This is a guide for *legally* and *passively* countering commonly-used technological surveillance in the USA. It does not guarantee that the reader will evade all forms of surveillance or tracking but is a practical guide that hopes to reduce the risk of their expression of free speech being used against them.

Primary Risks:

Most common means of technological surveillance target cellphones.

- **Attribution:** Use of smartphones may result in individuals being automatically identified by social media, advertisers, and other online trackers as having participated in a protest. This can be used to target the individual or track their activity online. In some cases, this may represent as much or more of a personal threat than police surveillance.
- **Police Surveillance:** Police in many places now employ passive and active surveillance technologies to track protesters and intercept their communications. These include systems such as stingrays, femtocells, IMSI-catchers, and facial recognition.

If you have reason to believe that facial recognition is being used, then wear a mask and sun/safety glasses. Also good for COVID-19, tear gas, and rubber bullets. Cover identifying marks such as tattoos.

Simplest cellphone option:

- ✓ If you have the spare money, purchase with cash a cheap no-contract phone to use at protests. If possible, do not provide your name or address when you buy. Set a strong password for the device. Do not sign in to any personal accounts on the device. Only use it for calls/texts and recording video. For communication, use end-to-end encrypted apps like WhatsApp, Telegram, or Signal. Retrieve recorded video or audio by downloading it to your computer with a USB cable

If bringing your own cellphone:

- ✓ Use a VPN app such as ProtonVPN, NordVPN, or TorGuard. Use them even with wifi off
- ✓ Use end-to-end encrypted apps for calls and texts such as WhatsApp, Telegram, or Signal
- ✓ Google “reset advertising ID for phone” and follow the instructions
- ✓ Put your phone in airplane mode when not in use. Or, turn off location, wifi, BlueTooth, and Data when you are not using them. These can be used to track the location of your device and your movements.
- ✓ Turn off geotagging for pictures and video
- ✓ Use a password to unlock your phone. Use your phone’s features (if available) to encrypt your local files with a password
- ✓ Sign out of any apps or accounts where possible
- ✓ Unless you are livestreaming, avoid using any apps from Facebook (other than WhatsApp), Google, or other social media while protesting
- ✓ If your phone has privacy settings, consider using those that are practical
- ✓ If recording video, photos, or audio, avoid third-party apps. Download to your computer via USB