Prepare for a Protest

ACTIVIST CHECKLIST

Last updated on **March 18, 2026** Takes about **30 minutes**

This copy was made on November 6, 2026. We update our guides often as threats change and as better ways to protect yourself become available. For the latest version, visit **activistchecklist.org/protest/**

When cops access one person's phone at a protest, they can map the whole network: contacts, Signal threads, location history. This guide protects you and the people you organize with. Before you go: power off if you can, set a strong passcode, disable biometric unlock, enable Signal disappearing messages, and hide notification previews. Organizers and people more likely to be targeted should go further.

When police access one person's phone, they can map entire activist networks (your contacts, your Signal chats, your location history, and more). The steps here are designed to help protect not just you, but the networks connected to you.

Who this checklist is for: Anyone attending protests, higher-risk protests, demonstrations, or events where police presence is expected. We have a separate guide for ICE watch digital security[1].

Planning to risk arrest? If you're taking part in a planned arrestable action (like a sit-in or blockade), follow our arrestable action digital security guide[2] instead. It covers phone agreements for your crew and handing your phone to a support person before you go in.

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).

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.

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 texts and calls to gather info about protest plans and participants
- **Location tracking** - Your phone constantly broadcasts signals that can reveal your location and prove you were at a protest
- **Mapping activist networks** - By getting data from one person's phone, police can identify entire communities of activists and organizers connected to them

There are many more, but these are a few of the top ones.

Do you need your phone?

The most secure phone is no phone at all.

If you can manage it, **just don't bring your phone at all**. This is the most secure option for your data and privacy.

That said, we often need to communicate during actions. If you can invest the time and money, a secondary phone[3] is the best middle-ground, because it has the least data on it.

We know that getting a secondary phone won't work for everyone. If you need to bring your primary phone, the list below will help make your phone more secure.

Baseline phone protections

EVERYONE This section is for anyone attending a low-risk protest (No Kings, etc.). Event coordinators and higher risk participants should also do the sections below.

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[3] so you have less sensitive data on it.

Disable Location Services system-wide before doing higher-risk activities

Important for higher-risk activities like protests or ICE watch.

DO: Disable location services on your entire phone while doing higher-risk work

Apps on your phone collect your precise location and sell it to data brokers. Cops buy this data without a warrant, using tools like Webloc[4] to see which phones were in an area, including at a protest. Location history saved by Google or Apple can also be subpoenaed.

Disabling location services on your whole phone stops apps from collecting your GPS location, so it can't be sold to data brokers or accessed by Google/Apple.

Disabling location services does not hide your location from your cell carrier. Whenever your phone is on and has cell service, your carrier can tell roughly where you are from the towers you connect to, and cops can get that data. From most to least protective:

1. Leave your phone at home.
2. Turn your phone off. A Faraday bag adds even more protection.
3. Turn on airplane mode **and** disable location services.
4. Disable location services only.

Airplane mode alone doesn't turn off GPS. Apps can still record your location and upload it once you reconnect.

HOW TO DISABLE LOCATION SERVICES

IPHONE

Settings → Privacy & Security → Disable Location Services

(Quicker shortcut: Say to Siri "Disable location tracking")

ANDROID

Settings → Location → Disable Use Location

Other tips:

- You might want to **print maps** or **save offline maps** for navigation.
- If you have any smartwatches or bluetooth "lost my keys/wallet" trackers, make sure to leave them at home or disable tracking there as well.

