Smartphone privacy

London CryptoParty 2013

Why worry about smartphone privacy?

Mobile phones are really **tracking devices that also make phone calls**

“Dumb” phones

- They still leak a lot about you:
  - Voice calls: who/what
  - SMS: who/what
  - Coarse historical location
- Tools exist to remotely hijack a phone & turn on the mic
- IMSI catcher – “who was at this meeting?”

“Smart” phones?

- All of the above…
- But a smartphone knows much more about you:
  - Access to your emails
  - Mapping of your social network
  - Precise location
  - Geo-tagged photos
  - And much more…

What **can't** be done about it

- ~~Hide your location~~ – required for service to function
- ~~Hide who you communicate with~~ (very hard)
- ~~Defend your phone from being hijacked~~
  - Open Source (like Android) is the only glimmer of hope we have

Plenty of commercial offerings out there to attack your phone

- Gamma International
- Cellebrite
- MicroSystemation XRY

For more, see the Wikileaks Spy Files

What **can** be done about it?

- Resist mass surveillance:
  - VOICE CALLS : ZRTP apps
  - SMS/TEXT: SMS encryption
  - EMAIL: OpenPGP
  - IM: OTR
  - BROWSING: Tor
- Bonus privacy points:
  - LOCAL FILES – Encrypted local/SD storage
  - LOCAL APPS – Xprivacy

Private voice calls

- The trick is encrypted VoIP – avoid GSM.

Recommended apps:

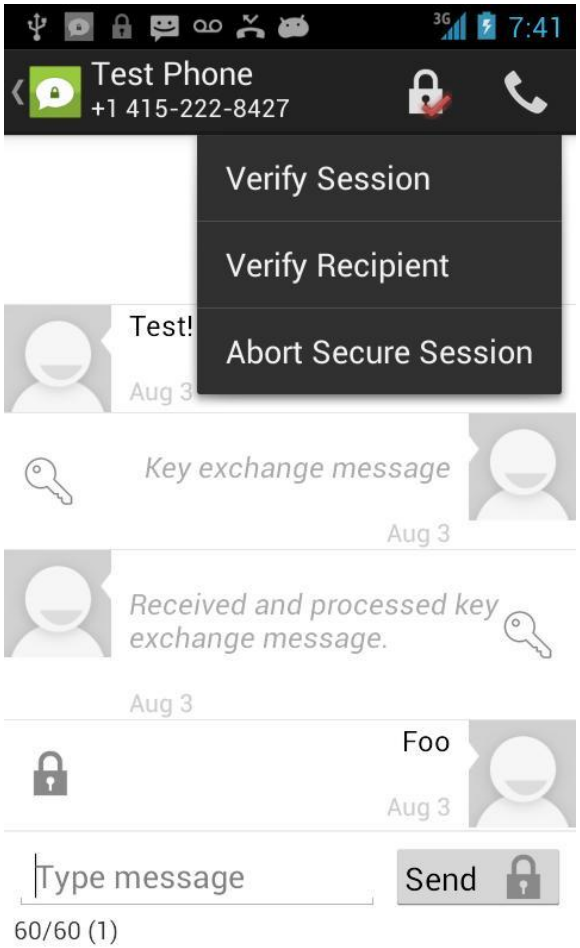
1. Red Phone
   - Just works!
2. Csipsimple + https://ostel.co
   - Compatibility with any SIP phone
3. Silent Phone
   - ~£70/year
4. Acrobits SoftPhone + https://ostel.co
   - ~£35 one-off

Private SMS

- TextSecure 

- Free app for Android
- Don’t forget – you need to “Start Secure Session”

Private SMS – demo!



