SURVEILLANCE SELF-DEFENSE

< < FURTHER LEARNING

Attending a Protest

Last Reviewed: May 02, 2024

For quick reference, we've created a handy guide designed to be printed, folded, and carried in your pocket (PDF download).

Now, more than ever, citizens must be able to hold those in power accountable and inspire others through the act of protest.

Protecting your electronic devices and digital assets before, during, and after a protest is vital to keeping yourself and your information safe, as well as getting your message out. Theft, damage, confiscation, or forced deletion of media can disrupt your ability to publish your experiences. At the same time, those engaging in protest may be subject to search or arrest, or have their movements and associations surveilled.

Remember that these tips are general suggestions for better data security and do not constitute legal advice or counseling. If you have specific legal concerns, seek the advice of a licensed attorney.

Before the Protest

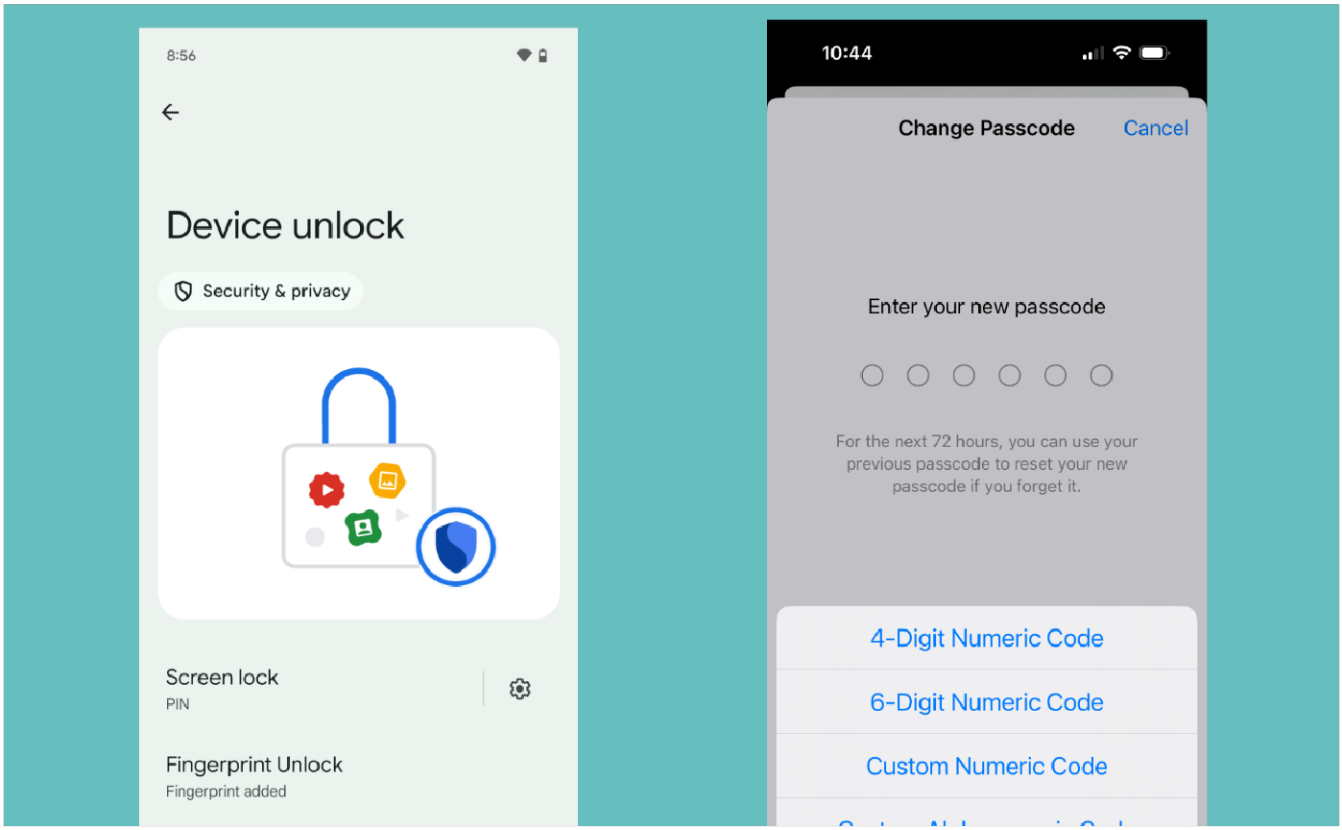
Enable Strong Encryption on Your Device

Full-disk and file-based are two types of device encryption, which ensures that the files across your entire device cannot be accessed by others. Both are forms of encryption that protects data at rest—not to be confused with "in-transit encryption," which protects data that is transferred over the internet. Full-disk and file-based encryption can help protect everything from your local database of text messages to the passwords stored in your browser. If your device is confiscated by police, or if it is lost or stolen, device encryption can help protect the data stored on your device. Protest situations can be unpredictable, so losing your phone is a distinct possibility.

