the far edges of the action.

HOW TO SET A PHONE AGREEMENT FOR YOUR ACTION

1. **Decide which roles actually need a phone.** Usually this is only a few people, like the tactical lead, police liaison, or medics. Everyone else leaves their phones with the support person. Anyone in a high arrest risk role should not bring a phone. (Or they should immediately hand it over after deployment.)
2. **Before deployment, the support person collects most phones.**
3. **Make a plan for getting phones back to people after they are released**. This usually means the jail support person brings the phones to people after they are released.
4. **Share the agreement early and repeat it** at trainings and the action briefing.

Tip: If there are a lot of phones and you need to confirm each person is the true owner of the phone they point to in the stack, you can ask them to unlock the phone in your presence.

Use Signal to communicate (texts/calls) for protests/actions

End-to-end encrypted messages protect your privacy from surveillance, while regular texts can be intercepted and read.

DO: Install and use the Signal (free) for your activism/political work

DO NOT: Use WhatsApp, Telegram, iMessage, regular texts (for your activism)

HOW TO INSTALL AND USE SIGNAL

1. Install Signal on your phone
2. Message or call your existing contacts using their phone number or ask someone for their signal username. They must have Signal installed also.

Check out our Signal Checklist for detailed instructions on configuring Signal to be as secure as possible.

- [ ] Important **Change your default settings so all new Signal threads have disappearing messages enabled**

This keeps everyone safer if someone's phone is ever confiscated or breached.

The best upgrade everyone can make to their use of Signal is to make sure that disappearing messages are enabled ***by default***. Most activists we talk to haven't enabled this by default. (And most people forget to enable it manually for each new thread.)

This keeps you safe and other people safe. We don't know who's phone will be seized by law enforcement. Even if we believe we're talking about perfectly legal things, the government can find ways to twist our words to attempt to make a case against us for our dissent

There are two things to track related to disappearing messages:

1. **First, change your default** so any thread you make has this feature enabled.
2. **Second, make sure it is enabled for threads that other people start:** if someone else starts the thread, it may not have disappearing messages enabled. You may need to enable it.

HOW TO ENABLE DISAPPEARING MESSAGES

1. **To change the default:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → set to your desired time (longer or shorter depending on your risk tolerance).
2. **(Android-only) Change your message retention limit:** This will delete messages on threads even that don't have disappearing messages turned on. (They will only be deleted on your device.) Open Signal → Tap your profile picture → **Settings** → **Data and storage** → **Manage storage** → **Keep Messages** → set to your desired max timeframe. Go back a screen and enable **Apply limits to linked devices**.
3. **To change existing threads:** Signal → 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 your desired time.
4. **Delete old messages/threads:** Disappearing messages does NOT apply retroactively. So you may want to delete old threads on your phone. This will not delete them on other people's phones, unfortunately. So if it is very sensitive, you may need to ask them to also manually delete the thread. (And while you're at it, encourage them to turn on disappearing messages by default!)

Choosing your disappearing message time: How long you set your disappearing times depends on the sensitivity of your messages. A question you might ask yourself is "if someone's device was confiscated or hacked, how important is it that these messages are not accessible?"

- For chatting about low-risk things with friends, you might choose 4 weeks.
- For standard political organizing, you might choose 1 week.
- For a higer-risk actions, you might set it to 1 day or 1 hour or 5 minutes, so the messages are gone before the action starts.

Note: Messages only disappear after the message has been read. So if the recipient doesn't read it for 2 weeks, and you have disappearing messages set to 4 weeks, it will actually disappear 6 weeks after you sent it.

Use Proton Docs to collaborate (instead of Google Docs)

Protect your group's data from Google tracking every doc you view

DO: Use Proton Docs (or Cryptpad) for organizing

DO NOT: Use Google Docs for organizing

Google tracks all user activity - including what documents you open, share, and access. Law enforcement can obtain this data through subpoenas/warrants, and they've been known to share it without proper authorization. Doing our organizing outside of Google Docs helps us keep each other more safe.

Proton Docs is a high-quality alternative to Google Docs. Your docs are end-to-end encrypted, which means that even if the authorities accessed Proton's servers, they wouldn't be able to see what was contained in your documents.

Proton Docs does not make you anonymous by default! If you are doing higher risk organizing, make sure to learn the limitations of Proton and how to use it safely.