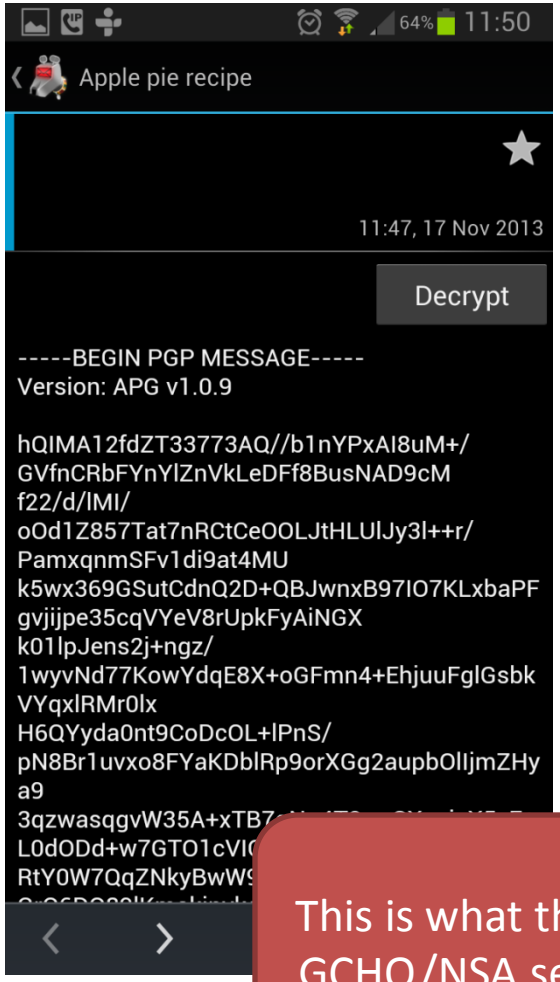
Establishing a secure SMS session

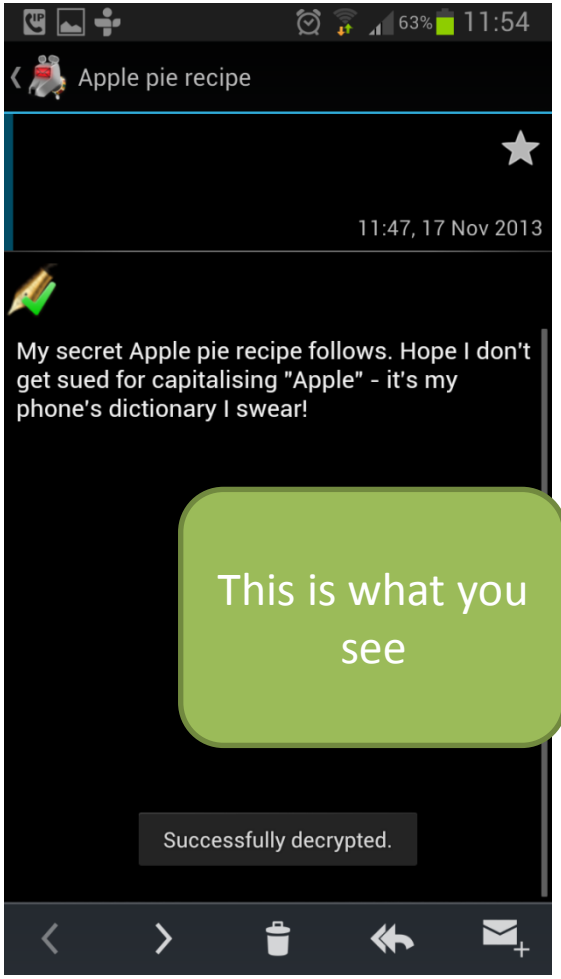
Private email

- Free solution for Android
  - K9 (email)
  - APG (encryption)
- Solutions for iOS exist
- Remember, you can hide only content, *not who you communicate with*.
- Trust only OpenPGP
- Don’t save your master key on your phone

https://alexcabal.com/creating-the-perfect-gpg-keypair/
https://grepular.com/Android_Privacy_Guard_and_Subkeys

Receiving private email – demo





Private IM

- ChatSecure
  - Android & iOS
- Uses OTR
  - As a protocol, almost sounds too good to be true

