FREEDOM & TRUTH
COALITION

Mobile Device Safeguards for Civil Protests: A Comprehensive Guide

This document provides a comprehensive guide to safeguarding your mobile device when participating in civil protests. Following these best practices will significantly reduce the risks associated with digital surveillance and protect your privacy. The most secure option is always to leave your personal phone at home, but if you must bring a device, take these precautions.

I. Device Preparation

Goal: Minimize data exposure if your device is seized or compromised and ensure you don't lose important information.

1.Back Up Your Device and Remove Unnecessary Apps and Data.

Why it's a best practice: Minimizing the data on your device reduces the potential impact if it's seized or compromised. Backing up ensures you don't lose important information. [1]

2.Enable Full-Device Encryption.

iOS: Enabled by default.
Android: Go to Settings > Security > Encryption > Encrypt Phone.
Why it's a best practice: Encryption protects your data even if the device is seized and accessed. [2]

3.Use a Strong Alphanumeric Passcode (at least 6 characters) instead of biometric unlocking.

Why it's a best practice: A strong passcode is harder to crack than a simple PIN or pattern. [17] Alphanumeric passcodes offer better protection than numeric PINs.

4.Disable Face/Fingerprint Unlock Features.

Why it's a best practice: Law enforcement can potentially compel you to unlock your device using biometrics. In the U.S., using a memorized passcode provides stronger legal protection under the Fifth Amendment against compelled device unlocking. [17]

5.Consider Using a Separate "Burner" Phone with a Prepaid Plan, Paid for in Cash.

Why it's a best practice: A burner phone is not linked to your personal information, minimizing the risk of exposing your identity and contacts. [1]

Burner Phone Best Practices (Expanded):

Purchasing Anonymously:

Cash Payment: Always pay in cash to avoid linking the purchase to your credit or debit card.

Point-of-Sale Awareness: Be aware of video cameras at the point of sale. Consider obscuring your face or wearing a hat and sunglasses to minimize facial recognition.

Purchase Location: Opt for smaller, local stores or pharmacies instead of large chain stores. Smaller stores are less likely to have sophisticated surveillance systems. Avoid purchasing near your home or regular haunts.

Receipt Management: Decline a printed receipt or dispose of it securely and away from your residence. The receipt contains a timestamp and store location, which could link you to the purchase.

Consider a Proxy: Ask a trusted friend or acquaintance to purchase the phone for you, further distancing yourself from the transaction.

Phone Number Considerations:

Prepaid SIM: Use a prepaid SIM card purchased separately with cash. Avoid SIM cards that require registration with personal information.

Avoid Number Reuse: Do not use the burner number for any personal accounts or services.

Limited Usage: Keep the burner phone usage strictly limited to protest-related activities.

Secure Storage: Store the burner phone and SIM card separately from your primary phone and other personal devices.

II. Minimize Data Exposure

Goal: Prevent location tracking and data interception.

1.Enable Airplane Mode Frequently to Disable Cellular, WiFi, and Bluetooth Connections.

Why it's a best practice: Disconnecting from networks prevents location tracking and data interception. It also conserves battery life. [13]

2.If Internet Access Is Needed, Use a VPN When Connecting to Public WiFi.

Why it's a best practice: A VPN encrypts your internet traffic, masking your IP address and protecting it from eavesdropping on public networks. [7]

VPN Considerations: Choose a reputable VPN provider with a strict "no-logs" policy. Be aware that even with a VPN, your traffic is still routed through the VPN provider's servers, so trust is essential. Some VPNs offer obfuscation features that can help to hide the fact that you are using a VPN. Consider using a VPN in conjunction with Tor for added anonymity.

3.Turn Off GPS, WiFi, and Bluetooth When Not in Use.

Why it's a best practice: These features can be used to track your location. Turning them off prevents unwanted tracking. [12]

4.Disable Location Services in Your Phone's Settings.

iOS: Settings > Privacy > Location Services > Toggle off

Android: Settings > Location > Toggle "Use location" off

Why it's a best practice: Disabling location services prevents apps and the operating system from collecting your location data. [9]

5.Use End-to-End Encrypted (E2EE) Messaging Apps Like Signal for Communication.

