Digital Security Guidelines for Protests

Engaging in protest can unfortunately result in the theft, destruction, or search and seizure of your mobile devices by malicious actors or law enforcement. Digital exposure of your movements, contacts, and associations can lead to surveillance, prosecution, and repression of civic space for yourself and the communities you work with. Before heading to a protest, consider the potential risks of data, images, or video from your personal devices getting into the hands of the authorities or other malicious actors. Will it put you, members of your community, or other protesters at risk of arrest or other problems?

If so, you can mitigate risks by following the guidelines below for steps to take before, during, and after a protest.

> *Please Note: these steps are NOT legal advice. They are meant for securing mobile devices that you feel are essential for you to bring to a protest. If you can safely attend without a mobile device, best practice is to leave it at home, or use a disposable "burner" phone while at a protest then recycle it after.*

Before a Protest

- Ensure That Your Mobile Device is Encrypted. Encryption makes it much more difficult for a lost, stolen, or confiscated phone to reveal your communication history or data on your device. Any newer iPhone or Android should come with device encryption by default.
- Remove Fingerprint Lock and FaceID and ensure your devices are protected with a strong PIN, password, or passphrase. While biometric features may be convenient, they do not provide the same legal protection as a memorized password and pose the risk of enabling law enforcement or malicious actors to easily compel or coerce you to unlock your mobile device.
- **Sign out of any accounts you are logged into on your mobile device** (Email, chat and meeting platforms, etc.) **including social media accounts** that you don't need to access to. If an unlocked mobile device is stolen or compromised at a protest, all the apps you're signed in to will be accessible and can reveal your location and connections. Protect your personal and professional information by making them inaccessible.
- **Use Secure Communications Apps** that offer full end-to-end encryption if you must make calls or send a message. While apps like Teams or WhatsApp offer such encryption, you should sign out of them for the reasons above. We recommend Signal for messaging while at a protest. Signal is a free app available on both iOS and Android that offers strong encryption to protect both text and voice calls. Use the disappearing messages feature for real time communications. Unlike a phone service carrier, Signal is unable to turn over meaningful call and text records to authorities, and disappearing messages cannot be recovered.
- **Back up your data!** Confirm that all important data and media is synced somewhere other than the device you bring to a protest, so that if your phone is taken you don't lose your data with it.

During a Protest

- **Leave your device locked while taking photos and video.** Photos and videos of protests can help document and support protest efforts, but you want to be able to do so as quickly as possible, without taking time to unlock your phone and risk losing it or having the phone taken while its unlocked. iOS and Android allow you to take photos and videos without unlocking your device.
    - *At the iOS lock screen, you can firmly press on the camera icon. Older iOS devices require you to swipe.*
    - *With Android Pixel devices, double press the power button. With Samsung or some others, swipe open the camera from the lower right of the lock screen.*
- **Enable Airplane Mode** If you do not need to make calls or send messages at the protest. Airplane mode ensures that your device will not be transmitting for the duration of your time at the protest and prevents your location from being tracked. If you have a smartwatch or other IoT devices, disable Wi-Fi and Bluetooth.

After a Protest

- Be mindful when considering sharing or posting photos or video from a protest to social media, and ensure you have consent of anyone whose face is visible. Photos and video files are tagged with metadata 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.
- **If your device is confiscated:** Changing your password on any personal apps should automatically log you out of them. Online services may provide logs of recent logins 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.

Links:

- **Ensure that your mobile device is Encrypted:** https://spreadprivacy.com/how-to-encrypt-devices/
- **Remove fingerprint lock and face ID:** https://ssd.eff.org/module/attending-protest#remove-fingerprint-unlock-and-faceid
- **Signal Messenger:** https://signal.org/
- **Set and manage disappearing messages:** https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
- **How to download and use Signal:** https://ssd.eff.org/module/how-to-use-signal