Using Phones in High-Risk Public Environments

Phones are high-risk tools in volatile settings. The most effective mitigation is not better apps, but better awareness:

- Assume your device is trackable.
- Assume it can be seized.
- Assume any data on it can be accessed.

Mitigation comes from minimizing digital footprint, rather than using (and trusting) new tools. We should be using technology intentionally and responsibly.

1. What You're Protecting Against

- **Device seizure or loss:** Law enforcement or other actors may attempt to access your phone.
- **Location tracking:** Cell towers, Wi-Fi, Bluetooth, and apps can log and expose your movements.
- **Surveillance and data harvesting:** Facial recognition, IMSI catchers (Stingrays), and Bluetooth/Wi-Fi sniffing.
- **Metadata exposure:** Who you contacted, when, and where, even if content is encrypted.
- **Network disruption:** Internet or cellular shutdowns can disable communication and navigation.
- **Doxxing and online harassment:** Public exposure of private information leading to in-person threats.

2. Device Preparation

Before entering a volatile environment:

- **Use a burner or secondary device.** Minimize personal data. Wipe and discard afterward.
  - A secondary phone reduces exposure of contacts, location history, messages, and photos. Consider a used iPhone (13+), Pixel 7+, or Tracfone with a prepaid SIM card.
- **Set an 8–10 digit numeric passcode.** Avoid biometrics (fingerprint or face unlock), which can be compelled by law enforcement.
  - A random 8-digit passcode takes 40+ years to crack. Use a random generator.

- **Turn off cloud sync.** Disable iCloud Photos, Google Photos, and backup services to prevent real-time data exfiltration.
- **Disable Wi-Fi, Bluetooth, and location services.** These emit identifiers that can be tracked even when not connected.
- **Disable voice assistants (Siri, Google Assistant).** They can be triggered while locked and used to extract information.
- **Remove or log out of sensitive apps.** Delete or log out of email, banking, Signal, or organizational accounts. For Signal, you can securely back up your messages to the cloud before deleting.

3. Limit Exposure

- **Use airplane mode.** This disables cellular, Wi-Fi, and Bluetooth—preventing tracking and remote access.
  - Re-enable only briefly if needed, then return to airplane mode.
  - May need to keep Bluetooth on if using a Bluetooth-enabled chat app like BitChat
- **Keep the device powered off when not in use.** A powered-off phone cannot be tracked or accessed remotely.
- **Take photos/video from the lock screen.** Both iOS and Android allow this. It minimizes unlock frequency.
- **Avoid unlocking the device unnecessarily.** If seized while unlocked, all active sessions are accessible.

4. Offline Chat Apps

Bitchat (iOS / Android)

- **Pros:**
  - Peer-to-peer, no internet required (works over Bluetooth).
  - End-to-end encryption in direct messages.
  - Open-source
- **Risks:**
  - No independent security audit as of early 2026.
  - Not designed for anonymity. Your phone can be connected to you.
  - Still immature software - it may not be reliable.

Briar (Android only)

- **Pros:**
  - Decentralized, peer-to-peer messaging app that works over Bluetooth, Wi-Fi, or Tor. No central servers or internet required for local mesh use.
  - Open-source and audited by third parties.
  - End-to-end encrypted by default.

    - No phone number or email required.
    - Works in offline, high-surveillance environments.
    - Resistant to network disruption and censorship.
- **Risks:**
    - Android only.
    - Requires pre-arranged connections for secure messaging (contacts must exchange keys in advance).

5. Stingrays and Network Disruption

- **Stingrays (IMSI catchers)** mimic cell towers to intercept calls, texts, and data.
- **Mitigation:**
    - Use airplane mode.
    - Disable cellular data.
    - Use a Faraday bag to block all signals.
    - Power off phone to be sure.

6. Push Button Alarms & Personal Safety Tools

Red Panic Button

- Sends SMS/email with GPS link to emergency contacts.
- Tracks location, may share data with third-party advertisers.
- Best for individuals needing a simple SOS, not secure environments.
- Not recommended for high-risk activism due to data collection.

Turnsignl

- Connects you via video to a live attorney during traffic stops.
- Real-time legal guidance, recording saved to cloud.
- Records video, stores data in U.S., subject to law enforcement requests.
- Best for de-escalation, not protest use.

7. Organizational Considerations

- Staff and leadership should not bring primary devices into high-risk environments.
- Burner phones should be provisioned with minimal data and clear wipe protocols.
- Incident response plans should include digital seizure scenarios—e.g., who to contact, how to verify safety.
- Training should emphasize that digital safety is not about perfect security, but reducing exposure.

Revision #6
Created 28 January 2026 15:58:43 by Josh
Updated 28 January 2026 16:58:37 by Josh