ICE Watch Digital Security

ACTIVIST CHECKLIST

Last updated on **February 2, 2026** Takes about **20 minutes - 2 hours**

Your phone has your Signal groups, your contacts, photos of community members, and threads with other organizers. If ICE seizes it, your whole network is exposed. This checklist protects you and the people you organize with, whether you're filming, doing rapid response, coordinating a patrol, or supporting from behind the scenes.

Who this is for: Anyone observing ICE's activities to hold them accountable: filming, foot patrols, adopt-a-corner, or rapid response. This includes ICE/DHS/CBP and any agency that is collaborating with them. (Note: accompaniment work and mutual aid work carry a different set of risks—many things in this guide may be useful in those situations, but it wasn't specifically designed for that set of needs.)

Scope: This guide is designed to help you reduce the risk of your private data being exposed to the state or right-wing actors. This includes steps to protect your identity, location, communications, organizing plans, and home address.

> **Note:** This guide does not directly address physical safety, operational security, or legal risks related to ICE observation. While you may find practices here that engage those realms, the goal of this guide is to help you manage digital risks.

Risks: ICE's primary activities center on detention and deportation. But digital infrastructure is integral to how they operate and how they attempt to surveil, repress, and punish accountability efforts. For example, we know that ICE is trying to track anyone who films them. Agents use facial recognition and social media monitoring, follow observers home, and do warrantless location tracking. The federal government has tried to build cases against activists for exercising their first-amendment rights. We also know that right-wing adversaries are infiltrating Signal threads, and doxxing activists.

But we can do a lot to protect ourselves! That may sound like a lot, but the federal government is not all-powerful (as they would like you to believe). There are a lot of steps we can take to make their digital surveillance harder, and to keep each other safe in the face of repressive tactics.

We keep us safe: Your phone doesn't just have *your* data on it. It has your Signal groups, your contacts, photos of community members, threads with other organizers, etc. If it gets seized, your organizing network could be exposed and put at risk. This guide offers steps to take to help keep you and your community safe.

Background: This guide was created in response to the ICE invasion in Minneapolis (early 2026) and was made in consultation with ICE watch organizers there and across the country.

> **Do this as a crew.** ICE watch security works best when your whole team is on the same page. Consider hosting a security party with your patrol, rapid response, or filming crew so everyone gets set up together.

Practices for all ICE observers

EVERYONE This section is for everyone engaging in accountability work around ICE activities including patrols, filming ICE, blowing whistles, accompaniment, etc.

If you only have 15–20 minutes, start with these items.

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 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 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.

Use Signal for encrypted texts and calls, especially your activism and political conversations

Normal calls and texts are not private and can be easily surveilled and turned over to law enforcement

DO: Use Signal

DO NOT: Use Facebook Messenger, Telegram, regular texts, etc. (Avoid WhatsApp if possible)

Most normal texts and calls can be observed by your cell phone provider and the government. Telegram is incredibly insecure. (See below for our thoughts on WhatsApp.)

Signal is the best option to keep your messages secure and to keep who you are talking to private.

HOW TO SET UP SIGNAL

1. Install Signal on your phone.
2. You can now message your existing contacts using their phone number (they must have Signal installed as well). If you're messaging someone new who you don't yet have trust with, you should exchange usernames instead of phone numbers when possible.
3. To start a new message: Press the "Create" icon in the top right of Signal, then type in either the person's phone number or username
4. Enable disappearing messages by default: Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → set to your desired time.
5. Follow the Signal Security Checklist to make sure you have the most security and privacy

When to use Signal

Some examples of when you would especially want to use Signal

- Discussing a protest/action that is not public
- Organizing a protest/action that is public, but the organizers want to protect their privacy
- Criticizing the government or other power-holders

Keep speaking out publicly! Moving some conversations to Signal for security isn't about going silent—it's about organizing safely while still voicing criticism of power holders openly. Do not obey in advance.