iOS and most Android devices have device encryption capabilities built into them. These should be protected by a strong password: 8-12 random characters that are easy to remember and type in when you unlock your device. If devices are not protected by a strong password, the encryption may be easier to break using a brute-force attack. iPhone 5s and later and many Android devices have specialized hardware to protect against this type of attack, but bypasses for this protection continue to be developed and so a complex, strong password is still the best practice. To enable or change your passcode:

- **On Android**: Open ***Settings*** > ***Security & Privacy*** > ***Device Unlock*** > ***Screen lock*** and select the type or length of passcode you'd like to use.

- **On iPhone**: Open ***Settings*** > ***Face ID & Passcode*** > then tap "Turn Passcode On" or "Change Passcode," then tap "Passcode Options" and choose the type or length of passcode you'd like to use.



Enabling a passcode on Android (left) and iPhone (right).

Encrypting your device will likely not encrypt external storage media such as SD or flash memory cards. You have to encrypt these separately, and may not be able to encrypt them at all. You might want to investigate where files are stored on your device using a file browsing app, or remove external storage media from your device altogether.

In addition, many digital cameras lack the ability to encrypt. It is safe to assume that photos and videos taken with digital cameras will be stored unencrypted, unless explicitly stated otherwise.

Alongside what's included in this guide, it's also important to establish some solid digital security fundamentals:

- Use strong passwords (a password manager helps simplify

this) and set up two-factor authentication for your online accounts.

- Protect yourself on social networks.
- Be mindful of what you share in online groups.