HOW TO USE PROTON DOCS

1. Create a Proton account if you don't have one already — choose the free plan
2. Visit Proton Drive → Click the **New** button → Select **New Document**
3. Once your document is ready for sharing, you can click the "Share" button and either share it with other Proton accounts or enable "Create public link" to share with people who don't have a Proton account. Be careful where you share the link since it will be less secure! We recommend using a password if you're turning on "anyone with link can view" mode.

Encourage the people you're organizing with to get a Proton account and you can all move toward being more secure.

Looking for forms? Proton doesn't have a solution like Google Forms. You can try Cryptpad forms or Jotform with the end-to-end encrypted option enabled.

Don't write down anything you wouldn't want read back to you in court

Chats, docs, and notes can end up in the hands of cops.

DO: Talk through sensitive details in person, with phones put away

DO NOT: Put who is risking arrest, or the details of the plan, in group chats or shared docs

We are in an era where the federal government is surveilling and prosecuting activists with a level of intensity we haven't seen in decades.

When doing mass organizing, we're always balancing the need for security with the need to grow our movements and build power.

One way we can reduce unnecessary risk is to be careful about what we write down. What we write down often ends up being used against us in court, even if we're using encrypted tools like Signal.

For any organizing involving risking arrest (or highly targeted organizing like ICE watch or Palestine solidarity), it's important to have agreements about what folks will not write down.

How the data ends up in court:

- **Someone's phone is seized.** If anyone in a chat is arrested and police get into their phone, they can read every message and document on it.

- **A company hands over your account.** Services like Google Docs aren't end-to-end encrypted, so the company can see your documents and give them to police who get a subpoena or warrant. In 2025, Google gave ICE a graduate student's account information in response to a subpoena, without telling the student first.
- **Someone in the group is an informant or undercover cop.** In the 2026 federal case against the Minnesota 15, undercover agents joined activists' Signal group chats and passed along what they read, which prosecutors then used in court.

HOW TO KEEP YOUR PLANS OUT OF THE WRITTEN RECORD

Avoid putting riskier things in writing in messages, documents, or even paper notes.

Before you type/write something, ask yourself: "Would I be ok hearing this read aloud in a court case against me?" If not, save it for an in-person conversation (ideally with all phones/devices in a different room).

Things you may want to avoid writing down:

- That you are planning to do something that carries the risk of arrest (even a very mild sit-in is usually breaking a trespassing law)
- Who is participating in the group or action
- Who is leading
- For actions: the location, the tactics, identifying information about people involved
- Other groups involved
- Jokes/venting/sarcasm that could read as a serious threat/intention.

Last step: Build practices to **delete/destroy things you did write down as soon as you no longer need them**. This often gets forgotten, so building in accountability systems can help.

Treat large or open groups as if an informant is in them. You usually can't tell who is an informant. And it's bad practice to start trying to "find the snitch" in a group. The more people in a group, the harder it is to know everyone. Keep the most sensitive conversations to small groups of people you know and trust.

☐ Pick a phone number you'll call if you're arrested. Write it on your body in sharpie.

This is the number you will call if you're arrested that can support you from the outside. This is relevant for higher risk situations.

HOW TO SELECT A PHONE NUMBER TO CALL IF YOU'RE ARRESTED

1. **Decide who to call if you're arrested:**
   - If you're not sure whether there is an active jail support hotline in your area, pick someone as your emergency contact and use their phone number. This can be a friend or trusted comrade who can help you get legal support. Make sure to get their consent in advance.
   - If you're doing a higher risk action, the organizers may have already established a specific legal hotline number for you to use.
   - If you're in a larger city, there may be a National Lawyers Guild jail support hotline that is staffed to support activists. Check out the list of NLG jail support hotline numbers here. We only recommend using a hotline if you've submitted a jail support form in advance, so they can call your contacts for you while simultaneously getting you support.
2. **Write the legal hotline number on your body in sharpie** where it can't easily be rubbed off (upper arm, leg, torso). Call that number if you're arrested and given a phone call to use.

Phone lockdown (for everyone bringing a phone)

If you are one of the people bringing a phone and have very sensitive data on your primary phone or are at high-risk of being targeted by the cops, we recommend following all of the steps in this guide using a secondary phone that will have less data on it.

- [ ] **Keep your phone (and laptop) updated to the latest operating system version**

  Protects you from hackers, spyware, and the phone hacking tools the cops use.