What about WhatsApp? (Avoid it if you can, use it if you must)

WhatsApp messages are secured with the encryption method developed by Signal, so the contents of your messages are secure. However, Meta harvests a lot of information about who you are talking to, how often, and what groups you're in. In 2024 alone, they turned over data for 78% of government requests. Your messages are safe, but who you are communicating with is not. It is an option to consider if the community you're working with is unlikely to move to Signal. It is safer than normal texts, Telegram, etc. If you do use WhatsApp, follow our WhatsApp security checklist to turn on Strict Account Settings and lock down your privacy settings.

- [ ] 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.

Configure Signal to be as secure and private as possible

Hide your real name, real photo, message previews, and set a username

The steps below help protect you if your device is confiscated by the cops, or an adversary (cop or right-wing) in a Signal group is trying to uncover your identity.

The list below captures the most important steps. For more detailed instructions and advanced steps, read our full Signal Security Checklist →

HOW TO CONFIGURE SIGNAL TO BE MORE SECURE AND PRIVATE

Change these Signal settings:

- [ ] **Enable disappearing messages by default:**
  Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → Set to your desired time (This will only affect threads that you start.)

- [ ] **Change your display name to not be your real name:**
  Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Click the top item with the silhouette of a person → Edit your profile display name

- [ ] **Change your profile photo to not be your face:**
  Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → **Edit photo** → upload a generic photo that you found online that doesn't relate to your identity, work, location, or interests.

- [ ] **Create a username and share that instead of your phone number:**
  Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Tap the **@** symbol → **Edit username** → set your username to something completely unrelated to your identity that you have used anywhere before. It must end in at least 2 numbers. (Tool: Random username generator). Give this username instead of your phone number to increase your privacy.
  Example: `@CarefreeMoose.22`

- [ ] **Hide message previews in notifications:**
  Open Signal → Tap your profile picture → **Settings** → **Notifications** → **Notification Content** → Select **No Name or Content**

- [ ] **Hide your phone number:**
  Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can See My Number** → Select **Nobody**

- [ ] **Enable incognito keyboard (Android-only):**
  Open Signal → Tap your profile picture → **Settings** → **Privacy** → **App security** → Enable **Incognito keyboard**

Ongoing Signal practices:

- If someone else starts a new thread (or group), it may not have disappearing messages turned on. Make sure to enable disappearing messages on that specific thread if they did not.
- Give out your Signal username instead of your real phone number.

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.

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.

☐ Fully disable face/fingerprint unlock (biometrics)

Protects you if the cops try to force you to unlock your phone.

Cops can try to force you to unlock your phone with your face/fingerprint (though this is supposed to require a warrant, but that doesn't mean that always happens).

You have stronger legal standing with a passcode than with biometric unlock.

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/fingerprint unlock can make it easier to use a strong passcode without typing it every time. If you feel you have to choose between a long passcode and disabling biometrics, we recommend a longer passcode.

iPhone locking tip: To force your passcode on the next unlock, either press the side button 5 times rapidly, or hold the side button and either volume button for a few seconds.

Test first: depending on your settings, these gestures may also start a countdown to call emergency services. You can change that.

Note: Doing this does not protect your data from phone hacking tools that cops use. The only way to do that is to fully power off your device.

Android locking tip: On most Android phones, you can temporarily disable face/fingerprint unlock by holding down the power button and tapping “Lockdown” on the menu that appears.

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: For most Android phones, you can open the camera without unlocking your phone by double-pressing the power button.

Filming securely

EVERYONE This section is for anyone filming ICE or other government agents.

The goal of filming law enforcement is two-fold:

1. **Deterrent** - We know filming won't prevent harm, but it sometimes does reduce the chance of it.
2. **Documentation/accountability** - If someone is harmed, we have the documentation to show the courts and the public.

It is completely legal and constitutionally-protected for you to film law enforcement. Check out this video training from ACLU.

Record videos without unlocking your phone (just swipe left!)

Protects your data if your phone is seized while you are filming

If your phone is confiscated while you are filming or photographing, the cops can get access to everything.

Your phone lets you take photos without unlocking first, so your data stays more secure.

HOW TO FILM WITHOUT UNLOCKING YOUR PHONE

First, make sure you have face unlock disabled. If you have it enabled, your phone might unlock automatically even if you are still on the lock screen.

IPHONE

Swipe left on the lock screen. (Or long-press on the camera icon.)