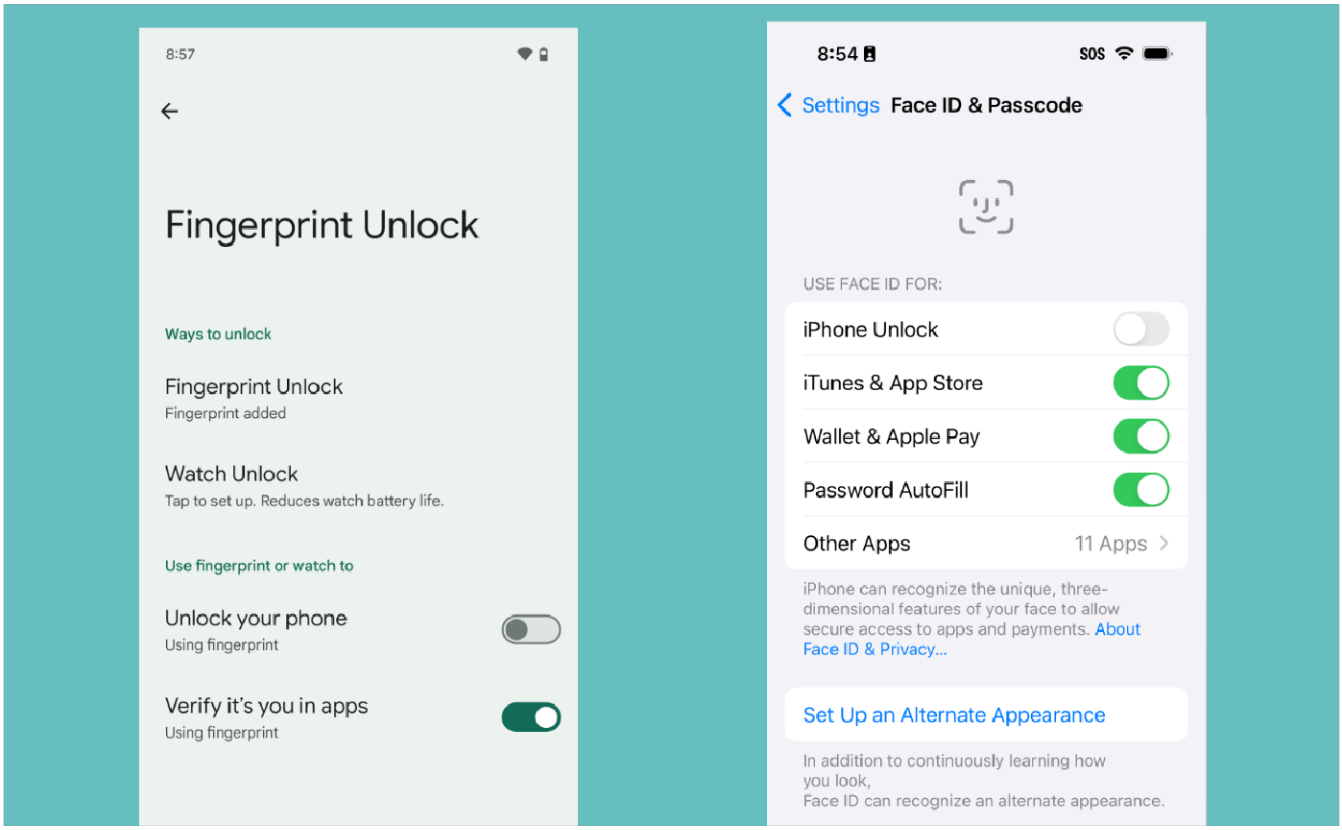
Remove Fingerprint or Face Unlock

Depending on your phone model, both iOS and Android allow users to unlock (and decrypt) their devices with their fingerprint or with face recognition. While these settings may seem appealing as convenient ways to enjoy the benefits of device encryption, enabling them means an officer could physically force you to unlock your device with your fingerprint or face. In protest situations in particular—or in any other situation in which you may be more likely to encounter a government demand to search your phone (such as at a border crossing)—we suggest you turn this functionality off.

In the United States, using a biometric—like your face scan or fingerprint—to unlock your phone may also compromise legal protections for the contents of your phone afforded to you under the Fifth Amendment privilege against compelled incrimination. Under current law—which is still in flux—using a memorized passcode generally provides a stronger legal footing to push back against a court order of compelled device unlocking/decryption. While EFF continues to fight to strengthen our legal protections against compelling people to decrypt their devices, there is currently less protection against compelled face and fingerprint unlocking than there is against compelled password disclosure.

- **On Android**: Directions for disabling biometrics will depend on your device manufacturer. For Pixel devices running Android 14, go into ***Settings*** > ***Security & Privacy*** > ***Device Unlock > Fingerprint Unlock*** and turn "Unlock your phone" off. If you have a phone by a different manufacturer, you may need to search online for specific directions for your model.

- **On iPhone**: Disable the biometric ID by going into ***Settings*** > ***Face (or Touch) ID & Passcode*** and turn "iPhone Unlock" off, or tap the "Reset Face ID" option.



Disabling the biometric phone unlocks on Android (left) and iPhone (right).

