Activists and human rights defenders are increasingly documenting their protests using cameras and mobile phones ? often to powerful effect. The following are useful tips for you to remember if you are going to a protest and are concerned about protecting your electronic devices if you?re detained by police.

Think carefully about what?s on your phone before bringing it to a protest. Your phone contains a wealth of private data, which can include your list of contacts, the people you have recently called, your text messages and email, photos and video, GPS location data, your web browsing history and passwords, and the contents of your social media accounts. Through stored passwords or active logins, access to the device can allow someone to obtain yet even more information on remote servers. (You can log out of these services).

In many countries, people are required to register their SIM cards when they purchase a mobile phone. If you take your mobile phone with you to a protest, it makes it easy for the government to figure out that you are there. If you need to keep your participation in a protest secret from governments or law enforcement, cover your face so that it is harder to identify you from photos. However, do note that masks may get you into trouble in some locations due to anti-mask laws.

**If it is important to keep your presence at the protest concealed, do not take your mobile phone with you.**

**If you absolutely must bring a mobile phone with you, try to bring one that is not registered in your name.**

To protect your rights, you may want to harden your existing phone against searches. For the full set of advice on how to manage the security of your mobile phone, go the **Mobile Phone Lesson.**

* **Passwords:** Always password-protect your phone. While password-protecting your phone is a small barrier to access, please be aware that it is not an effective barrier to expert forensic analysis.
* **Encryption:**Some phones have encryption options available ? these should be applied. If you have an Android phone this can be done in Settings -> Personal -> Security -> Encryption. The Electronic Frontier Foundation has a guide on how to encrypt iPhones.
* **Download secure apps:** Make sure you and your colleagues have downloaded apps that will allow you to communicate and operate securely. (These are explained in detail later in this lesson)
  + **For communicating**: Textsecure and RedPhone (for Androids) or Signal (for iPhones)
  + **For filming/photographing:**ObscuraCam and InformaCam
  + **For emergencies:** Panic Button (Android only)
* **Back up your data:** It?s important that you frequently back up the data stored on your phone, especially if your device lands into the hands of a police officer. You may not get your phone back for a while (if at all) and it is possible that its contents may be deleted, whether intentionally or not.
* **Keep an emergency number:** Consider writing one important, but non-incriminating phone number on your body with a permanent marker in case you lose your phone, or are in police custody but are permitted to make a call.
* **Use a throwaway:** You should also consider bringing a throwaway or alternate phone to the protest that does not contain sensitive data, which you?ve never used to log in to your communications or social media accounts, and which you would not mind losing or parting with for a while. If you have a lot of sensitive or personal information on your phone, or you need to conceal your presence at the protest, this might be the best option for you.

If you are concerned about being arrested at the protest, it?s best practice to pre-arrange a message to a trusted friend or colleague who is in a safe place. Write your text message to that person in advance and queue it up so that you can send it quickly in case of an emergency to let them know you have been arrested.

If you have an Android phone an easier way of doing this is by using an app, Panic Button, which turns your mobile phone into a secret alarm for when you're in trouble. When triggered, it sends alerts every 5 minutes with your location to your chosen contacts. This is a very useful tool to have when going to a protest where trouble could occur and we recommend you download it before you go.

Similarly, you may want to plan a pre-arranged call after the protest with a friend?if they don?t hear from you, they can assume you?ve been arrested.

In addition to being made aware that your phone has been seized and you have been arrested, that trusted friend might be able to change the passwords to your email and social media accounts in case you are coerced into giving up your passwords to the authorities.

Please note that deliberately concealing or destroying evidence may be considered an illegal act in itself in some jurisdictions (including many social democracies).

Be sure you understand the law and the risks before engaging in this plan. For instance, if you are protesting in a country with a strong tradition of the rule of law and where protesting in itself is not a crime, it may be that conspiring to lock out law enforcement from your accounts may lead to you breaking the law when previously you would be able to leave without charge.

On the other hand, if you are concerned for the physical safety of you and your colleagues at the hands of a unchecked militia, protecting your contacts? identities and your own data from them may be a greater priority than complying with an investigation.

Once you are at the protest, keep in mind that law enforcement may be monitoring communications in the area. You may wish to encrypt your messages using Textsecure (Androids) or Signal (iPhones), or encrypt your phone calls using RedPhone (Androids) or, again, Signal (iPhones). All these apps are compatible. You can read more about them in the Sending a Message or Making a Call lessons.

Please remember that even if your communications are encrypted, your metadata is not; this means your mobile phone will still give away your location and information such as whom you are talking to and for how long.

When capturing pictures or video it is important to be careful of privacy and safety of those pictured. For example, if you take photos or record video of a sensitive event, it might be dangerous to you or to those who appear in the recordings if your phone fell into the wrong hands. The Guardian Project has created an app called ObscuraCam to detect/select faces on photos and blur them. It also deletes the original photos and if you have set up a server to upload the captured media, it provides an easy way to upload it.

Metadata such as phone identity and location are also captured on photos and videos. In some instances, such information is really important to have to prove the credibility of images and video so that they could be used as evidence in courts of law. At other times metadata can put you or others at risk. The Guardian Project has made a plugin tool for ObscuraCam called InformaCam that allows you to store a version of the image/video with metadata while also creating a redacted version without any sensitive data that can safely be shared on social media.

Swipe right for this lesson?s checklist

Go to the Beginner lesson for advice on covering a protest as a journalist.

### RELATED LESSONS/TOOLS

* [Mobile Phone Lesson](umbrella://lesson/mobile-phones)
* [Sending a Message Lesson](umbrella://lesson/sending-a-message)
* [Making a Call Lesson](umbrella://lesson/making-a-call)

### FURTHER READING

* EFF ? Attending protests