ANDROID

Swipe left on the lock screen, or double-press the power button (if enabled in **Settings** → **System** → **Gestures** → **Quickly open camera**).

Share videos of ICE encounters carefully (don't immediately post them online)

In some situations, posting can put other activists at legal risk

DO: Coordinate with your activist network before sharing/posting

DO NOT: Post online immediately after filming

Videos of interactions with law enforcement are very important in our work. And they can also create legal risk for activists or other individuals.

Before posting, consult with your activist network and/or movement-aligned lawyers.

HOW TO SHARE VIDEOS/IMAGES SECURELY

- **Consult activist community:** The people in your network are best positioned to know how to use videos in a way that protects our communities while holding adversaries accountable
- **Consult movement-aligned lawyers:** Ask your community if there are local lawyers who are aligned with your cause. If you don't know who to talk to, reach out to CLDC (rapid response hotline: 541-603-6891) or NLG.

Share videos/photos securely (via Signal, etc.)

DO: Send photos using encrypted channels: Signal or Proton Drive or OnionShare

DO NOT: Use a cloud sharing system like Google Photos or iCloud

If you share sensitive videos/photos with trusted activists or lawyers, you want to do it using secure channels. Cloud providers like Apple/Google could turn over your data to the police with a court order.

HOW TO SHARE VIDEOS SECURELY

- Signal: Sharing media via Signal is the easiest and most secure. It also automatically removes "metadata" (like location). But be aware that if your video is long, it will reduce the quality.

  Quality: Make sure to turn on "high quality" media sharing in Signal settings. Open Signal → Tap your profile picture → **Settings** → **Data and storage** → **Media quality** → **Sent media quality** → Set to **High**

- Proton Drive: You can store files up to 5GB on a free account.
- OnionShare: Best if you need to send a lot of large files. End-to-end encrypted. The person receiving it will need to use Tor Browser.

Advanced: Want to store your videos with an extra level of security/encryption? Check out Tella. Want to add extra verifiable metadata to prove you took the video at a certain time and it hasn't been tampered with? Check out Proofmode.

Consider using a "regular" camera to film instead (if possible)

Most of the digital security advice on this page relates to your phone being confiscated or surveilled.

If you can manage without your phone and are able to get a "regular" camera, that can provide even more protection.

If you have your phone entirely powered down, it is much more protected from surveillance or "phone hacking" tools that cops use.

HOW TO USE A "REGULAR CAMERA" TO FILM

Option 1: Phone not with you. The most secure approach is to not have it on you at all while filming in case you are arrested, but many of us need it.

Option 2: Phone with you but entirely off. Make sure it has a strong passcode and the latest operating system.

Cameras to consider:

- Action cam (GoPro, Akaso, Crosstour, etc)
- Body cam (BOBLOV, etc)
- Find a point-and-shoot camera
- Or just bring a secondary phone

Remove hidden photo info (location, etc.) before posting/sharing

Photos you share can reveal your location or identity if you don't remove that data first

By default, photos and videos from your phone include hidden data ("metadata") that reveals your exact GPS location, timestamp, and phone model.

If we post the photo online, this metadata can be used to track and identify you by law enforcement or right-wing adversaries.

When to keep metadata: If you're documenting misconduct or violence (by cops, right-wing actors, etc.), keep an original with metadata for potential legal use. But do remove metadata when you're sharing publicly.

HOW TO REMOVE HIDDEN INFO FROM PHOTOS BEFORE SHARING

Our recommendation: Send over Signal

Any photo/video you send over Signal automatically has all of the metadata removed.

If you are trying to share it online, you can send the photo to yourself, then re-save it from Signal and delete the original.

Other secure options

- The Image Scrubber web app will help you remove metadata, but only for images.
- ExifCleaner - Desktop app (Mac, Windows)
- ImageOptim - Mac app

Practices for frequent ICE observers

MEDIUM-THREAT This section is for anyone who is doing frequent work to hold ICE accountable. Upgrading your security is important because you are taking on more risk.