Install Signal

Signal is an app available on both iOS and Android that offers strong encryption to protect both text messages and voice calls. This type of protection is called end-to-end encryption, which secures your communications in transit. Of course, there are other communication app options, but they come with caveats. For example, WhatsApp is also end-to-end encrypted, but collects more metadata than Signal. Apple's Messages is end-to-end encrypted, but only if everyone in the chat has an iPhone. Signal is the easiest option to ensure everyone involved in the chat is set up securely by default.

In addition to encrypting one-to-one communication, Signal enables encrypted group chats. The app also allows the user to set messages to

disappear some amount of time after they are first read. In contrast to some other services like Snapchat, these ephemeral messages will never be stored on any server, and are removed from your device after disappearing.

In 2016, a grand jury in the Eastern District of Virginia issued a subpoena to Open Whisper Systems, the developers of Signal. Because of the architecture of Signal, which limits the user metadata stored on the company's servers, the only data they were able to provide was "the date and time a user registered with Signal and the last date of a user's connectivity to the Signal service." A similar situation, with the same results, happened again in 2021 (twice).

People at protests will sometimes have to make tradeoffs. You might have good reasons to send a Signal message; for example, to tell a friend what you are seeing at a protest so they can alert others or to send relevant photos and videos to friends so that if your phone is confiscated you have a way to retrieve the media later. You might also have good reasons to block adversaries from using your phone to prove you were at a protest; this requires turning off its connectivity or leaving it at home, as we explain below. Unfortunately, if you go to a protest and use your phone to communicate, even with Signal, the phone's connectivity might expose your location.

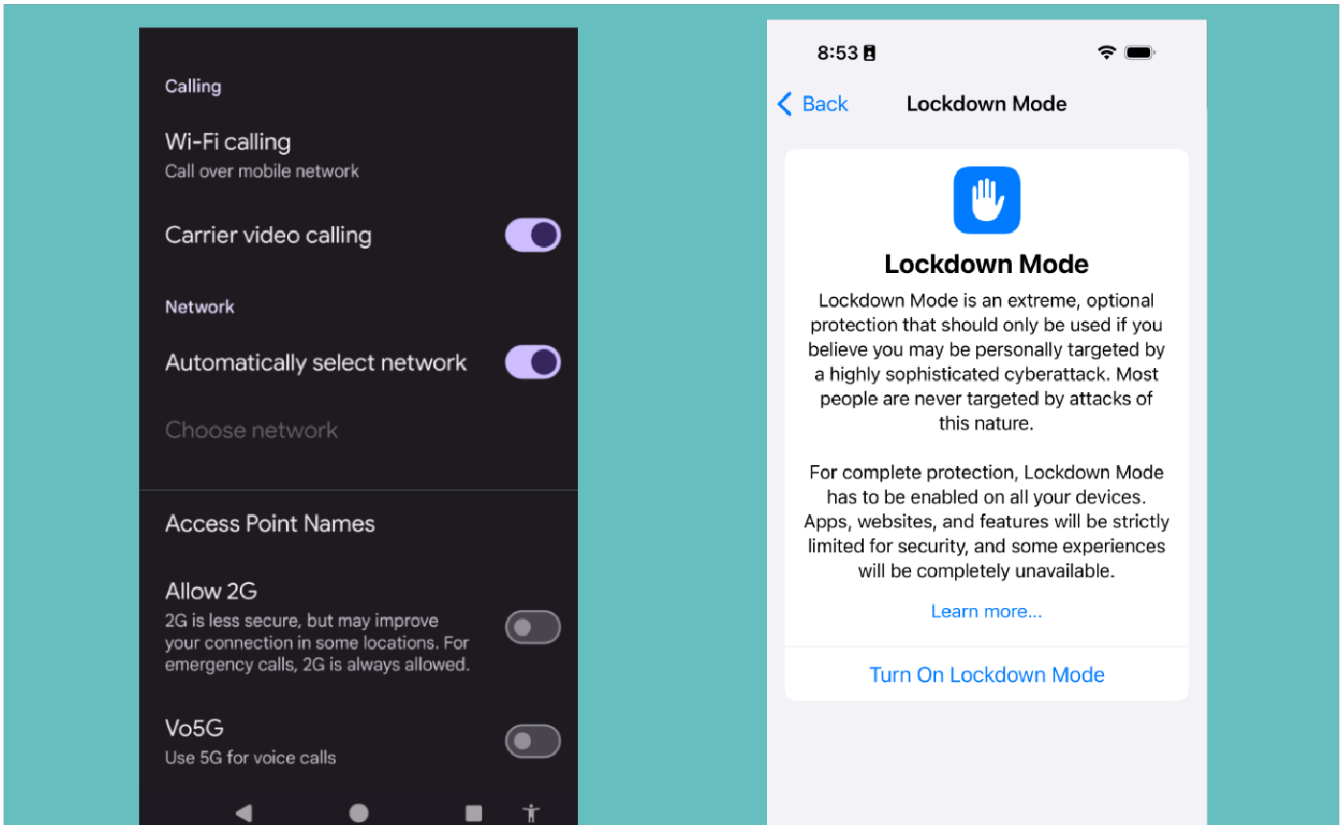
Prevent Cell-Site Simulators from Tracking Your Phone