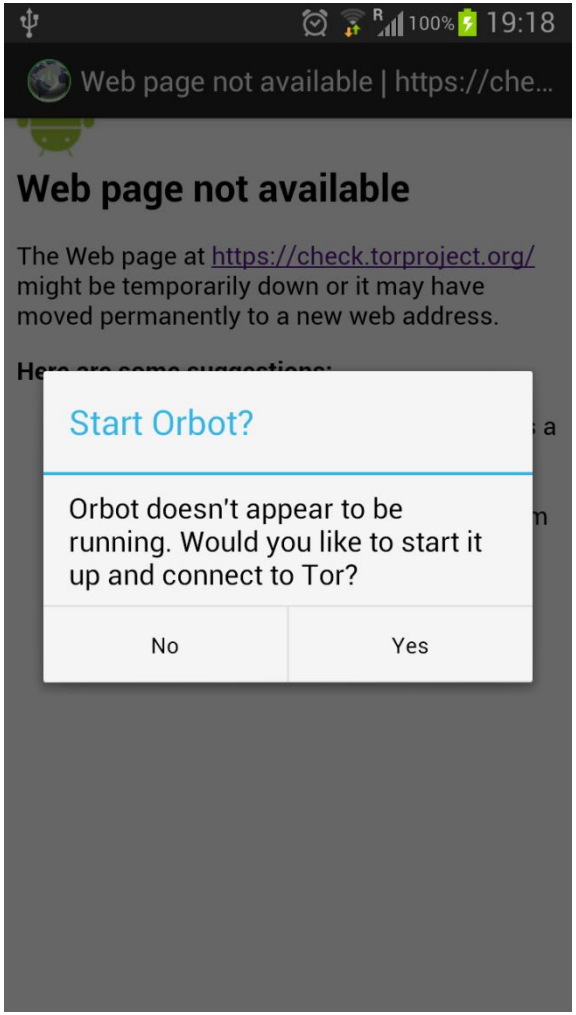
- But…
  - Must be always connected to the network
  - Configuration & operation are not intuitive

Private Browsing

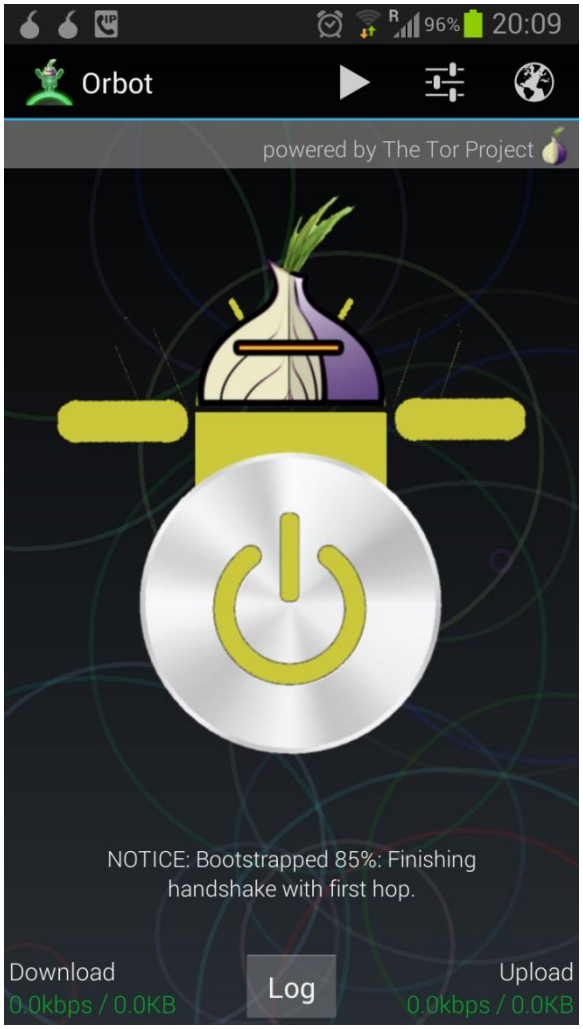
- Orbot (Tor) + Orweb (Tor browser)
  - Android only