Important **Consider getting a secondary phone for ICE watch and rapid response**

Protect you and your community because there is less data revealed if your phone is confiscated

ICE watch and rapid response work comes with a higher risk of arrest. The best way to keep not just yourself, but your community safe is to have ***as little data as possible*** on the phone that gets confiscated. And the easiest way to accomplish that is to only have a secondary phone with you when doing higher-risk work.

Getting an extra phone may not be accessible to everyone, but we encourage you to ask your network for support—people often have old phones sitting around that still work.

Don't let not having a secondary phone stop you from doing this work.

What should be on a secondary phone:

- Phone numbers for anyone you may need to be in contact with (friend, family, kids, etc.)
- Signal threads for that day's work only (leave all other Signal threads, delete all DMs)
- Private map app like Magic Earth
- Photos/videos documenting ICE (delete anything not from today after you've saved it somewhere safe)
- ... And next to nothing else!

Option 1: The more-anonymous approach

HOW TO GET A MORE-ANONYMOUS SECONDARY PHONE

- Follow our in-depth secondary phone guide if you want more anonymity. This will help you if you think you might be a target for state surveillance (monitoring your phone location because your political work). This guide takes multiple hours to complete.

Option 2: The easier approach

HOW TO GET A LESS-ANONYMOUS SECONDARY PHONE

Not everyone needs the extra anonymity of Option 1 above. This easier approach is linked to your identity—the main goal is simply minimizing data on your phone so you don't put the people you organize with at risk if it's confiscated.

1. **Find a phone:** Any phone works—ask around for an old one. Have a tech-savvy friend check if it's "unlocked" (can accept any SIM card).
2. **Get service:** Buy a prepaid SIM (Tracfone, Mint Mobile) at Costco, Walmart, or a corner store. Or add a line to your existing plan.
3. **Create a new Apple/Google account:** Don't log in with your normal account—your data will sync, defeating the purpose.
4. **Leave your primary phone at home:** Only bring the secondary phone for high-risk work. Let close contacts know to reach you there for emergencies.
5. **Keep minimal data:** Don't make this your phone for all activism—if confiscated, it would still contain risky data. Only join the day-of Signal thread, skip general coordination channels, and leave threads when your shift ends.

Note: If you must bring your primary phone with you for emergencies, make sure it 1) is powered off, 2) has an up-to-date operating system, and 3) has a truly-random 8-digit passcode. Those three combined will make it hard for law enforcement to crack it.

☐ Use a privacy-focused map/navigation app (Apple Maps or Magic Earth)

Protect yourself from Google turning over your data to law enforcement

DO: Use Apple Maps (iPhone-only) or Magic Earth (free)

DO NOT: Use Google Maps

Your location history reveals a lot about your interests, friends, and political activity. It can also be used against you in court.

Your phone is always revealing your approximate location to your cell provider because it knows what cell tower you are connected to. But any app you give your exact GPS location to has much more detail.

You can protect yourself by using a mapping app that is more privacy-preserving.

Apple Maps (iPhone only) offers privacy protections that are stronger than you might expect and is much more private than Google. However, as a big tech company, it's best for everyday use rather than sensitive organizing. We recommend it because it provides live traffic and public transportation features that privacy-focused alternatives lack.

HOW TO SET UP APPLE MAPS (IPHONE ONLY)

1. Apple Maps is installed by default (you can re-install it if you removed it).
2. Go to **Settings** → **Privacy & Security** → **Location Services** → **System Services**, then disable **iPhone Analytics**, **Routing & Traffic**, and **Improve Maps**.

Magic Earth (iPhone or Android; free) offers strong privacy. It is much easier to use than our other cross-platform suggestion (CoMaps). Some features are only available in the paid version, though.

HOW TO SET UP MAGIC EARTH (IPHONE OR ANDROID)

1. Install Magic Earth (free; paid for live traffic)
2. It functions mostly like Google Maps or Apple Maps!

CoMaps (iPhone or Android; free) is less user-friendly than Magic Earth or Apple Maps, but has the strongest privacy promises. You can operate it entirely offline, which is especially helpful for activists doing sensitive work. That said, it doesn't have live traffic data or public transit routes, which makes it hard to use as your main navigation app.

Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)

Spyware is an advanced type of attack, exploiting sophisticated vulnerabilities on our devices. In response, Apple and Google have introduced an advanced security mode that offers enhanced protection against spyware.

On iPhones, it's called **Lockdown Mode** and on Android, it's called **Advanced Protection Program**. (You can also enable Advanced Protection Program on just your Google Account even if you don't have an Android phone.)

We have **no reports** of anyone getting infected with spyware who had Apple's Lockdown Mode enabled. Android's Advanced Protection is more recent and its effectiveness has yet to be tested.

Usability trade-offs: Both features come with some functionality sacrifices. See the full list of trade-offs. If you encounter issues that don't work for your needs, you can always disable the feature later.

HOW TO ENABLE LOCKDOWN MODE FOR IPHONES

IPHONE

Settings → **Privacy & Security** → **Lockdown Mode** → **Enable**

This feature is available for iOS version 16 and above.

HOW TO ENABLE ADVANCED PROTECTION ON ANDROID

ANDROID

Settings → **Security & Privacy** → under **Other Settings** tap **Advanced Protection**

Note: The location of this setting may vary between Android devices, so we recommend searching for 'Advanced Protection' in the Settings search bar.

This feature is available for Android 16 and above.

Important Remove yourself from “people search” sites using an automated service (like EasyOptOuts)

Using a tool to automatically remove yourself from all these sites saves a lot of time.

DO: Sign up for EasyOptOuts ($20/year) — or Optery Ultimate ($249/year) for more coverage

DO NOT: We don't recommend DeleteMe because it's less effective than EasyOptOuts

"People search" sites are a type of "data broker." They collect information from public and private records to form a "profile" for basically everyone. If you've ever had a phone number, used a credit card, or voted, you're probably on one of these sites.

Try it out: Search this site for your name or phone number (we use this one as the example because it returns results immediately without making you sign up). Most people are surprised how much information is readily available. Other major sites in this category include Whitepages, Spokeo, BeenVerified, and a growing number of AI-powered lookup tools.

Why pay for automatic removal services: You can do this "opt out" process manually, but it takes an incredible amount of time, and you have to re-do it every few months when the data broker sites change. It's ridiculous that we have to pay to protect our privacy, but it saves a lot of time for us to focus on our organizing.

Which automatic removal tool should I use?

- **EasyOptOuts (recommended)** - $20/year - It is among the most effective and the cheapest.
- **Optery Ultimate** - $250/year - Slightly more effective if you can afford the additional investment. They can take a copy of your ID (with ID number removed) and opt you out from sites that require an ID.
- **What about DeleteMe? -** It's the most well-known option, but it was only 27% effective at removing profiles compared to EasyOptOuts (65%) and Optery Ultimate (68%). (Source).

HOW TO REMOVE YOURSELF FROM "PEOPLE SEARCH" SITES USING EASYOPTOUTS

Time required: 5–15 minutes

1. **Sign up for EasyOptOuts** ($20/year)
2. **Enter your personal information:** Follow the prompts. It is most important to include your **current** information (address, phone number, email). If you can't find all your past addresses, that's okay.

   > **Warning:** Do NOT enter **alias names** or **burner phone numbers** that you use exclusively for activism that are already fully separated from your true identity. You wouldn't want those linked up inside this system.

3. Continue to the next checklist item to do **manual opt-outs** for the sites that EasyOptOuts can't handle.
4. Consider asking anyone who lives at your house to sign up as well. If someone finds out you live together, they could look up that person just as easily and then target you.

Timing: It can take a few days for the initial removals to complete and sometimes up to a couple of months for certain sites.

FYI: We don't get any commissions for any paid services we link to. We recommend them because they're the most effective ones we've found.

EasyOptOuts Privacy: Some people are concerned about entering all their information into a site like this. While no site is immune to data breaches, we trust this site based on their history and reputation. And the information is necessary to do removals.

Alternate tool: Kanary is a free app that searches Google for your personal info and walks you through manually removing it. It is still very time intensive and people are likely to abandon it before they finish all the removals.