Cell-site simulators (CSS)—also known as IMSI Catchers and Stingrays—are a tool that law enforcement and governments use to track the location of phones, intercept or disrupt communications, spy on foreign governments, or even install malware. CSS can also be used to send spam and engage in fraud. A common tactic with CSS is to trick your phone into connecting to a fake 2G cell tower. To prevent your phone from automatically connecting to a CSS, you can disable 2G on your phone.

- **On Android**: Depending on which version of the operating system you're running, the manufacturer of your phone, and your carrier, you

may be able to disable 2G, require encrypted cell connections, or both. Open up ***Settings*** > ***Network & Internet*** > ***SIMs*** > ***[Your carrier name]***, find the "Allow 2G" option, and turn it off to disable 2G entirely. You may also see an option on the SIMs page to "Require Encryption." If you see this option, turn it on to prevent your phone from using a "null cipher" when connecting to a cell tower. Since most U.S. cellular companies do not have 2G networks anymore, you can consider leaving these settings as-is even after the protest.

- **On iPhone**: You'll need to enable "Lockdown Mode," a special mode on your phone that locks down several features for people concerned about being attacked by mercenary spyware or nation level state attacks. It also, as of iOS 17, disables 2G. Lockdown Mode will disable a number of features on your iPhone after you enable it, including the ability to send and receive certain types of message attachments (like sharing your location), and blocking incoming FaceTime calls unless you have called that contact in the past. You can read more about what will be disabled on your phone here. To enable Lockdown Mode, open ***Settings*** > ***Privacy & Security*** > ***Lockdown Mode*** and tap the "Turn on Lockdown Mode" option. You can always reverse this decision later when you're back home from the protest by following the same directions and choosing "Turn off Lockdown Mode."



Disabling 2G on Android (left) and enabling Lockdown Mode on iPhone (right).

Back Up Your Data

Take precautions to limit the potential costs of losing access to your device, whether it's lost, stolen, or confiscated by law enforcement. Back up your data regularly and store that backup in a safe place to save yourself from a headache later on. If you're storing your iPhone's backups online, we strongly suggest enabling the optional Advanced Data Protection feature, which turns on end-to-end encryption for most of the data stored in iCloud. For Android, we suggest choosing an online backup service which provides (so-called) "zero knowledge," keeping your data safe from even the backup service itself (note that some services use different names for this feature).

Buy a Prepaid, Disposable Phone

In the United States, federal regulation does not require you to show your ID to purchase a prepaid SIM card (but your state might). Most countries require you to provide a form of ID to purchase a prepaid SIM card, thus linking the card to your identity and removing the possibility of anonymity.

If you're concerned about protecting the data stored on your device, don't bring it to the protest. Instead, purchase a prepaid mobile phone. These devices can be purchased along with a SIM card at most large retail stores. Let your friends know your temporary number, and use this to coordinate activities.