Why it's a best practice: E2EE ensures that only the sender and receiver can read the messages. Not even the messaging service provider can access the content of the messages. [10]

E2EE Recommendations: Verify the encryption status within the app. Be aware that metadata (who is communicating with whom, when) may still be visible, even with E2EE. Other E2EE messaging apps include Wire and Element.

6.Enable Disappearing Messages for Real-Time Communications.

Why it's a best practice: Disappearing messages automatically delete after a set period, reducing the risk of messages being intercepted or stored. [11]
7.When Checking Email, Use a VPN or Tor.

Why it's a best practice: VPNs and Tor can help mask your IP address and location, providing additional privacy when accessing your email account. The email headers can expose your location if not used. [12]

III. Protect Against Surveillance

Goal: Reduce the risk of being tracked or having your communications intercepted.

1.Be Aware of Potential Stingray/IMSI Catcher Usage by Law Enforcement.

Why it's a best practice: Stingrays can be used to track your location and intercept communications. Being aware of this risk helps you make informed decisions about your device usage. [13]
2.Disable 2G Connections (if possible on your device).
3.Use Airplane Mode or Turn Off the Device Completely When Not Actively Using It.

Why it's a best practice: This minimizes the device's ability to be tracked. [14]
4.Consider Leaving Your Phone at Home, as It's the Most Secure Option.

Why it's a best practice: If you don't bring your phone, it can't be tracked, seized, or compromised. [15]
5.Important Note Regarding Stingray Detection: While awareness of Stingray/IMSI catcher technology is crucial, actively detecting their use is generally beyond the capabilities of most individuals. Detecting Stingrays requires specialized equipment, in-depth technical knowledge of cellular network protocols, and the ability to analyze complex radio frequency signals. Many of the indicators that might suggest Stingray use (e.g., rapid battery drain, dropped calls) can also be caused by other factors related to network congestion or device malfunction. Therefore, instead of focusing on detection, we strongly recommend focusing on preventative measures such as those outlined in this guide (encryption, VPNs, minimizing data exposure, etc.) to mitigate the risk of surveillance. If you have serious concerns about being targeted, consult with a qualified security professional or legal expert.

IV. Additional Precautions

Goal: Ensure access to critical information and maintain device functionality.

1.Write Down Essential Information (Emergency Contacts, Lawyer's Number) on Paper or Your Body.

Why it's a best practice: This ensures you have access to critical information even if your phone is inaccessible. [16]
2.Familiarize Yourself with Protest-Specific Apps and Ensure All Apps Are Up-to-Date.

Why it's a best practice: Some apps can assist with communication, documentation, or safety during protests. Keeping apps updated ensures you have the latest security features. [17]
3.Bring a Portable Battery Pack to Keep Your Device Charged.

Why it's a best practice: A charged device is essential for communication and documentation. [18]

4.Be Mindful of Others' Privacy When Taking Photos or Videos.

Why it's a best practice: Respecting the privacy of others builds trust and avoids legal issues. [3]

5.Consider Using Encrypted Walkie-Talkies for Communication (check local laws).

6.The only foolproof way to guarantee a phone is not transmitting signals is to physically remove the battery. However, this is not possible with most modern smartphones.

7.Faraday Bag: A Faraday bag is a specially designed pouch that blocks electromagnetic signals, preventing the phone from communicating with the outside world, even in these low-power states.

Protest-Specific Apps (Examples):

Bridgefy: A messaging app that uses Bluetooth to communicate when internet access is unavailable (useful in areas with network shutdowns). Note: Bluetooth range is limited.

Signal: For secure, encrypted communication (as mentioned previously).

Secure Camera Apps: Apps that allow you to take photos and videos with metadata stripped (location, timestamps, device information) to protect the privacy of yourself and others.

Mapping/Navigation Apps with Offline Functionality: Apps like OsmAnd or Maps.me allow you to download maps for offline use, which can be helpful if cell service is unreliable.