☐ Opt-out of Clearview AI to make facial recognition harder for the cops

Helps make it harder for cops to criminalize you for your legal dissent

ICE is using Clearview AI to target protesters and observers. Many law enforcement agencies also use this platform to do warrantless surveillance.

You can protect yourself by opting out of Clearview AI. (FYI - ICE is investing in other facial recognition tools that you can't opt-out of.)

HOW TO OPT-OUT OF CLEARVIEW AI FACIAL RECOGNITION

Submit an opt-out form for Clearview AI - Requires sending a photo of yourself.

Frustratingly, opt-outs are only possible in states that have passed privacy laws.

Install a trusted VPN app with ad-blocking to make it harder for cops to do warrantless surveillance

A VPN makes it harder for websites to track you and prevents your internet provider from logging your traffic.

DO: Install a trusted VPN app on your device(s) and keep it on. We recommend IVPN ($6/mo).

DO NOT: Use a random VPN you find online. Nord VPN, Surfshark, ExpressVPN, etc, are popular but not as trustworthy.

Anytime you connect to the internet (phone or computer), your internet provider is revealing your approximate location to every site/app you use.

We know that law enforcement agencies are using tools to track your location using data gathered from apps you have and ads you see. Using a VPN with ad-blocking features enabled makes it much harder for them to track you. Also, a vetted VPN won't track your browsing; police can get a subpoena for your internet traffic that gets tracked by your internet provider.

A VPN helps mask your location and makes you slightly harder to identify.

A VPN with ad-blocking enabled on your phone can help prevent warrantless location tracking (through ad networks).

Check out our dedicated VPN page for more info on when a VPN is actually useful and when it is not.

A VPN doesn't make you fully anonymous. For sensitive browsing requiring higher anonymity, consider Tor Browser as a second browser alongside your everyday one.

Options: These are the VPNs we recommend for most activists (see our full list of vetted VPNs):

- **IVPN (top recommendation)**: Easy to use and renews automatically.
- **Proton VPN** has a solid free plan, but it is only for 1 device. To get ad-blocking, you need a paid plan. (If you use Proton, see our guide to using Proton safely.)

HOW TO SET UP IVPN

1. **Generate your account:** Go to IVPN and click Generate IVPN Account ($6/mo or $60/yr). Under **Standard Plan** click **Select** (choose the **Pro Plan** if you have more than 2 devices).
2. **Write down your Account ID:** Save it somewhere safe like your password manager. There is no "forgot password" option, so if you lose it, no one can recover it for you.
3. **Pay:** Select monthly or yearly, check the **Automatic renewal** box, enter your payment details, and click **Make Payment**.
   - Instead of a credit card, you can also order a voucher card for IVPN so that your identity is even more protected.
4. **Install the desktop app** (Mac, Windows) and sign in with your Account ID.
5. **Enable autoconnect:** Find IVPN in your toolbar → **Show IVPN** → ⚙️ **Gear Icon** → **Settings** → **General** and enable **Launch at login**, **Autoconnect on launch**, and **Allow background daemon to manage autoconnect**.
6. **Enable ad-blocking:** Turn on **AntiTracker** in the main IVPN app screen to block ads (which can help you keep your location private, especially on your phone).
7. **Install the mobile app** (iPhone, Android) and sign in with the same Account ID, then turn on the same settings listed above. (Autoconnect is not a setting on iPhones because it is on by default.)

We recommend keeping your VPN on at all times unless you're having trouble connecting to a site (see our list of downsides to using a VPN).

Why we no longer recommend Mullvad: Mullvad used to be the #1 most-recommended VPN by activists and at-risk populations. Their VPN technology is still the best out there, but one of their co-founders recently ruined their stellar reputation by donating hundreds of thousands of dollars to a far-right political party in Sweden. So we can't recommend them anymore.

Practices for group coordinators

HIGH-THREAT **This section is for:**

→ Anyone taking on a **coordination** role within ICE watch networks.

→ Anyone who is taking an intentionally **public-facing** role

Make sure to do all the items in the sections above as well.

☐ Use Proton Docs and Mail for activism instead of Google Docs and Gmail

Protect yourself and your community from government data demands that you don't know about.