Remember that the location of mobile devices can be determined by the cell towers they connect to. So, if you don't want your identity and location known, turn off your prepaid device before going home or anywhere that might reveal your identity. As we explain below, you might also toggle the settings on your prepaid phone to end connectivity and thus block location tracking.

When you're done with the phone, it can be safely recycled or discarded from a location that is not linked to you. Keep in mind that if you carry both your regular device and a prepaid one with you, the location of these devices can be correlated and compromise your anonymity.

Dress for Anonymity and Safety

Many law enforcement agencies have access to sophisticated surveillance technology that can be used to identify people attending a protest. To protect yourself, it's important to dress in ways that preserve your anonymity and protect your physical safety.

Wearing the same clothing as everyone in your group can help hide your identity during the protest and keep you from being identified and tracked afterwards. Dressing in dark, monochrome colors will help you blend into a crowd. Be aware that you may not be as visible to cars in the dark, and should take extra precaution when crossing streets or walking near moving vehicles.

If you have visible tattoos or bright unconventional hair colors, cover them up. Tattoos can be used to identify you later, and may be added to databases for tattoo recognition. Dark monochrome hats, scarves, gloves, long sleeves, and full-length clothing will help cover these identifying features so you blend more easily into a crowd.

During the Protest

Take Photos and Videos without Unlocking Your Device

Catching that perfect image is something you want to be ready for, and powerful images can help support your cause. If you have a digital camera, even a cheap point-and-shoot, that might be the best option for capturing photos easily. But your phone works too. If you've chosen a strong password, entering it into the device takes precious time, and you risk the moment passing before you're able to take the picture. Luckily, iOS and Android allow you to take photos and videos without unlocking your device.

- With Android Pixel devices, double-press the power button.

- From the iPhone lock screen, firmly press on the camera icon. Older iPhone models require you to swipe up.

Be Mindful of Other Protesters in Your Photos and Videos

If you are taking photos or videos of people at the protest, be mindful of what you post. If you post photos online where protesters or bystanders' faces are identifiable, law enforcement or vigilantes might track them down and arrest or harass them. Obscure the faces of anyone in the image. There are a handful of ways to do this:

- You can edit photos in the default Android or iOS photo editing apps. Be sure to block out or blur other identifying features such as tattoos or unique clothing (blurring can sometimes be reversed so blocking out is better if you have the option).
- If you're using Signal, the app has a blurring tool built into it. You can create a message conversation with yourself (the app refers to this as a "Note to Self") to easily save the image to your phone for sharing.
- Image Scrubber is an online tool that can be used on either mobile or desktop devices to blur or block out a face.

Scrub Metadata on Photos

Once you are ready to post your photos, it's a good idea to scrub the metadata contained in the image files so you don't leak personally identifying information. Metadata on photos can include information such as the model of camera the photo was taken on, the exact time and location where the photo was taken, and even your name. You have a few approaches to handling this:

- Remove any original photo metadata by transferring the photo onto a desktop computer, taking a screenshot of the image, and posting the screenshot instead of the original photo.
- You can also take a screenshot of the photo on your mobile device to remove the metadata, but the image quality may not be as high. You can then post that screenshot instead of the original photo.
- Send yourself a copy of the photo in the Signal app (which strips metadata when sending images), then download the sent image for posting.

Things to be aware of while traveling to and from the protest

Driving Considerations

Automated License Plate Reader Systems (ALPRs) automatically record the license plates of cars driving through an area, along with the exact time, date, and location they were encountered. This technology is often used by law enforcement in the United States and many other countries, or employed by private companies such as Vigilant and MVTrac who then share license plate data with law enforcement and other entities. Amassed in huge databases, this data is generally retained for lengthy periods of time. Essentially, your location can be tracked over time based on the driving history of any car registered to you, with very few legal limits in place as to how this data can be collected, accessed, shared, and retained.