Revoke location permissions from individual apps that don't need it (which is most of them)

Protect yourself from apps with location access giving the government or data brokers a detailed log of your movements

DO: Turn off location tracking for most apps

DO NOT: Let every app know where you are

HOW TO REVIEW LOCATION PERMISSIONS ON IPHONE

1. Go to **Settings → Privacy & Security → Location Services**
2. Review each app and set to one of these options:
   - **Never: Best choice for most apps**
   - Ask Next Time Or When I Share: Good for apps you rarely need location for
   - While Using the App: Only for essential navigation apps
   - Always: Almost no app should have this permission
3. Make sure to set the **Camera** app to "**Never**" so you don't risk revealing your location when you share or upload photos.
4. Go to the app labeled **System Services → Disable Significant Locations**

HOW TO REVIEW LOCATION PERMISSIONS ON ANDROID

1. Go to **Settings** → **Privacy** → **Permission manager** → **Location**
2. Review each app and set to one of these options:
   - **Don't allow: Best choice for most apps**
   - Ask every time: Good for apps you rarely need location for
   - Allow only while using the app: Only for essential navigation apps
   - Allow all the time: Almost no app should have this permission

It is especially important to disable location tracking for your camera/photos app

These apps might genuinely need location while in use:

- Navigation (Apple Maps, Magic Earth, CoMaps)
- Ride-sharing (but only while actively using)

Some apps might need temporary permission:

- Food delivery apps only need location when you're actually ordering

Apps that definitely do NOT need location access:

- Photo apps
- Social media apps
- Games
- Most shopping apps
- Banking apps
- News apps
- Most productivity apps

Remember: Every app with location access is a potential privacy leak. When in doubt, disable location and only re-enable if you find you actually need it.

Disable face/fingerprint unlock (biometric)

You have stronger legal standing[5] 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**.

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

iPhone

1. **Verify your device is still supported:** Check if your iPhone is still supported[6]
2. **Operating System:** Settings → **General** → **Software Update**
3. **Apps** are set to update automatically by default. To check, go to **Settings** → **Apps** → **App Store** and make sure **App Updates** is on.

Mac

1. **Verify your device is still supported:** Check if your Mac is still supported[6]
2. **Operating System:** Apple menu → **System Settings** → **General** → **Software Update**
3. **Apps installed via the Mac App Store:** These apps are set to update automatically by default. To check, open the **App Store**, go to **App Store** → **Settings**, and make sure **Automatic Updates** is on.
4. **Other apps:** Check for updates by going to top menu bar → Click on the app name → Click either **Check for updates** or **About** [APP NAME], or look inside **Settings...**. If you don't see an option to update, it may be set to automatically update in the background.

Android

1. **Verify your device is still supported:** Check if your Android is still supported[6]
2. **Operating System:** Settings → **System** → **System Update** (may vary by manufacturer)
3. **Apps** from the Google Play Store are set to update automatically by default. To check, open the **Play Store**, tap your profile icon, then go to **Settings** → **Network preferences** → **Auto-update apps**.

Windows

1. **Update your system:** Start → **Settings** → **Update & Security** → **Windows Update**
2. **Verify your device is still supported:** Check if your Windows machine is still supported[6]
3. **Microsoft Store apps:** Make sure you enable automatic updates[7] (on by default).
4. **Other apps:** Look for updates in menu bar → **Help** → **Check for Updates**, or search for **Updates** or **About** in the app's settings.

☐ 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[8] (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[9] 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[10] for detailed instructions on configuring Signal to be as secure as possible.

Disable previews in Signal notifications

If your phone is confiscated (and still on), the cops can read the messages on your home screen without unlocking it.

HOW TO DISABLE SIGNAL NOTIFICATION PREVIEWS

Open Signal → Tap your profile picture → **Settings** → **Notifications** → **Notification Content** → Select **No Name or Content**

Keep your phone in airplane mode whenever possible at a protest

Protect your location data by disabling wireless connections. This keeps your protest activities private and secure.

Airplane mode will not disable the GPS location tracking. You must disable location services.

If you're bringing your phone, you may need it to communicate. Be mindful that anytime you have cell service, your location can be approximated based on the cell towers you're connected to.

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[11] 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[11]. (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[11].

Enhanced phone protections

MEDIUM-THREAT **This section is for you if:**

→ **You're an organizer or leader** in social movement spaces.

→ **You're likely to be targeted** by the cops based on identities you hold (race, sexuality, documentation status, etc.).

