

Let's talk about...

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

Android Privacy Guide

Why choose Android when you care about your privacy

- It's an open source operating system, which means you can audit the code to see how it works and make sure it's doing what you want it to do.
- There's a large community of developers who are constantly improving the system and adding new features.
- You can choose to use the open source version of the operating system, which means you can see exactly what's going on under the hood.

Encrypted storage

- Full disk encryption
- Android → A-Clearly better for data protection
- Also available on iOS (Apple's HealthKit, Keychain)
- Android can use BitLocker (Microsoft's software) or FileVault (Apple's software)
- Applications can use their own encryption
- Also available on iOS (Apple's HealthKit, Keychain)
- Available on Android (e.g. Signal, Proton Mail, etc.)

Anonymization techniques

- Tor network (anonymous web browsing)
- VPNs (anonymous web browsing)
- Mixers (anonymous web browsing)
- Anonymous email services
- Anonymous chat services
- Anonymous social media

Encrypted communication

- Email encryption
- PGP encryption (used in PGP Mail, K9 Mail, etc.)
- S/MIME encryption (Outlook)
- Instant messaging encryption
- Local on-premise encryption
- Signal (end-to-end encrypted)
- WhatsApp (end-to-end encrypted)
- Telegram (not end-to-end encrypted)
- iMessage (not end-to-end encrypted)

Conclusion

- Android is a better choice for privacy-conscious users.
- It's an open source operating system, which means you can audit the code to see how it works and make sure it's doing what you want it to do.
- There's a large community of developers who are constantly improving the system and adding new features.
- You can choose to use the open source version of the operating system, which means you can see exactly what's going on under the hood.

Let's talk about...

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

Android Privacy Guide

Why choose Android when you care about your privacy

- It's an open source operating system, which means you can audit the code and see how it works.
- It's not tied to a specific hardware manufacturer, so you can choose the device that best fits your needs.
- It's not tied to a specific carrier, so you can choose the carrier that best fits your needs.
- It's not tied to a specific country, so you can choose the country that best fits your needs.

Encrypted storage

- Full-disk encryption
- Android → A-Crypter before for disk encryption
- Also available in the form of an application: Cryptor
- Android can use BitLocker (only if you're using a USB drive with Windows recovery)
- Applications: VeraCrypt, Cryptor
- Also available in the form of an application: Cryptor
- Also available in the form of an application: Cryptor
- Also available in the form of an application: Cryptor

Anonymization techniques

- Tor network
- VPN
- Proxy servers
- Anonymous email
- Anonymous web browsing
- Anonymous social media
- Anonymous chat
- Anonymous search engines
- Anonymous file sharing
- Anonymous file storage
- Anonymous file hosting
- Anonymous file sharing
- Anonymous file storage
- Anonymous file hosting

Encrypted communication

- Email encryption
- PGP encryption (used in PGP Big Mail, better Mail, etc.)
- S/MIME encryption (S/MIME)
- Instant messaging encryption
- Local in PGP or PGP
- Encrypted chat (Signal, etc.)
- Encrypted voice (Signal, etc.)
- Encrypted video (Signal, etc.)
- Encrypted file sharing (Signal, etc.)
- Encrypted file storage (Signal, etc.)
- Encrypted file hosting (Signal, etc.)

Conclusion

- Android is a good choice for privacy-conscious users.
- It's an open source operating system, which means you can audit the code and see how it works.
- It's not tied to a specific hardware manufacturer, so you can choose the device that best fits your needs.
- It's not tied to a specific carrier, so you can choose the carrier that best fits your needs.
- It's not tied to a specific country, so you can choose the country that best fits your needs.

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)
- Acrobats 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!