Public Transit Considerations

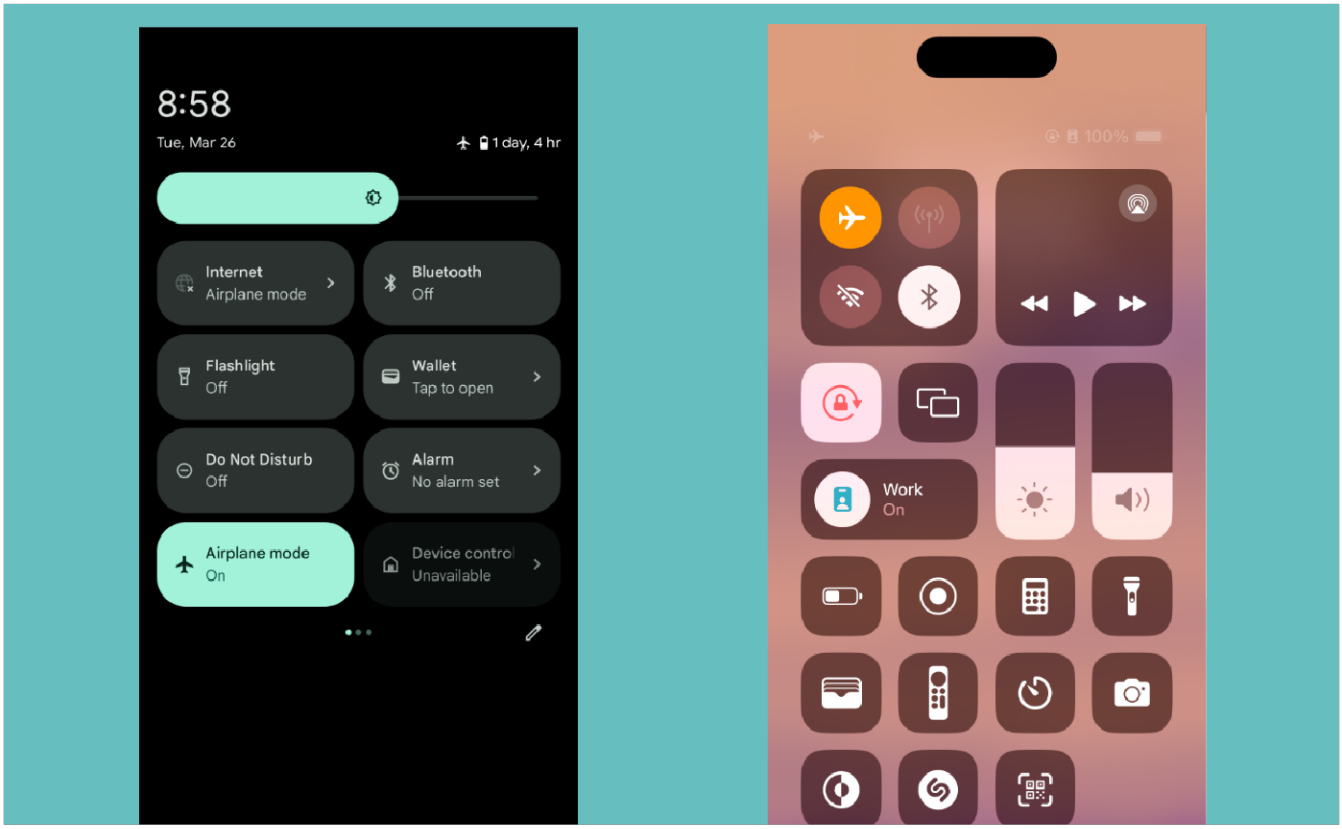
Be careful when traveling to and from the protest location on public transportation. If you're using payment methods or transit cards that are linked to you, law enforcement may be able to determine you attended the protest and track your movements. Consider using cash when possible, or alternative means of public transportation if you would prefer that your movements and associations remain private.

If you are able, consider biking or walking to and from the protest to minimize exposure to these types of surveillance risks.

