Android Privacy Guide

Let's talk about...

- Why choose Android?
- Encrypted storage
- Encrypted communication
- Privacy-aware searching
- Anonymization techniques
- Other privacy recommendations

Let's talk about...

- Why choose Android?
- Encrypted storage
- Encrypted communication
- Privacy-aware searching
- Anonymization techniques
- Other privacy recommendations

Android Privacy Guide

Encrypted storage
Full disk encryption
Application-specific encryption
Why choose Android when you care about your privacy
Anonymization techniques
Other privacy recommendations
Privacy-aware searching
Use DuckDuckGo.com instead of Google!
Disable Geolocation services
Encrypted communication
Email encryption
Instant chat encryption
Voice encryption
Conclusion

Let's talk about...

- Why choose Android?
- Encrypted storage
- Encrypted communication
- Privacy-aware searching
- Anonymization techniques
- Other privacy recommendations

Why chooSe Android when you care about your privacy

Why Yes:

- It is open source - easily and completely auditable what is crucial for security (iOS, Blackberry, Windows Mobile are proprietary close-source platforms) - you know there isn't anything hidden that might violate your privacy (e.g. Carrier IQ)
- There is a "privacy-aware" Android distribution - Cyanogenmod that has removed any Google spying functionality, incognito mode, torification etc.
- It supports all advanced Linux security features (e.g. SELinux, Truecrypt full disk encryption, etc.)

Why Not:

- iOS marketplace is more conservative, it may contain less malware/trojans

Encrypted Storage

Full disk encryption

- Android >=4.0 supports native full disk encryption
- other alternatives are Luks encryption, Cryptonite
- encrypt your root filesystem including all your external SD cards and your Titanium backups!

Application-specific encryption

- at least AES256 storage for your sensitive information (credit card numbers, credentials, private keys, etc)
- B-Folders, KeePassDroid, NoteCipher

Encrypted communication

Email encryption

- PGP encryption based on APG (K9 Mail, Kaiten Mail, r2mail2)
- S/MIME encryption (r2mail2)

Instant chat encryption

- based on OTR or PGP
- Gibberbot (quite unstable), IM+ Pro with OTR plugin

Voice encryption

- based on ZRTP protocol and SIP/TLS
- CSipSimple (can be used with Ostel.me)
- Acrobits Softphone with ZRTP outgoing module (or Groundwire)

Privacy-aware Searching

Use DuckDuckgo.com instead of Google!

- Google is not a privacy-aware search engine, it tracks everything about you!

Disable Geolocation services

- If you don't use them

Anonymization techniques

Outgoing connection / browsing anonymization

- based on Tor, torification of all outgoing connections from smartphone is possible
- Orbot and Orweb v2, AdBlockPlus Firefox plugin

Payment transactions

- based on Bitcoins
- Bitcoin Wallet

Face obscure

- ObscuraCam

Other privacy recommendations

Use trustworthy software

- Always check application's permission during installation
- Use applications from official Android Market only
- Use antivirus and firewall (DroidWall), Network Log

Avoid using social networks

- They have usually access to all your sensitive information stored on your smartphone

Avoid using banking applications

Use trustworthy tracking / wiping software

- With the possibility of "remote wipe" and "remote lock"
- Secure wipe InTheClear

Conclusion

- Care about your privacy - privacy intrusions by 3rd parties (government, corporations, your competitors) will be more likely in the future
- You are already tracked (by data retention law, all social networks, Google) and can be easily monitored (by any secret or other government agencies)
- The Internet is a permanent storage - some your sensitive data may be never erased when they are leaked

Thanks for your attention!

Contact me!