→ **You have close connections** to many at-risk individuals.

If you're at a higher risk, we recommend setting up a secondary phone[3] for protests and activism if you can. Doing so will protect you and your network much more than is possible when using your primary phone.

- [ ] **Set Signal disappearing messages to 5-15 minutes on all active threads during the protest/action**

  Your disappearing messages will expire even if your phone is confiscated (but only if you've read them).

  HOW TO ENABLE DISAPPEARING MESSAGES

  Open Signal → Open each thread (one at a time) → Tap the name of the contact or group → Select **Disappearing Messages** → Set timer to **5-15 minutes**.

  You can set it to a longer time after the action.

  Important: Messages only disappear after they have been READ — so new messages will stay on a confiscated phone and be accessible to cops. If you know who's been arrested, remove them from the group.

  We recommend also setting disappearing messages for all new threads by going to Open Signal → Tap your profile picture → **Settings** → **Disappearing Messages** → **1 week**.

- [ ] **Hide message preview and sender name for Signal notifications**

  If your phone is confiscated, the cops can get access to your noficiation history.

  If your phone is confiscated, there are two ways the cops can get access to your notification history:

  1. They can see the notifications on your home screen without unlocking your phone.
  2. If they use hacking tools, they can get access to the log of notifications your phone has received. (Example from the Prairieland case[12].)

  This only applies to incoming messages. And this is a risk even after the message has disappeared from Signal (if you have disappearing messages enabled).

HOW TO DISABLE SIGNAL NOTIFICATIONS

IPHONE

Open Signal → Tap your profile picture → Settings → Notifications → Notification Content → **Select "No Name or Content"**

ANDROID

Open Signal → Tap your profile picture to open Settings → Notifications → Show → **Select "No name or message"**

If you disable Signal notifications at the phone operating system level, you won't be notified about incoming Signal calls.

If you use Signal Desktop, make sure to disable notifications there as well.

FYI: If you want to clear the notification log that iOS has already stored, the only way to do that is to factory reset your phone and restore it as a new device — not from a backup, as backups include the notification history.

Follow our Signal security checklist

HOW TO SECURE SIGNAL

Complete all the steps in our Signal Checklist[10] to make Signal more secure and private.

Signal Security Checklist →

Disable Advertising ID (which can let cops track your location)

Law enforcement uses tools that rely on your advertising ID to track you

We know that ICE and other law enforcement agencies are using location tracking tools[4] that partially rely on the "advertising ID" that your phone provides. These tools are often using these to repress social movements.

Advertising IDs have also been used to pick targets for spyware[13] that gets delivered through ads.

iPhones have this feature disabled by default. On Android, it is on by default and needs to be disabled.

HOW TO DISABLE ADVERTISING ID

IPHONE

Settings → **Privacy & Security** → **Tracking** → **Disable app tracking**

By default, iPhones already have this setting disabled. But you can double-check to make sure.

ANDROID

Settings → Click the search icon and search for "ads" or "advertising" → Tap **Delete advertising ID**

This setting is different on different phones, so searching is easiest.

Disable voice assistants while your phone is locked (Siri or Google Assistant)

Protect yourself from the cops using your phone to do basic commands even when it is locked.

HOW TO DISABLE VOICE ASSISTANTS

IPHONE

Settings → **Siri** → Disable **Allow Siri When Locked**

ANDROID

Settings → **Google** → **Settings for Google apps** → **Search, Assistant & Voice** → **Google Assistant** → Disable **Lock screen**

Don't share photos/videos with identifiable faces, tattoos, etc.

Be mindful about sharing photos with people's faces visible. These can be used as evidence against them if they're arrested.

Taking photos is both risky and important. Our documentation of actions is often an essential part of sharing our story and winning people over. And we don't want to create evidence that the state can use to track and prosecute activists.

