How to secure your phone before attending a protest

Back in June of 2020, when this article was first written, people were taking to the streets to organize for justice and protest against systemic racism and police brutality. Now, nearly two years later, people are again taking to the streets, this time to protest the possibility that the Supreme Court may overturn *Roe v. Wade*, the 1973 decision that guaranteed people the right to terminate their pregnancies. There were protests across the country on Tuesday, May 3rd, 2022, when the news hit; there are bound to be more in the coming weeks.

As a result, we thought it would be a good idea to revisit this examination of how you can protect your phone data when attending a protest. Here goes:

Be aware

If you're attending or even just watching the protests, then be aware: not only is your phone a trove of information about you and the people you communicate with, but it also functions as a tracking device. That's why it's important to keep your digital footprint as small as possible – any evidence placing people at protests could be enough to get them arrested.

You should account for the fact that your phone may get lost, stolen, or broken. There's also a risk of your phone being confiscated by authorities – which means that if they're able to unlock your phone, they'll have access to data on you and people you know. It could give authorities access to information about what is being organized and who is doing the

organizing and might even give them the information necessary to shut down or prevent protests and arrest those involved.

It’s important to keep your digital footprint as small as possible
In other words, it never hurts to prepare for the worst, especially considering recent events.

The steps we’ve listed here are a basic start toward protecting your privacy before you attend a protest, but there are additional precautions you can take. Circumstances and situations vary, and none of these methods is 100 percent foolproof, but they do offer increased security for you and your info.

Data security is an ongoing issue, and we’re still learning the ways in which information is collected and sold, what kinds are gathered, who gets access to them, and what can be learned from them. While the following strategies are important if you’re participating in a protest, they are also useful if you want to be careful in your everyday technology use.

Here are some strategies you should consider.

If you can, leave your phone at home

Your phone carries a lot of information about you specifically. When you take it to different locations, it can reveal where you live, where you work, and what protests or demonstrations you’ve attended. In addition, every app you use collects a certain amount of information on you and has a detailed log of your activity. So, for example, if you use Twitter or Instagram at a protest, that activity and your social media account get tied to the protest.

Your phone carries a lot of information about you

So it’s better to just avoid carrying all of that data with you. If you can, purchase and use a burner phone instead, and only turn it on when you’re at the site of the demonstration. Download and use more secure, encrypted apps for communication rather than the default text messaging apps on the phone (we’ll share some examples later).

If you’re bringing your own phone, back up your device in case it gets confiscated and remove all personally identifiable information from the phone. You can also wipe your phone entirely (after you’ve backed up all your stuff, of course) and add the apps and information you need to it. Try to keep your phone off unless you absolutely need to use it.

Use a password rather than biometrics to secure your data

It’s a good idea to change the settings on your phone so that you can’t unlock it using your fingerprint or facial recognition. These methods make it easier for someone else to get into your phone, especially if you’re there, and law enforcement can legally force people to unlock their phones using their fingerprint or facial recognition. Instead, use a passcode, PIN, or password, which are protected under the Fifth Amendment.

Adjust your settings so that you can’t see message content in notifications when your phone is locked. At the protest, try not to unlock your phone unless you absolutely have to. If you are taking photos and videos, try to access your camera without unlocking your phone. (On an Android phone, this varies depending on your model; for example, on a Pixel, you just press the Power key twice. On an iPhone, you can open the camera from the lock screen by long pressing on the camera icon in the lower right corner or swiping to the side of your lock screen.)

Encrypt your device

It’s always a good practice to encrypt your personal information, but in the event that your phone is confiscated, stolen, or lost, you don’t want any information linking you or others to the protests to fall into the hands of authorities (or anyone else). So if you haven’t done so already, now’s a good time to secure your device and any information on it.

Now’s a good time to secure your device and any information on it
It’s a quick and easy process. If you have an Android phone, go to **Settings > Security> Advanced settings > Encryption & credentials > Encrypt phone**. (As always, this may vary somewhat, depending on the phone’s manufacturer.)

For an iPhone, as long as you’ve set a passcode up and you see the text “Data protection is enabled” at the bottom of the **Face ID & Passcode** (or **Touch ID & Passcode**) page (which you’ll find in your Settings menu), your information is secure.

Turn on airplane mode

Your phone actually gives off a lot of information about you, including where you’ve been. And not only can those signals be intercepted, but they can also be used to locate you and connect you to others. So while you’re at a demonstration, you’ll want your phone to communicate as little information about you as possible.

