The purpose of this document is to educate the reader on the basics of cyber security in a protest context. It will explain some of the tactics used by law enforcement to identify protesters.

This document will start with things you, as a protester, can do to remain anonymous at a protest. It will then cover numerous tactics law enforcement can, and will do to conduct espionage through digital means. And of course, how to detect and avoid them.

A Protester's Guide to Staying Anonymous and Outsmarting Digital Surveillance

Part I: 🕳️ Stay Ghost: Protest Anonymity Tactics

1. Cover Your Face Smartly

- **Masks**: bandanas, balaclavas, N95s, covid masks, just hide your face.
- **Hood up, logos off**: Neutral clothing, no identifiable patterns.
- **Gloves on**: Avoid leaving fingerprints on protest signs, banners, or bottles.
- **Switch up the fit**: Don't wear the same outfit in every action. Cameras remember.
- (Facial recognition tools are able to scan a protesters face, and search for matches around the web, including social media.)

2. No Phones on the Frontline

- **Leave it at home or bring a burner**. Airplane mode ≠ stealth. Cell towers can ping your last location, no matter what mode.
- **Faraday bags**: Blocks all signals; easy to DIY with foil & a zip bag. Search for tutorials on youtube
- **Disable biometrics**: Cops can force your finger or face to unlock, but they can't force a password (legally).
- **Never text about direct action. Ever.** Use encrypted apps like Signal, and set auto delete.

3. Move in Silence

- Don’t post live, protesters faces found in social media can be used to incriminate you **AND** the people around you

- Don’t tag.

- Don’t talk about the next move on public channels.

- Assume all group chats are compromised unless vetted.

Part II: 🕳️ Law Enforcement Tactics Revealed

1. Facial recognition

- New AI facial recognition technology has become **more available** to law enforcement. It allows them to pull up matching photos found **online**, using facial geometry.

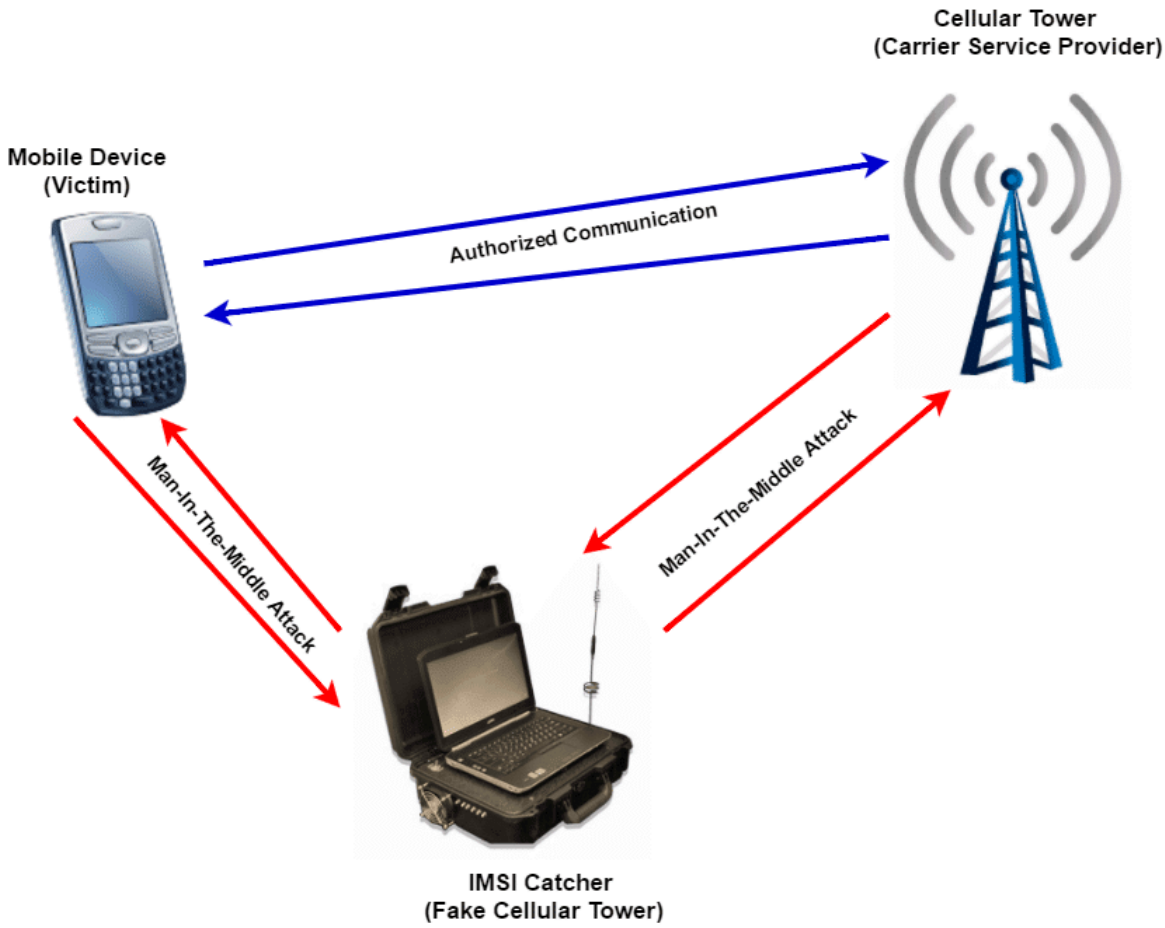
- This grants them the ability to pull data on people who are **NOT** in the system, unlike before.

- This is why it is more imperative now than ever before, to utilize **facial covering** and **refrain** from posting on social media

2. IMSI Catchers (Stingrays)

- Imsi catchers, informally known as **stingrays,** are devices that **impersonate** cell towers. This causes phones in a nearby area to connect to them.

- After connecting, police are then able to **intercept** unencrypted calls and messages from said phones. They are also able to verify the user was in a specific location at a specific time.



- These devices are commonly hidden in nearby vehicles
- One indicator that a stingray may be nearby, is a sudden drop in cell signal, due to the stingray's inability to provide as strong a signal as an actual cell tower

3. Geofencing

- Geofence warrants allow law enforcement to request location data from apps or tech companies for all devices within a specific area at a set time.
- Authorities can then track users through this, and collect additional data like social media accounts.
- However, this data is in **bulk** and **indiscriminate** typically. But it is still a valid reason to consider leaving a device altogether.