Data Privacy and Security Guide

(Radical Bloom)

General Principles

- Minimize Data Sharing: Only provide necessary personal information online or in person.
- Use Strong Passwords: Create unique, complex passwords for different accounts. Use a password manager if needed.
- Enable Two-Factor Authentication (2FA): Use 2FA wherever possible for an added layer of security.
- Limit Social Media Exposure: Adjust privacy settings to restrict who can view your personal information.
- Be Wary of Phishing Attacks: Avoid clicking on suspicious links or downloading unknown attachments.

Device Safety

- Remove Biometrics: Avoid using Face ID or fingerprints, as law enforcement can use these to unlock your device.
- Encrypt Your Data: Use full-disk encryption to protect sensitive files.
- Use a Secure VPN: A virtual private network helps mask your IP address and browsing activity.
- Turn Off Location Services: Disable GPS tracking unless absolutely necessary.
- Secure Your Hard Drives: Store external drives in separate locations and use encryption.
- Regularly Clear Your Cache and Cookies: Prevent tracking by websites and third parties.

Communication Safety

- Use Encrypted Messaging Apps: Apps like Signal, Session, or Keybase offer end-to-end encryption.
- Burner Phones for Activism: Replace burner phones every week or two to avoid tracking.
- Store Contacts in Code: Save phone numbers using anagrams or shorthand to obscure their real identities.
- Avoid Unsecured Wi-Fi: Use mobile data or a VPN when connecting to public networks.

Online Presence Management

- Use Pseudonyms When Possible: Avoid linking personal details to online activism accounts.
- Delete Old Accounts and Data: Regularly audit and remove unused accounts.
- Scrub Metadata from Photos: Remove geotags and EXIF data before sharing images.
- Beware of AI Tracking: Many platforms use AI to track behavior; limit usage of services that overly intrude on privacy.

Emergency Preparedness

- Back Up Important Files: Keep encrypted backups in separate locations.
- Have a Data Wipe Plan: Know how to remotely erase devices if they are lost or seized.
- Know Your Legal Rights: Understand what law enforcement can and cannot demand regarding your digital data.
- Create Secure Storage for Sensitive Documents: Consider storing physical copies in safe locations.

By following these steps, you can better protect your data and maintain your privacy in an increasingly monitored world.