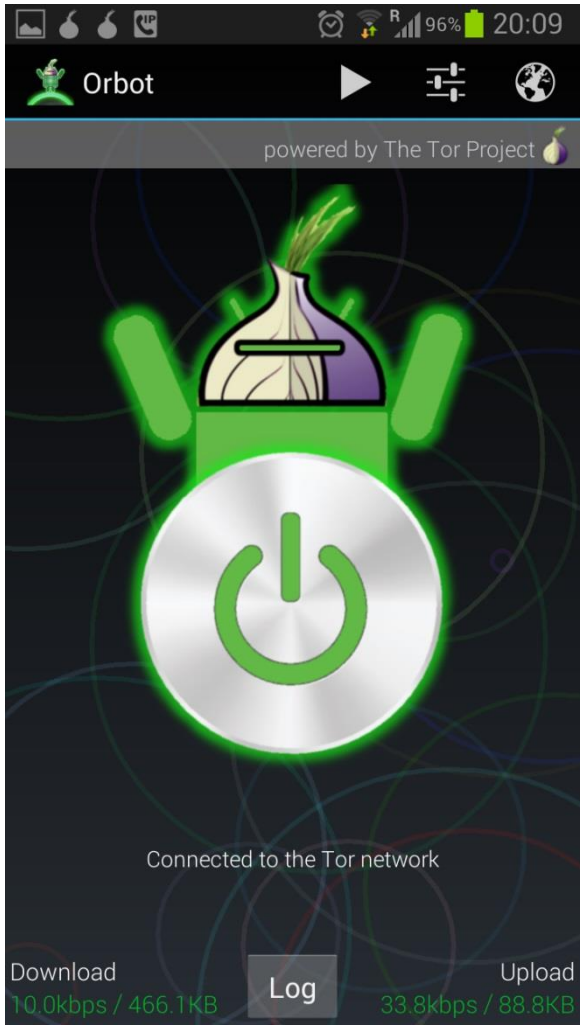
PS: Shout out if you're not sure what "Tor" is

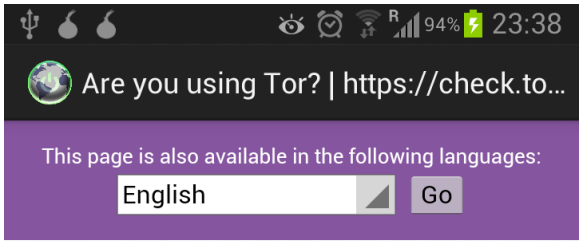
Private Browsing – demo (1)



Private Browsing – demo (2)