DO: Use Proton Docs and Proton Mail

DO NOT: Use Google Docs and Gmail for activism communications

Tech companies (like Google) often receive government demands to turn over all the account data for an activist. This often includes a "gag order" which means the company can't tell the user until months or years later.

Encrypted cloud tools like Proton Mail, Drive, Docs, and Sheets ensure the company doesn't hold readable copies of your data to hand over. If the government wants it, they'd need to demand it from you—giving you notice and the opportunity to challenge it with legal support.

Limitations of encrypted email: Proton encrypts everything on their servers. But encryption only protects both ends if the recipient also uses encrypted email. If you email a Gmail user, Google has a copy they can hand over.

For sensitive communication, always use Signal with disappearing messages enabled.

HOW TO SET UP AND USE PROTON DOCS AND PROTON MAIL

Create a Proton account

Suggestion: Choose a random username and random display name. so you have the option of not revealing you share this email address.

1. **Sign up** for a free Proton account.
2. **Verify:** When asked to verify if you are a human, choose the “CAPTCHA” option rather than the “email” option, so you don't link your true identity.
3. When asked to set your phone number / email as a recovery method, choose **Maybe later.**

Use Proton Drive/Docs/Sheets

- **Create and edit** documents collaboratively much like Google Docs. Someone must have a Proton account to be shared directly.
- **Share securely:** Only use "share by link" when necessary, set a document password, set the "public link" to have an expiration date.

Use Proton Mail

- **Use Proton Mail for:** website accounts, newsletters, public-facing communications needing anonymity, and non-sensitive organizing work.
- **Don't use any email for:** truly sensitive communications that might put someone at legal risk.
- **What gets encrypted vs not:** Messages between Proton Mail users are automatically end-to-end encrypted. Messages to people using a different email provider will not be encrypted, but you can send a password-protected email.

CryptPad is another popular encrypted doc option, but it is very difficult to use. If it has features you need, it accomplishes the same result.

Using Proton safely: Proton is a big upgrade over Gmail/Google Docs, but it has real limitations you should know about. See our guide to using Proton safely for what's encrypted, what's not, and how to avoid common pitfalls.

Opt-out of "face search" sites

Protect yourself from a photo being used to find your identity.

You can protect yourself by opting out of "reverse photo search" sites. This makes it harder for someone to use your profile picture online to find out your legal name, which can lead to them finding you on the people search sites mentioned above.

HOW TO REMOVE YOURSELF FROM "FACE SEARCH" SITES

Each of these sites will (ironically) require you to upload a headshot. This is a necessary evil if you want to be removed. You have to decide if the risk of giving them more data is worth the payoff of being opted out.

> **Note about uploading your government ID**: Some of these sites are awful and require you to upload a photo of your government ID or passport with sensitive information hidden. The easiest approach is to put tape over everything on your ID except your name and photo, then take a picture.

Sites to opt-out from:

1. Opt-out of Clearview.ai - Only requires a photo, not a government ID. Frustratingly, opt-outs are only possible in states that have passed privacy laws. ***Clearview is used primarily by law enforcement agencies, so it is important to opt-out of.***
2. Opt-out of PimEyes - Requires a photo of your government ID. (Block out your ID number!)
3. Opt-out of FaceCheck.ID - Instead of uploading a government ID, you can upload a selfie you take with two fingers touching your chin. Also, you must manually select which photos you want them to remove.

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**

Enable iCloud Advanced Data Protection (iPhone) or Google Advanced Protection Program

Apple, Google, and other services offer additional security features to protect against targeted attacks on your accounts and data. These protect your online accounts with each company, not your device itself.

Apple's Advanced Data Protection enables end-to-end encryption for most of your content.

HOW TO ENABLE ADVANCED PROTECTION ON YOUR EMAIL/CLOUD ACCOUNTS

Protect your data:

- iCloud Advanced Data Protection - Enables end-to-end encryption for almost all data stored in iCloud, protecting your information against government court orders. Make sure you save the recovery key somewhere very safe (like a password manager).

Protect your account:

- Google's Advanced Protection Program - Helps protect your account from phishing and unauthorized access.
- Microsoft's Account Guard
- Proton Sentinel

Configure Signal so your phone number is not discoverable

Even though your phone number isn't visible on Signal by default, people can still type in your phone number and find you. If you're at risk of harassment, you may want to only share your Signal username with folks instead.