Keep your phone off or put it on airplane mode, which turns off cellular data and Wi-Fi by default. This stops cell carriers from knowing where you are based on what cell towers you connected to. This will also protect against any stingray attacks, which is when a device pretends to be a cell tower and collects data, including location, from phones around it. Police have been accused of using stingrays, or cell-site simulators, to collect information about phones.

Airplane mode does not disable location services, so it’s a good idea to make sure all of those services are switched off. If airplane mode interferes with your activities, then switch off cellular data, Bluetooth, location services, and Wi-Fi individually, and only switch on what you need.

Use guided access or pin your screens

Android and iOS both have features that let you access one app while effectively locking the rest of the phone, so you can use that app while keeping the device secure. This is a safer way to post to social media or take photos during a protest, and it’s helpful in the event that you need to show someone, including law enforcement, something on your phone.

The iOS feature is called Guided Access. To enable it, go to **Settings > Accessibility > Guided Access** and toggle it on. Once it’s on, you’ll see additional settings such as setting the time limits for guided access and locking your display using a passcode.

To use Guided Access, open the app you would like to use. Press the home button three times, which will lock down all the other apps on your phone. (If you want to disable any specific features of the app you’re allowing access to, you can circle them on the screen.) You may need to press **Start** in the top right corner and enter a passcode in order to switch on Guided Access. To disable Guided Access, press the home button three times, then enter your passcode and tap **End** on the top left corner of the next screen.

On Android, the process is called app pinning. Go to **Settings > Security > Advanced settings > App pinning** and toggle it on. You can set it so it will ask for your PIN before unpinning. To pin an app, swipe up (if you’re using gesture navigation)

or press the square Overview key at the bottom of your screen (if you're using button navigation) to see all your open apps. When you see the app you want to pin, long-press the app's icon at the top of its screen and select **Pin**. To unpin it, either swipe up and hold or long-press the back and Overview keys.

Use secure apps

If you're using your own phone, or even if you're using a burner phone, it's a good idea to use especially secure apps. The Electronic Frontier Foundation has a list of recommended tools to keep your phone secure, or you can try one of these.

For texting, one of the apps that's most often recommended is Signal, a secure, open-source, end-to-end encrypted messaging app that doesn't store message metadata. If you're communicating about protests and demonstrations, this is one of the safest ways to do so. For added safety, you should also take advantage of some of its more secure features by adjusting your privacy settings to, for example, set up a PIN or use call relays. It also has a handy disappearing message feature that causes every message sent in a conversation to disappear after a specific time limit.

If you're using an Android phone, you may want to use a more secure browser than Chrome. Chief among them is Tor (Android only), which protects your identity and information by bouncing your activity through a set of relays. Other security-minded browsers include Brave (Android and iOS), which is aggressively anti-advertising, and Vivaldi (Android only), which has a number of privacy-enhancing tools. If you've got an iPhone, Apple controls the security of its Safari browser pretty strictly (although there have been occasional blowups).

Finally, a search engine like DuckDuckGo won't store your search history or connect it to your IP address.

Use a VPN

In or out of a demonstration, it’s always a good idea to download and set up a VPN on your phone. A VPN hides your activity by encrypting your connection. When choosing a VPN, you may want to look for those that are headquartered outside of the United States and Europe because companies in those countries are required to submit personal data to authorities if requested. Also keep in mind that VPNs that charge a subscription fee are usually more trustworthy than free ones.

Secure your social media accounts

If you want to protect your identity and keep the history of your personal (and business) tweets, Facebook posts, and other social media history private, consider creating a separate email account that isn’t linked to any personal information. You can then use that to create separate social media accounts for protest or demonstration photos and footage.

It’s also always a good idea to have two-factor authentication set up on all of your accounts.

If you’re taking photos and videos

Try not to take any photos or videos with identifying information about others without their consent. Be mindful of objects in the photos, such as street signs and landmarks, that may give away the location if that’s something you’d want to hide. Afterward, blur out other demonstrators and scrub the photos of any metadata.

If your device is confiscated

Don’t unlock it if at all possible. (As previously mentioned, your Fifth Amendment rights are covered if it’s locked using a

PIN or password, but not if you can unlock it with a fingerprint or face image.) As soon as possible, change your passwords for any apps or accounts you have on there and disconnect your accounts from that device.

Update May 5th, 2022, 5:20PM ET: *This article was originally published on June 4th, 2020. It has been updated to be more in sync with current events and to work with more recent software versions.*

https://www.theverge.com/21276979/phone-protest-demonstration-activism-digital-how-to-security-privacy