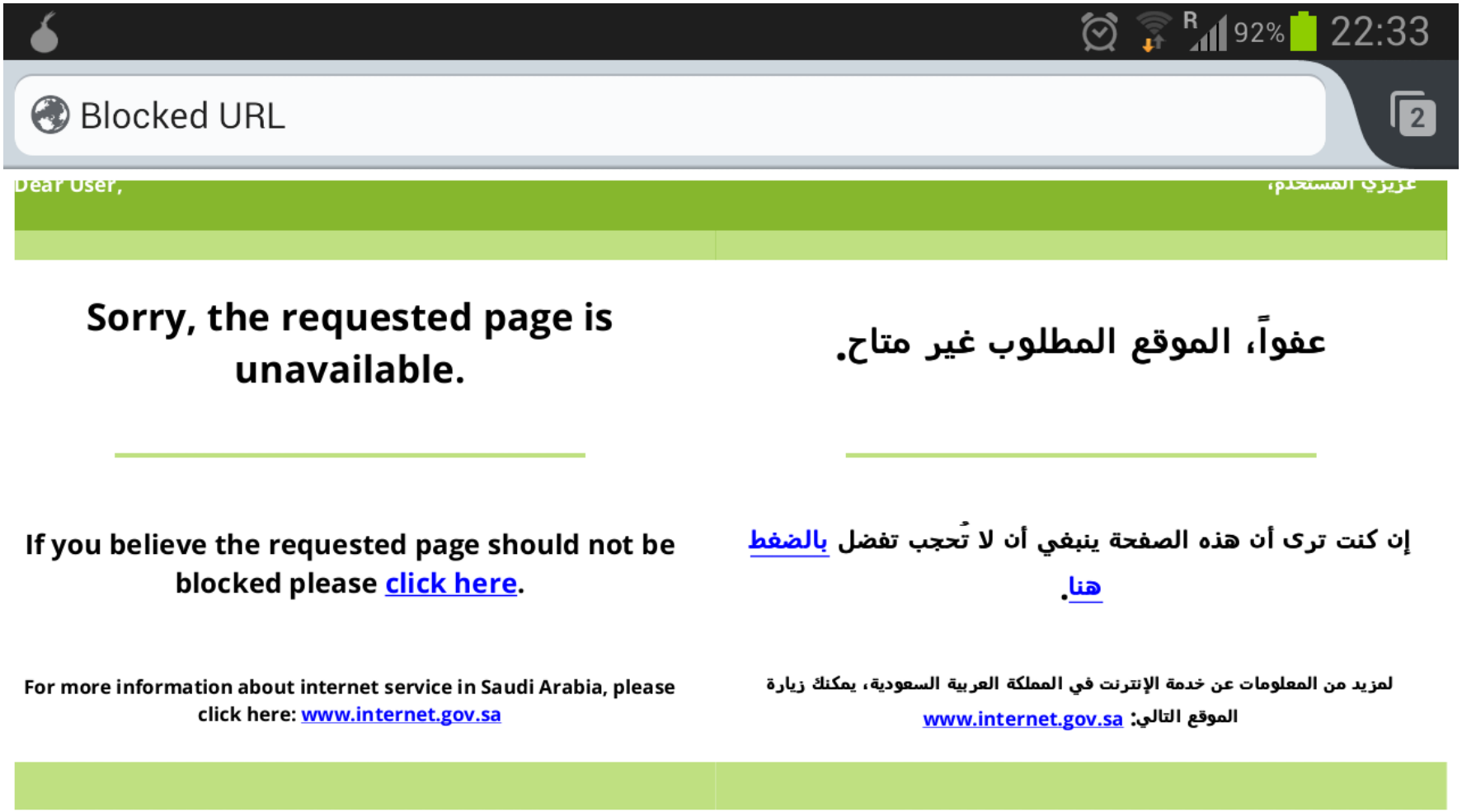


Congratulations. This browser is configured to use Tor.

Your IP address appears to be:
178.32.172.126

Please refer to the Tor website

Pleasant side-effects of Tor: Anti-censorship



Here comes the bonus part

- With the tools mentioned so far you can get some privacy when using your smartphone

- Bonus points
  - Stop casual thieves grabbing your files
  - Control rogue app permissions

Encrypted local storage

- iPhone: it’s just there
- Android: you need to do it
  - Remember to encrypt phone and SD card