HOW TO MAKE YOUR PHONE NUMBER NOT DISCOVERABLE ON SIGNAL

1. **If you want to change your username:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Tap the **@** symbol → **Edit username** → set the username to something **completely unrelated** to your identity, or any usernames you've used anywhere before. It must end in at least 2 numbers.
2. **Hide your phone number:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can See My Number** → Select **Nobody**.
3. **Make your phone number not discoverable:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can Find Me By Number** → Select **Nobody**.
4. Tell people your username instead of your phone number when you want to connect with them on Signal.

Use small group chats with short disappearing message timers

A 50-person chat means 50 phones that could be seized, lost, or breached—any one of them exposes the whole conversation. While we sometimes need big Signal groups, don't run all your organizing through one big group chat. When coordinating something specific—an action, a project, a sensitive decision—spin up a small group with only the people who need to be there, and set messages to disappear quickly.

HOW TO KEEP SIGNAL GROUPS SMALL

- **Create a small group** with only the people directly involved in a process.
- **Set a short disappearing message timer** (1 hour to 1 day for active coordination; 1 week max for ongoing work). The messages only disappear after the person reads them, so you can even set it to 1 hour in some cases.
- **Delete or leave the group** when the coordination is done. Do an occasional scrub of old chats you forgot to delete. Remind others to leave and delete.

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.

☐ Scrub your private data online and social media accounts to defend against harassment/doxxing

Protect yourself from the government or right-wing trolls using publicly available data to target you.

The government uses social media tracking tools to surveil activists without a warrant. Right-wing adversaries use "people search" sites and social media to attempt to scare us into not organizing.

You can scrub your personal information to make it harder to be a target for these attacks.

HOW TO DEFEND YOURSELF AGAINST DOXXING

We have a detailed guide on how to defend yourself from doxxing and harassment like this.

Doxxing Defense Checklist →

Here are a few of the most important steps from that guide:

1. Opt-out of "people search" sites using EasyOptOuts ($20/year)
2. Lockdown your social media accounts using Block Party (free or $50/year if you use JOINTHEPARTY promo code)

Practices for higher-risk activists

HIGH-THREAT **This section is for:**

→ Immigrant activists (regardless of documentation status) or anyone whose skin color or presentation might put them at higher risk of being targeted by ICE while observing

Make sure to complete the sections above as well.

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.

Create your emergency plan if you are arrested (or feel unsafe at home)

Planning in advance can help make a stressful situation somewhat easier to navigate.

As dissent is becoming increasingly criminalized, it is useful for us to prepare for the possibility of arrest or feeling threatened at home by adversaries.

HOW TO DO EMERGENCY PLANNING

Short emergency planning

If you need the "mini-version" of that guide, here are a few questions to answer to start:

1. **Who is in your support network?** If you got arrested tonight, who would you call? Do you have their number memorized?
2. **Who will you notify if you know you're going into a higher-risk situation?** A simple Signal group works well for this.
3. **Do they have what they need?** Do they have: a list of who else to contact, your medical info, and a legal hotline number? Do they have what they need to care for your pets/kids/etc?
4. **Where would you go if you felt unsafe at home?** If you had to leave your home tonight because you felt unsafe, where would you stay? Does that person know?

Detailed emergency planning

If you have the capacity, we recommend completing our full emergency guide.

Personal Emergency Planning checklist →

Other resources

- **Starting rapid response or foot patrol group:**
  - Bay Area rapid response guide and zine
  - Minneapolis guides
  - Minneapolis lessons
  - Charlotte toolkit (Google docs link)
  - Dignity Toolkit - How to create connections among existing resources in your community
- **Safety:**
  - Risk assessments and community safety toolkits from Vision Change Win
  - Safety resources from Kala Mendoza
  - Street medic 101
  - Riot Medicine Handbook

Keep learning with these related guides

Doxxing defense

Protect yourself from doxxing and online harassment.

Emergency planning

Establish an emergency support network in case you're detained or threatened.