Toggle Your Phone's Settings

To reduce the risk of somebody tracking your location through your phone, consider turning off some of its features:

- **On Android**: Pull down from the top of the screen to access the Notification Shade. Tap "Airplane Mode" to enable it, then tap "Internet" and "Disable Wi-Fi" if it wasn't already turned off. Next, tap "Bluetooth" to turn it off. Finally, head into ***Settings*** > ***Location*** and disable "Use location." Go into your Google account to make certain Location History is turned off. This should ensure that your device will not be transmitting for the duration of your time at the protest, and prevents your location from being tracked.
- **On iPhone**: Open ***Settings*** and enable "Airplane Mode." Then, tap Wi-Fi and turn it off, head back to the ***Settings***, and do the same for Bluetooth (You can also pull down from the top of the screen and do this all in Control Center, as pictured below). Head back to the Settings page one more time, scroll down to ***Privacy & Security*** > ***Location Services*** and turn location services off entirely. You may also want to go into ***Settings*** > ***Privacy & Security*** > ***Location Services*** > ***System Services*** > ***Significant Locations*** and turn this off.



Enabling Airplane mode on Android (left) and iPhone (right).

However, even when Airplane Mode is turned on and Location Services, Wi-Fi, and Bluetooth are turned off, apps may be able to store your GPS location and transmit it once you connect to the internet again. The only way to ensure this does not happen is to turn the phone off completely.

Turning on Airplane Mode and turning off Wi-Fi also means that you won't be able to message or call your friends, so plan accordingly. Before going to the protest, agree on a spot where you and your friends can meet if you get separated.

If you need to navigate using GPS, use an offline maps app like Organic Maps. You should download a map of the area of the protest beforehand.

If You Are Arrested in the United States

If you are detained and questioned by police, you have a right to remain silent, and to speak with an attorney before and during any questioning. It is best to say “I want my attorney and I choose to remain silent” and then refuse to answer questions until you have a chance to talk to a lawyer.

If you choose to answer questions, be sure to tell the truth. It can be a crime to lie to a police officer and you may find yourself in more trouble for lying to law enforcement than for whatever it was they wanted to talk to you about in the first place.

If the police ask to see your phone, tell them that you do not consent to a search of your device. Police might respond by seizing your phone and trying to search it later, but at least it will be clear that you did not give them permission to do so.

If the police ask for the password to unlock your device (or ask you to unlock it directly), you can refuse. You may suffer adverse consequences at the hands of law enforcement—from having your phone seized to being booked into custody—for refusing to provide your password or biometric key. Every arrest situation is different, however, and you will need to consider your own threat model.

After the Protest

What To Do if Your Device Is Confiscated

If your device has been confiscated, you may have legal recourse to get it back. In the United States, your attorney can file a motion for the return of your property if it is not being held as evidence in a pending case. If the police believe that evidence of a crime was found on your device, including in your photos or videos, then the police can keep it as evidence. They may also attempt to end your ownership of your device, but you can challenge such asset forfeiture in court.

You can also revoke access for some services that are logged in on your device. For instance, on X (formerly Twitter) if you go to ***Settings and privacy*** > ***Apps and devices,*** you can revoke access from devices that have permission to connect to your X account.

For other services, changing your password or passphrase may prompt the app to log out. But beware that revoking law enforcement access may expose you to the risk of being charged with obstruction of justice or the destruction of evidence. You should always speak to your attorney first before deciding how to proceed. Online services may provide logs of recent log-ins for your account. If you are worried your device is being used to access accounts without your consent, it might be useful for you to see if such logs are available and monitor them.

If law enforcement confiscates your device, they may use a "forensic" tool such as Cellebrite to try to extract data from your device, such as images, contacts, messages, and location history. This is more likely to be successful if your phone is older or unencrypted. For this reason, it's important to carry the bare minimum of data with you, and use the strongest level of encryption, when going into a risky situation like a protest.

SURVEILLANCE SELF-DEFENSE