Mobile Privacy

Nov 2014

By @saltire and @dmix

Mobile privacy: is it possible?

What kind of data am I leaking?

- Identity
- Location
- Browsing history
- Session data
- Communications
- Contacts

How does my device leak data?

- Data connection
- Wireless
- NFC
- Bluetooth
- Browser exploits
- Rogue apps / malware
- Physical access

Android security

Settings:

- Wireless & Networks > Disable NFC
- Location access > Off
- Security > PIN lock
- Backup & Reset > don’t auto-restore, don’t back up data
- CM Statistics > Disable reporting
- Developer options > Device hostname: localhost

Android security

Core features

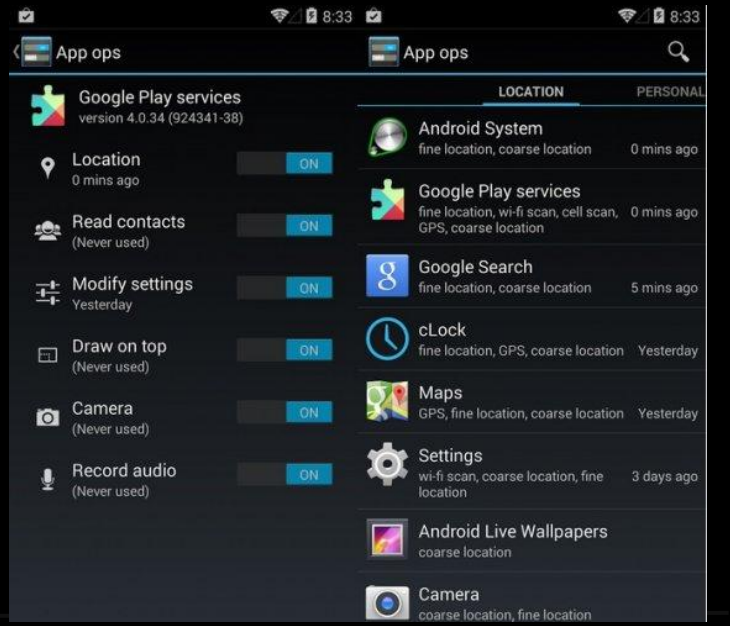
- Full-disk encryption
- Don’t forget airplane mode!

Android security

Limit app privileges with App Ops

Two ways to access this:

- F-droid > Launch App Ops
- CyanogenMod > Settings > Privacy Guard



Connecting to Tor

Orbot: Connect to Tor
Optional: route all traffic through Tor

Orweb: Tor browser

ChatSecure

- Connects to Facebook,
  Google Hangouts, any XMPP service
- Supports Off-the-Record encryption
- Optionally connects through Tor
- Android & iPhone

Also: **Xabber**

TextSecure

- Replacement for Android messaging
- OTR-like encryption, optimized for text messages
- Falls back to regular SMS for non-TextSecure contacts

RedPhone (Android) / **Signal** (iPhone)

- Replacement for voice dialer
- Upgrades to an encrypted call when calling another RedPhone / Signal user
- Interoperable

Conclusion

Questions?

To learn more,
visit the Mobile Privacy workstation