DO: Install updates as soon as you're prompted

DO NOT: Keep pushing the "update later" button

Every time a new operating system update comes out, it is fixing security holes. Each update you haven't installed represents a longer list of ways the cops can hack into your device. Think of it as a big building with more and more doors left unlocked.

If your operating system is not up-to-date, many of the other recommendations in this guide will not protect your data.

Start with your phone. If you're doing something higher risk, make sure to update all your devices.

HOW TO RUN UPDATES

Because security updates are so important, **we designed a tool to walk you through the process**.

Check your phone and computer updates →

HOW TO RUN UPDATES MANUALLY

If you prefer to run updates manually, here is how to do it for each device:

Click to show the manual steps

Set your phone passcode to 8 to 10 random digits

It takes years for cops to crack an 8-digit random passcode. They can probably guess your current passcode in less than 5 minutes with automated tools.

DO: Use a random passcode generator to create an 8 to 10-digit code

DO NOT: Use any passcode you thought of yourself (dates, patterns on the keyboard, etc.). Do not use 6-digit passcodes if possible.

HOW TO CHANGE YOUR PASSCODE

1. Generate a random 8 to 10-digit passcode using this random passcode generator. (Don't make one up yourself—humans are bad at choosing randomly!)
2. Change your passcode:

   IPHONE

   Settings → **Face ID & Passcode** → **Change Passcode** → **Passcode Options** → **Custom Numeric Code**

   ANDROID

   Settings → **Security** → **Screen Lock** → Enter Current Lock → **PIN/Password** → Enter a Passcode
3. **Practice the new passcode** at least 10 times in a row right now so you are more likely to remember it. (Disabling biometrics will force a passcode request every time you lock the phone.)
4. Write your new passcode on paper and keep it somewhere safe at home until you've memorized it. Then destroy it after 2–3 weeks. Setting a reminder on your phone can help.

How long does it take to crack a passcode?

TYPE	TIME IT TAKES TO CRACK (AVERAGE)	EXAMPLE
6-digit *easy-to-guess* pattern	**Less than 24 hours** to crack	*333666 (common pattern)* or *110585 (date pattern for Nov 5, 1982)*
6-digit *random* code	**200 days** to crack	*238253*
8-digit *random* code	**40+ years** to crack	*34780026*

Note: These times only apply to phones. Computers can be cracked much more quickly, and need much stronger passwords.

Sources: The estimates in the table above assume real-world observed attempts/second from police forensic hacking tools. If you need more security, use a 10-digit passcode, which will protect you even under the highest-possible cracking scenarios. See the sources linked in the passcode FAQ here.

Disable face/fingerprint unlock (biometric)

You have stronger legal standing with a passcode than with biometric unlock. Cops can try to force you to unlock with biometrics.

HOW TO DISABLE FACE/FINGERPRINT UNLOCK

IPHONE

Settings → **Face ID & Passcode** → Disable **Use Face ID for iPhone Unlock**

(You can leave the rest enabled.)

ANDROID

Settings → **Lock Screen** (or **Security**) → **Biometrics and Security** → **Disable both Face Recognition and Fingerprint Unlock** for unlocking your phone

Caveat: Face and fingerprint unlock let you use stronger passwords without typing them all the time. If you have to choose, it's better to have a longer passcode than to turn off face/fingerprint unlock. If you leave biometrics on, make sure you know how to quickly turn them off if you're heading into a high-risk situation (see tips below).

Fully powering off your phone is the best way to temporarily disable biometrics because it also encrypts your data. The next unlock will require your passcode.

iPhone locking tip: If you leave face/fingerprint unlock on, you can force your passcode to be used for the next unlock by **pressing the side button 5 times**.

iPhone camera tip: You can take photos without unlocking your phone by **swiping left** on your home screen. (In case you get arrested while filming.)

Android camera tip: On many Android phones, you can launch the camera without unlocking by **pressing the side/power button twice**.

Leave Signal groups that might put others at risk

This helps protect your network if your phone is confiscated.

If your phone is confiscated by law enforcement, one of the biggest risks is exposing your entire network. Even if people aren't using their real name on their Signal account, there is still a unique ID behind every Signal username. And the cops can use this to correlate someone's identity across many seized devices.

You need to both leave AND delete the group:

- If you only leave the group, old messages stay on your phone as well as the history of who was in the group.
- If you only delete the group, new messages will still come through and the thread re-appears.

