

OpenArchive's Citizen Journalist Survival Guide

Harm reduction tactics to keep you, your
media, and others safe while documenting.

BEFORE RECORDING

Countering Surveillance

DO

- Consider leaving your primary/personal phone at home and getting a phone just for documentation.
- If you bring your primary phone, delete sensitive messages from Signal.
- Join a Signal group with other people you know and trust.
 - Turn on disappearing messages, set to < 4 hours.
- Turn off biometrics (fingerprint and face unlock) on your phone & set up a 6-digit (or longer) passcode.
- Disable message previews on lock screen.
- Delete history from web browsing apps.
- Set a pin-control to access your SIM data.
- Enable airplane mode and disable GPS, or put your phone in a Faraday Bag.
- Study the route/location beforehand & find out the access points if you need to make quick escape.
- Consider deleting apps with personal info (e.g., Facebook, Twitter, LinkedIn).

DON'T

- Publicly post locations or other action details (on social media, etc.).
- Coordinate plans using unsecure messaging apps (i.e. SMS, Snapchat, Telegram, Facebook, WhatsApp, Messenger).

Why use disappearing messages? 😊

Keeping messages on your smartphone still puts you and those you communicate with at risk, even if your data is protected through end-to-end encryption,

Use WIRED's Guide to Protect Yourself from Surveillance



WHILE RECORDING

If you are a documenting events, make sure you don't expose others to mass surveillance. Thoughtless reporting can put people at risk of doxxing, arrest and violence.

Best Practices

- **Enable airplane** mode and **disable GPS** during the action.
- If you need to disable airplane mode to communicate with others, **don't connect to local wi-fi networks** as you will be easily tracked.
- Document injustice without incriminating victims:
 - **Avoid photographing faces**/other identifying marks of others;
 - Respect boundaries. If someone doesn't want to be filmed or photographed, **listen to them**;
 - **Don't tag** the location or people on social media posts.
- Do strip metadata* from the media you want to share on social media.

*EXIF metadata in media sent through Signal is automatically removed.

Keep in mind ✈️

While airplane mode can circumvent some surveillance, it doesn't make you "invisible." Your GPS can still be tracked even when airplane mode is enabled, so make sure to **disable GPS** in your phone settings.

What is EXIF metadata? 📷

EXIF (Exchangeable Image File Format) data contains information about your phone/camera, as well as where and when the photo or video was taken.

Why metadata matters



Surveillance Self-Defense guide

[Electronic Frontier Foundation](#)



Metadata Guide

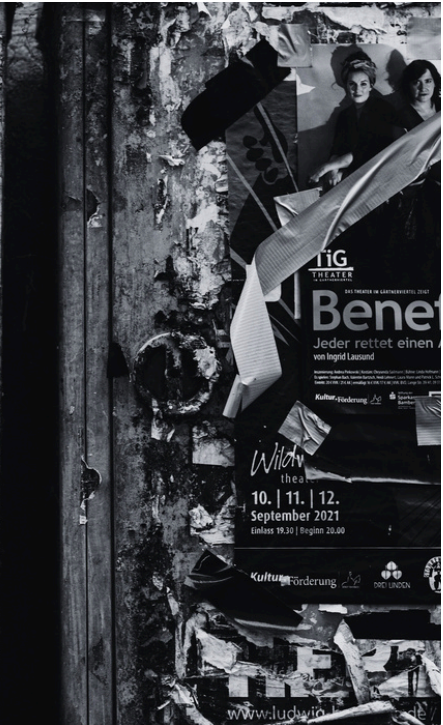
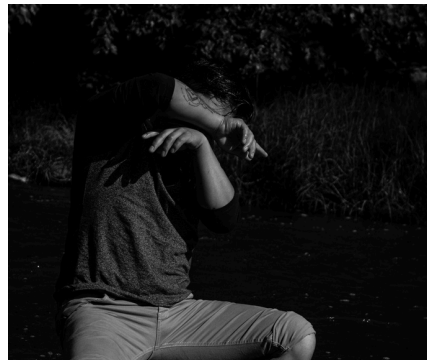
[Freedom of the Press Foundation](#)

What to document

- Violence and weapons or anything else used to harm people (not property)
- Police badge numbers
- Flags, logos, patches, or tattoos of extremist imagery and symbols
- Posters, flyers, leaflets, stickers, art, or other propaganda

Get Consent 🗨️

Sometimes capturing people's faces/other identifiable characteristics is unavoidable. If you do have this footage, and it could possibly be used for evidentiary purposes, try to share that evidence directly with the legal aid organizations. Make sure to get the person's consent before saving it or sharing it elsewhere.



AFTER RECORDING

To determine whether it's safe to share the media you've documented, ask yourself these questions:

1

Can the photo/video possibly endanger or incriminate someone?

If it can, don't share it publicly.

2

Does your photo or video contradict what the police are saying?

If so, safely archive it.

3

Could posting it harm the video's legal value?

If you're unsure, consult the NLG or ACLU first.

4

Are there faces, tattoos, or identifiable features in your content?

If yes, the risk of doxxing, harassment, and incrimination increases. Blur all identifiable features before posting.



5

Can you share pseudonymously or anonymously?

Protect yourself and the people in the photo from doxxing, harassment, and incrimination.

More guides and resources

Mobile Phone Security For Activists & Agitators
Riot Medicine



<https://opsec.riotmedicine.net/static/downloads/mobile-phone-security.pdf>

Know Your Rights
ACLU



<https://www.aclu.org/know-your-rights/protesters-rights>

7 Digital safety tips for people documenting Human Rights abuses
WITNESS



<https://library.witness.org/product/7-digital-safety-tips-for-people-documenting-human-rights-abuses/>

A Quick and Dirty Guide to Cell Phone Surveillance at Protests
EFF



<https://www.eff.org/deeplinks/2020/06/quick-and-dirty-guide-cell-phone-surveillance-protests>

Copwatch Guide to Copwatching during Protests
Berkeley Copwatch

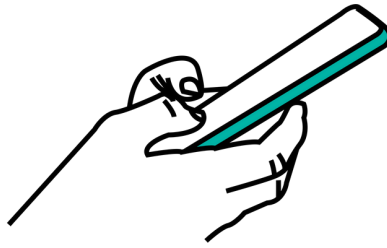


https://www.berkeleycopwatch.org/_files/ugd/9faa72_f7e3368f6a4d40d3980069938712e131.pdf

What to do if your phone is seized by the police
Freedom of the Press Foundation




<https://freedom.press/training/mobile-security-for-activists-and-journalists/>




**Learn more about
OpenArchive:**

open-archive.org



 [@Open_Archive](https://www.instagram.com/Open_Archive)

 [@OpenArchive.bsky.social](https://bsky.app/profile/OpenArchive.bsky.social)

 mstdn.social/@OpenArchive