Zello: A walkie-talkie style app that can be useful for group communication (but relies on internet connectivity). Encrypt your communications.

Important Notes About Apps:

Carefully research any app before installing it.

Be aware of the permissions that the app requests.

Only download apps from trusted sources (e.g., official app stores).

V. Legal Considerations

Goal: Understand your rights and the legal consequences of your actions.

Important Note: The information provided in this section is for general guidance only and does not constitute legal advice. "Know Your Rights" legal advice is beyond the scope of this document. You should consult with a qualified attorney for advice tailored to your specific situation.

1.Understand That Wiping Your Device or Revoking Online Account Access Could Potentially Lead to Obstruction of Justice Charges.

Why it's a best practice: Knowing the legal consequences of certain actions helps you make informed decisions. [15]

2.Be Aware of Your Rights as a Protester, Including First Amendment Protections and Potential Restrictions.

Why it's a best practice: Understanding your rights empowers you to assert them if necessary. [16]

3.If Your Phone Is Seized, Invoke Your Right to Remain Silent and Request a Lawyer.

Why it's a best practice: Legal representation protects your rights and ensures due process. [17]
4.Remember That Law Enforcement May Need a Warrant to Search Your Mobile Device, and You Have the Right to Refuse Consent.

Why it's a best practice: This protects you from unwarranted searches and seizures. [18]

By following these safeguards, you can significantly reduce the risks associated with digital surveillance and protect your privacy while participating in civil protests. It's important to stay informed and adapt your strategies as technology and surveillance tactics evolve.

Citations

1. https://www.consumerreports.org/electronics/privacy/protect-phone-privacy-security-during-a-protest-a5990476708/
2. https://www.icnl.org/post/analysis/protesting-in-an-age-of-government-surveillance
3. https://themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024
4. https://www.aclu.org/know-your-rights/protesters-rights
5. https://www.aclupa.org/en/know-your-rights/know-your-rights-protest
6. https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/
7. https://www.acludc.org/en/how-defend-against-police-surveillance-protests
8. https://www.aclu-il.org/en/news/protest-and-surveillance-during-dnc
9. https://www.phila.gov/media/20200630153838/PAC-Protest-Monitoring-Guide.pdf
10. https://news.ycombinator.com/item?id=42829317
11. https://www.pcmag.com/how-to/how-to-lock-down-your-phone-for-a-protest
12. https://afsc.org/newsroom/digital-security-guidelines-protests
13. https://www.amnesty.org/en/latest/campaigns/2020/06/tactics-to-secure-phone-before-a-protest/
14. https://freedom.press/digisec/blog/advice-column-is-it-safe-to-unlock-my-phone-with-my-face/
15. https://theflaw.org/articles/suppression-by-surveillance/
16. https://www.biometricupdate.com/202311/un-rights-chief-remote-biometric-surveillance-of-protests-brings-unacceptable-risks
17. https://ssd.eff.org/module/attending-protest
18. https://www.privacyguides.org/articles/2025/01/23/activists-guide-securing-your-smartphone/

Disclaimer

The topic of mobile device security and surveillance is enormous, as such, this guide is not comprehensive. The information provided in this document is for informational purposes only and is intended to serve as a convenient resource. [FTC] makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained in this document for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will FTC , its affiliates, partners, officers, employees, agents, or licensors be liable for any loss or damage including without limitation, direct, indirect, incidental, special, consequential, or punitive damages, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this information, including, but not limited to, reliance on the information, or the inability to use the information. This includes any actions you take or refrain from taking based on the information provided.

The information provided in this document is not intended as, and shall not be understood or construed as, legal advice. It is essential to consult with a qualified legal professional for advice tailored to your specific circumstances.

Company X assumes no responsibility or liability for any errors or omissions in the content of this document. FTC does not endorse, guarantee, or warrant the accuracy or reliability of any information or content provided by third parties, including any linked websites or sources.

By using this information, you agree to these terms and conditions. If you do not agree, please do not use this information.