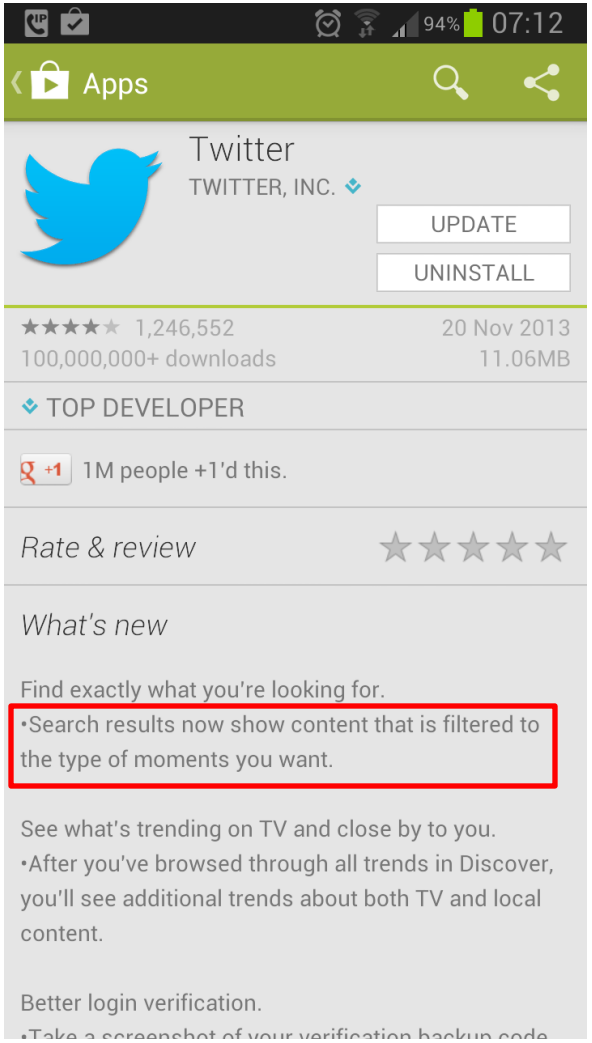
- No defence against law enforcement, just casual (low-tech) thieves

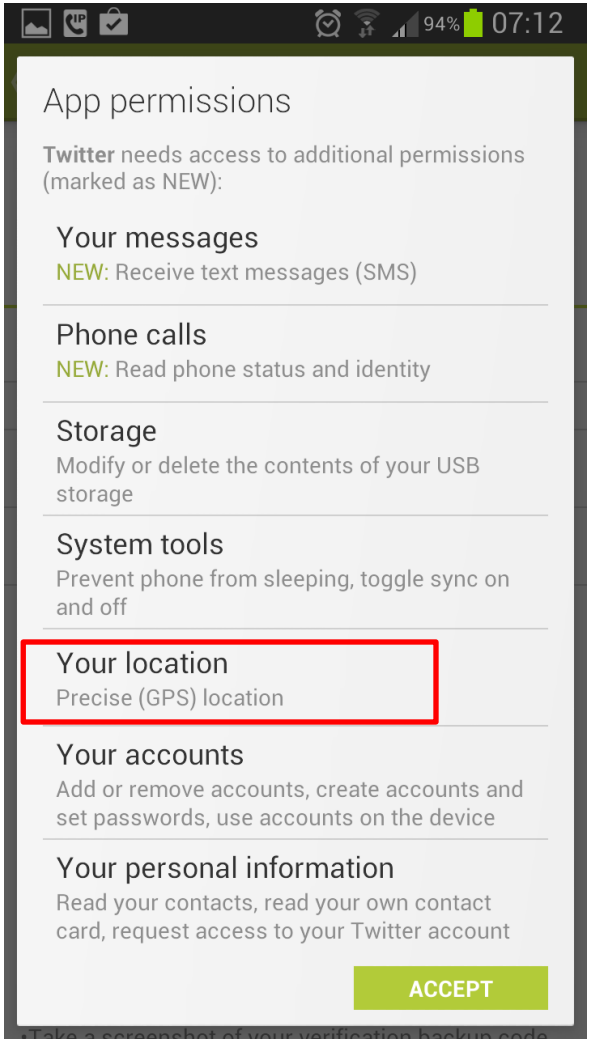
Privacy from local apps

- Current model: “Take it or leave it”
- Xprivacy
  - gives control back to you
  - Example: When an app asks for your location, Xprivacy can answer with fake coordinates

- But
  - Andoid only
  - Phone must be rooted

Example of “take it or leave it”





Parting thoughts

- Smartphones are taking over the world
- Policy changes will take years
- Get some smartphone privacy **now** by using the tools we discussed

Questions?

Keep the discussion going at
http://apapadop.wordpress.com