



DIGITAL SECURITY GUIDE FOR PROTESTERS

DON'T BE TRACKED

Law enforcement can intercept your SMS messages and track your location when you are protesting. With new exemptions for COVID-19 contact tracing, it's easier than ever.

Bring a **burner phone** instead of your own phone.

If you must bring your real phone, keep it in **airplane mode** and in a **signal-blocking pouch** unless you need to live stream, message for coordination, or document.

If you need to use your phone, make sure **all location services are turned off**.

If you need to message others, use **Signal, Wire**, or another encrypted messaging app. WhatsApp and iMessage are encrypted, but are owned by Facebook and Apple.

If you need to take photos, use Signal. You can automatically **blur out faces** in Signal, and you should **blur landmarks** like street signs and house numbers. Signal does not save location metadata to the photos.

Be careful sharing videos and photos online, as it can allow people shown to be identified.

DON'T GIVE UP YOUR IDENTITY

Make sure your phone is **encrypted**. With iOS this is automatic; with Android it must be enabled in Settings.

Do *not* use your face or thumbprint to unlock your phone. Use a password (longer is better, at least 6 digits). Someone could force your hand or face to unlock your phone, but they can't legally force you to tell them your password.

Update your settings so notifications do not show when your phone is locked. You do not want someone seeing messages if your phone is taken.

Practice **turning your phone off quickly**, in case you need to do so.

Be safe out there.

— LA Cryptoparty + Resistant Systems

This guide was influenced by many other guides, articles, and years of work. We can't list everything here, but we highly recommend this amazing guide from Lebanon: <https://github.com/frombeirutwithlove/ProtestTips>