HOW TO LEAVE AND DELETE A SIGNAL GROUP

1. **Make a plan to re-join afterwards:** When headed into a situation with possible arrest, make a list on paper at home or somewhere safe of all the groups and who you need to message who can re-add you after the action or border-crossing is complete.
2. **To leave the group:** Signal → [Group] → Tap the group icon at the top → **Leave group**
   - If you're the only admin, you have to either remove all members or assign another admin.
3. **To delete the group from your phone:** Signal → Main screen → Swipe left on the thread → **Delete**
   - This won't delete it for anyone else.

Security hygiene tips:

- Set a recurring reminder to clean up your Signal thread every 3 months.
- Make sure you take note of which groups you are leaving and who you can ask to re-add you after the action.

Note: If you find this process very annoying and cumbersome (because it is!), that's another good reason to use a secondary phone for actions. That phone would only ever be in the one or two groups needed to pull off the action that day.

During the action (if you brought a phone)

Important Fully power off your phone if your risk of arrest is going up

Your data is most protected when your phone is off (not just locked)

When your phone is fully powered off, it's more secure against data extraction by the cops. The data is encrypted until after you enter your passcode for the first time.

Therefore, the number one thing you can do to protect your data is turn your phone off as soon as you think your risk of arrest is going up.

HOW TO POWER OFF YOUR PHONE

1. IPHONE
   Press the screen lock button on the side **5 times** to quickly bring up the **Power off** option

   ANDROID
   Press and hold the power button until the power menu appears → tap **Power off**
2. **Practice** this a number of times so you can do it quickly.
3. During the high-risk situation, **remind people near you** to power off their phones as well.

Trade-offs: We recognize there are trade-offs in turning off your phone. Sometimes it is more important to film the police or coordinate with our allies. Think through what is the priority for you. If you need to film, consider bringing a secondary phone so you have less sensitive data on it.

Hand your phone to someone not risking arrest

Not having your phone on you when you are detained is the best way to protect your data and the movement. Powering it fully off is the second best approach.

HOW TO HAND YOUR PHONE TO SOMEONE NOT RISKING ARREST

- **If you're planning to risk arrest**: turn off your phone and hand it to your designated support person before deployment.
- **If you need a phone during the action**: Folks in a support role (tactical, medic, de-escalation, etc) may need a phone during the action. Depending on the action design, and the unpredictability of the cops, they may or may not be able to leave when arrest risk goes up.
  - If your action design allows it and you need your phone up until the last minute, hand it off.
  - If you need your phone and you can't hand it off, make sure you fully power it off before arrest.

After the action

After the action, delete the planning docs and Signal groups

Old chats and docs can still be read if a phone is seized or an account is subpoenaed later.

Once the action is over, the documents and chats you made are no longer needed. The longer they stick around, the more chances that they can end up in the hands of the cops through a seized phone, a subpoena, or an informant in the group.

Before the action, agree on a cleanup plan. Create an accountability system to help you follow through.

> **If anyone was arrested or charged, check with your legal support team or a lawyer before deleting anything.** Deleting records once you know about an investigation, subpoena, or charges can be treated as destroying evidence, which is a separate crime. This is another reason to turn on disappearing messages with a short timer before the action, so most messages are already gone.

HOW TO CLEAN UP AFTER AN ACTION

1. **Delete the documents.** This includes planning docs, Proton/CryptPad docs, spreadsheets, jail support forms, and any written notes. Then empty the trash.
2. **Shut down the Signal groups**: Signal groups can be useful for ongoing organizing but the list of members also presents a risk to everyone if anyone's phone gets seized in the future. Consider moving everyone into a bigger announcement-only group for ongoing organizing rather than keeping that one small group going.
   - Post a message letting everyone know the group is closing, and ask them to delete the chat from their phones. Remove each member yourself to make sure it happens.
   - Delete the chat from your own phone: Signal → Main screen → Swipe left on the thread → **Delete**. (This won't remove the group from other people's phones, just yours. Disappearing messages will auto-delete from everyone's phones, though.)
3. **If you're not an admin,** leave AND delete the group and encourage everyone else to do the same.
4. **Shred any paper notes**, maps, or lists.

Learn More

- CLDC - Expect the Unexpected: Secure Your Phone Against Confiscation or Loss (2021)
- Freedom of the Press Foundation - What to do if your phone is seized by the police (2016)

Keep learning with these related guides

Safety checklist for action organizers

Physical, digital, and legal safety for organizers.

Host a security party

A template agenda for getting your group through the checklists together.

Prepare for a protest

Digital security for anyone attending a protest.