HOW TO TAKE PHOTOS WHILE PROTECTING IDENTITIES

- When possible, try not to capture faces in the first place.
- Disable automatic cloud uploads on Google Photos, iCloud Photos, etc so that you don't automatically upload photos before you've had a chance to review them and blur them.
- If you do capture a photo that has a face, use the blurring tool[14] in Signal if you're sending a photo that anywhere. Also blur unique features like tattoos or distinctive clothing.
- Be very cautious of photos you post on social media. Cops consistently monitor and search these sites to track activists.
- If you're organizing with a known group of people, discuss in advance what your agreements are for documentation and sharing.

Print directions or use offline maps

Your Google Maps history shows everywhere you've been, and the cops can get this data with a warrant.

DO: Use printed directions or Magic Earth[15] offline maps or Apple Maps offline maps

DO NOT: Use Google Maps

You can protect yourself from the "geofence warrants" that cops use to track anyone in a given area.

HOW TO USE PRIVATE NAVIGATION

- **Turn off location services** before you leave for the action/protest.
- Keep your phone in **airplane mode** as much as you can so your cell carrier also doesn't know your location.
- Use old-school **printed directions** if you can. Print these from Open Street Map[16] to keep your search more private. (Access Open Street Maps using Tor Browser[17] for even more privacy.)
- Use an app that allows private, offline mapping and directions. Magic Earth maps[15] are the best (Android and iPhone), but Apple Maps also lets you download offline maps and does a good job. Find the feature inside the app to download an area in advance, then keep your phone in airplane mode the entire time. Automatic navigation features won't work, so you will need to manually step through the directions.

Disable Bluetooth and Wi-Fi

Cops can use tracking tools[18] to identify who is in an area based on the Bluetooth and Wi-Fi signals your phone is emitting.

If you're bringing your phone, we assume you're using it to communicate and need a cell connection, and that turning on airplane mode probably won't work for you. Given that, it's best to **disable Bluetooth and Wi-Fi** to reduce tracking.

> **iPhone Warning:** Swiping down and using "**control center**" to disable Bluetooth/Wi-Fi doesn't actually turn it off. It just disconnects you from current networks, but it is still transmitting signals that can be tracked. To fully turn it off, you need to follow the instructions below.

HOW TO DISABLE BLUETOOTH AND WI-FI

IPHONE
Settings → **Bluetooth** → **Disable Bluetooth**

IPHONE
Settings → **Wi-Fi** → **Disable Wi-Fi**

ANDROID
Settings → **Bluetooth** → **Advanced** (or three-dot menu) → **Disable Bluetooth** and **turn off Bluetooth scanning**

ANDROID
Settings → **Wi-Fi** → **Advanced** (or three-dot menu) → **Disable Wi-Fi** and **turn off Scanning** or **WiFi scanning**

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[3] for actions. That phone would only ever be in the one or two groups needed to pull off the action that day.

☐ Backup your phone

In case your phone gets confiscated and you need a new one.

We recommend backing up your phone on a computer rather than the cloud for more security. The cops can get a warrant for your iCloud/Google backups, online photos, online documents, etc.

HOW TO BACKUP YOUR PHONE TO YOUR COMPUTER

For iPhone: Connect to computer via USB cable, open iTunes/Finder, select your device, click "Back Up Now" under the manual backup section, and ensure "Encrypt local backup" is selected for securing your data. (Save your password)

For Android: Connect phone to computer via USB cable, choose "File Transfer" mode when prompted, then manually copy your desired folders (DCIM, Downloads, etc.) to your computer's hard drive.

☐ Use a faraday bag to block all trackable signals from your phone

A faraday bag blocks all signals (GPS, cell, Wifi, Bluetooth, etc) coming in and out of your phone.

In theory, turning your phone off should do the same thing. While not common, there are ways[19] to hack a phone so it can connect to the network even if it is off[19]. A faraday bag provides an extra level of assurance.

A few options for where to buy faraday bags:

- Faraday bag from Mic Lock[20] ($13) - cheapest, but can leak a little signal
- Faraday bag from MOS Equipment[21] ($23)
- Faraday bag from SLNT[22] ($30)

Other protest safety tips

EVERYONE This section is for anyone doing activism or advocacy work.

