ReconcilingWorks
LUTHERANS FOR FULL PARTICIPATION

Digital Safety Practices for Protesters

Based on guidance from the American Civil Liberties Union (ACLU) and other expert-sources. This is ***not legal advice****, but rather a set of best-practices to help you think through how to stay safer online and offline when exercising your rights to protest.*

---

1. Know your rights

1. **Right to assemble and record**
   a. The First Amendment protects your right to assemble and express views through protest. American Civil Liberties Union
   b. You generally have the right to photograph or video in public places (including police) so long as you are not interfering with law enforcement. Indivisible
2. **Limits & permits**
   a. Authorities can impose *time, place, and manner* restrictions (e.g., requiring a permit for a large rally, or regulating sound amplification) but not discriminate based on viewpoint. American Civil Liberties Union
   b. Check local regulations in the city/town where you'll protest.
3. **Interaction with law enforcement**
   a. If you are approached by police: you may ask whether you are free to leave; you have the right to remain silent and the right to an attorney.
   b. If your device is seized, staying calm and knowing your rights helps.
4. **Privacy & surveillance concerns**
   a. The ACLU notes that while you may expect some level of privacy, in many situations authorities or others may collect data or monitor you. American Civil Liberties Union

---

2. Digital safety: before the protest

1. **Device preparedness**
   a. Encrypt your device. The ACLU says encryption helps protect your phone if it is lost or confiscated. ACLU of DC

    b. Disable biometric unlock (face/fingerprint). Use a strong passcode instead. Biometrics are easier to coerce; a passcode has stronger legal protection. ACLU of DC
    c. Remove or sign out of unneeded accounts. The fewer credentials on your device, the less risk if it falls into the wrong hands. American Friends Service Committee

2. **Consider whether to bring your phone or leave it at home**
    a. If possible, leave your main phone at home. Bring a "burner" or secondary device if you must. The less personal data you bring, the less risk. Privacy Guides
3. **Clean up location/digital traces**
    a. Turn off location services, WiFi, Bluetooth; clear saved networks. This helps prevent your movements or presence from being logged or tracked. Digital Defense Fund
4. **Secure communications**
    a. Use end-to-end encrypted messaging apps (for example, Signal). Enable disappearing messages where possible. American Friends Service Committee
    b. Update all your software (OS, apps). Many breaches come from unpatched vulnerabilities. American Civil Liberties Union
5. **Backup & minimal data**
    a. Back up any important data before going out. Limit the amount of data on your device for the protest. American Friends Service Committee

---

3. Digital safety: during the protest

1. **Device usage best practices**
    a. Keep your phone locked when not actively in use.
    b. Use airplane mode if you don't need cellular data — this reduces tracking risk. Privacy Guides
    c. Avoid using your primary device if possible. Minimize connectivity if you can.
2. **Capturing video/photos thoughtfully**
    a. Be cautious about capturing identifying features of others (faces, tattoos, etc.) unless their consent is secured — this is especially important if the footage could be used against them. Indivisible
    b. If you take photos/videos of the protest or police, consider how that could later be used (by you, media, or law enforcement) and whether location cues are embedded in metadata.
3. **Buddy system & communication**
    a. Stay with friends, have check-in times. Let someone know your whereabouts.
    b. If you are using a second device or coordinating group communications, keep things simple, encrypted, and minimal.
4. **Face recognition and surveillance awareness**
    a. Wear sunglasses, hat, mask (if safe/legal) to reduce facial recognition risk; avoid unique clothing that makes you easily identifiable. Digital Defense Fund

    b. Be aware that public areas, buildings, drones, and body cameras may be collecting data. WIRED

---

4. Digital safety: after the protest

1. **Device and account follow-up**
    a. If your device was confiscated or lost: change your passwords, remove access credentials, alert your contacts. The Verge
    b. Remove any footage or data you don't want publicly traceable. Think about metadata (location, timestamps) when sharing.
2. **Reflect on what you shared**
    a. Before posting videos or photos, consider whether the content reveals identities, locations, or could be used to target individuals.
    b. When sharing, consider blurring faces or removing location metadata if privacy is a concern. Indivisible
3. **Organizational / group digital hygiene**
    a. If you're part of a protest-group or collective, clarify digital roles (who records, how data is stored, how long it's kept, who has access).
    b. Consider secure data storage practices, access controls, and perhaps "sunsetting" data when it's no longer needed.
4. **Legal & psychological care**
    a. Document any adverse interactions with law enforcement; if you believe rights were violated, consult legal counsel or organizations such as the ACLU.
    b. Consider the emotional impact of being surveilled, targeted, or arrested — seek peer or professional support if needed.

Specific tips & checklists (quick reference)

Before you go

- ○ Encrypt your device & set a strong passcode (disable biometrics)
- ○ Decide if you bring your phone or a burner
- ○ Log out of unnecessary apps/accounts
- ○ Turn off location/WiFi/Bluetooth; clear saved networks
- ○ Install trusted encrypted messenger (Signal)
- ○ Update operating system & apps
- ○ Backup important data
- ○ Inform a friend or support person of your plan & check-in time

During protest

- Use airplane mode if possible
- Keep phone locked and in a safe place
- Capture what you need, but limit personally identifying data
- Be aware of surroundings, surveillance cameras, drones, etc.
- Use buddy/partner system, check in with support person
- Note witness contacts or legal help info in case something happens

After the protest

- If your phone was confiscated or lost: immediately change passwords, alert your contacts
- Review any photos/videos before posting — remove metadata, blur faces/locations if needed
- Delete or archive data you don't need
- Provide legal/psychological support as needed
- If part of an organizing group: hold a debrief on digital security, update practices

---

6. Why this matters

- Technology & surveillance capacity are rapidly expanding. The ACLU observes that consumer tech, networks, and apps can be co-opted for monitoring, tracking, and interfering with free speech and assembly. American Civil Liberties Union
- Phones and devices carry much more than calls: location history, contacts, photos, metadata, apps—all can reveal *who you are*, *where you've been*, *who you know*, and *what you believe*.
- Even innocuous-looking data at a protest can provide law enforcement or adversaries with meaningful information (e.g., attendance at protest = affiliation with cause).
- Ensuring digital safety is not just about personal protection: it affects the safety of others in your community and your movement. If one device is compromised, broader networks might be exposed.

ReconcilingWorks
LUTHERANS FOR FULL PARTICIPATION