☐ 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[23]. 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.

☐ Dress to blend in, consider hiding your face if you want more privacy

Cops can use facial recognition technology[24] to identify you from security camera footage. Our adversaries often use "reverse image search" tools to find you and harass you online.

HOW TO BLEND IN

- **Wear neutral clothing** that is hard to identify (avoid really distinct patterns or colors).
- **Cover tattoos** or anything identifiable that would cause you to stand out in photos/videos.
- **Wear a KN-95 mask** for both COVID safety and additional anonymity.

☐ Plan your trip with surveillance in mind

Think through the level of risk you're taking and consider the level of effort you want to put in to avoiding surveillance.

Some tracking to be mindful of:

- **Automated License Plate Readers:** These are everywhere, but especially prevalent at toll booths and bridges.
- **Surveillance cameras**[25]: Cameras exist inside and outside most businesses/stores/etc and on public transportation. Also think about consumer cameras that exist on things like smart doorbells.
- **Transit Card**: If you are taking public transit using a transit card, this creates a digital trail. Consider paying in cash or buying a single use card when traveling to a protest. (Also: Most public transit always have a lot of surveillance cameras.)
- **Credit Card**: If you use your credit card or tap to pay, you are creating a digital trail that places you at a certain location at a specific time. Consider using cash when possible to increase privacy.
- **Rideshare apps (Uber/Lyft):** Using a Ride Share App to arrive at the protest will create a clear record of your movements and location.

Learn More

Tip: Before your next action, consider running this checklist as a group session[26] with the people you're going with. It's more fun, and you'll all actually finish the steps.

- Electronic Frontier Foundation - Attending a Protest guide[5] (updated 2024)
- CLDC - Expect the Unexpected: Secure Your Phone Against Confiscation or Loss[27] (2021)
- Freedom of the Press Foundation - What to do if your phone is seized by the police[28] (2016)
- Freedom of the Press Foundation - Mobile security tips: Nine steps to prepare your phone before an action[29] (2020)
- Freedom of the Press Foundation - Your smartphone and you: A handbook to modern mobile maintenance[30] (2024)
- The Markup - How Do I Prepare My Phone for a Protest?[31] (2024)

Keep learning with these related guides

Security essentials

Core security practices every activist should follow.

Signal security

Secure your Signal messaging app for safer communications.

Travel & flight security

Digital security practices for activists traveling.

Links

1. activistchecklist.org/ice/
2. activistchecklist.org/action/
3. activistchecklist.org/secondary/
4. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
5. ssd.eff.org/module/attending-protest
6. activistchecklist.org/updates/
7. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
8. signal.org
9. signal.org/download/
10. activistchecklist.org/signal/
11. strongphrase.net/passcode
12. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
13. activistchecklist.org/spyware/
14. signal.org/blog/blur-tools/
15. magicearth.com
16. openstreetmap.org
17. activistchecklist.org/research/
18. unwall.app/www.wired.com/story/dnc-hidden-signal-hunt/
19. theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data
20. mic-lock.com/products/signal-blocking-faraday-bag
21. mosequipment.com/collections/all-products/products/mission-darkness-non-window-faraday-bag-for-phones
22. slnt.com/collections/faraday-phone-sleeves/products/faraday-bags?variant=48508947005734
23. nlg.org/chapters-2/
24. sls.eff.org/technologies/face-recognition
25. sls.eff.org/technologies/surveillance-camera-networks
26. activistchecklist.org/party/
27. cldc.org/expect-the-unexpected-secure-your-phone-against-confiscation-or-loss/
28. freedom.press/training/mobile-security-for-activists-and-journalists/
29. freedom.press/training/mobile-security-protest-preparation-tips-activists/
30. freedom.press/training/your-smartphone-and-you-handbook-modern-mobile-maintenance/
31. themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024