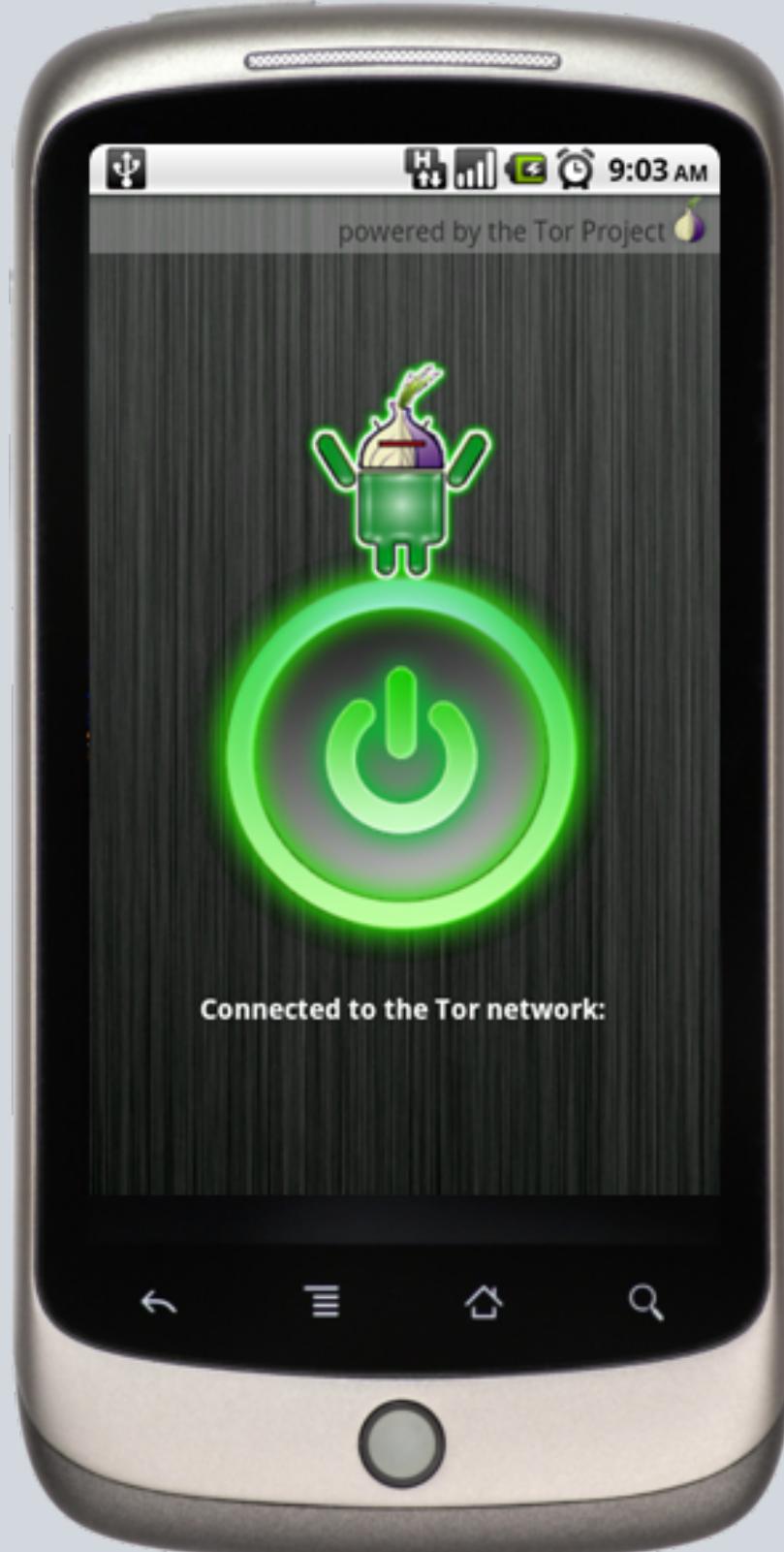


ORBOT

Tor on Android: providing free software and an open network that helps defend against network traffic analysis - a form of surveillance that threatens personal freedom and privacy

- With root access, proxy all application traffic through Tor
- Firefox on Android integration through ProxyMob Add-on
- Works on 2.5G, 3G and Wifi nets
- Supports running servers on hidden services for advanced applications
- Enables devices to be a Tor hotspot



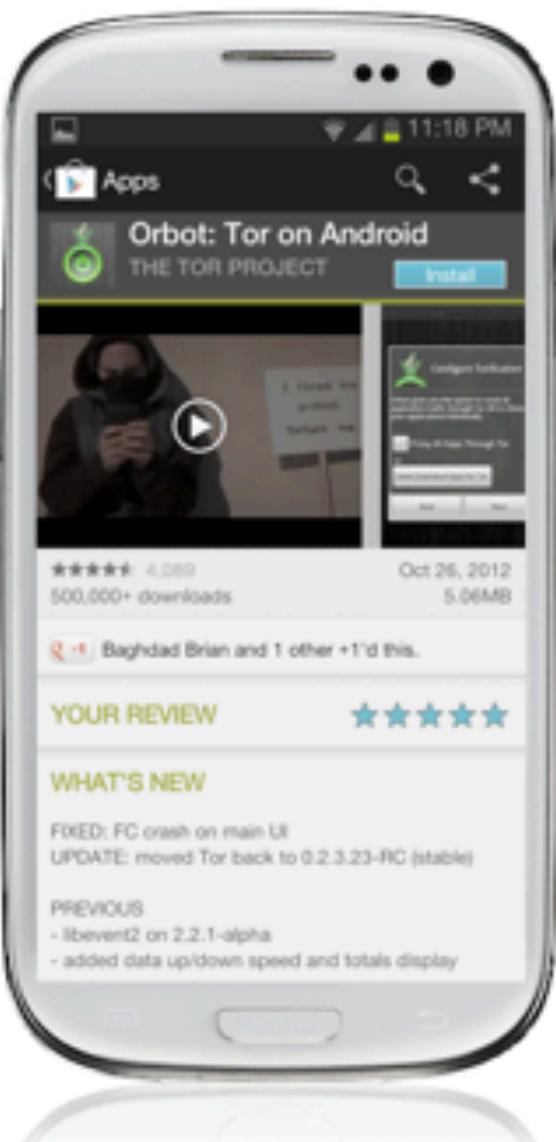
So you want to bypass censorship on Android?

1. Open the Google Play Store. [Easy](#). [Next?](#)
[It's blocked. Help!](#)



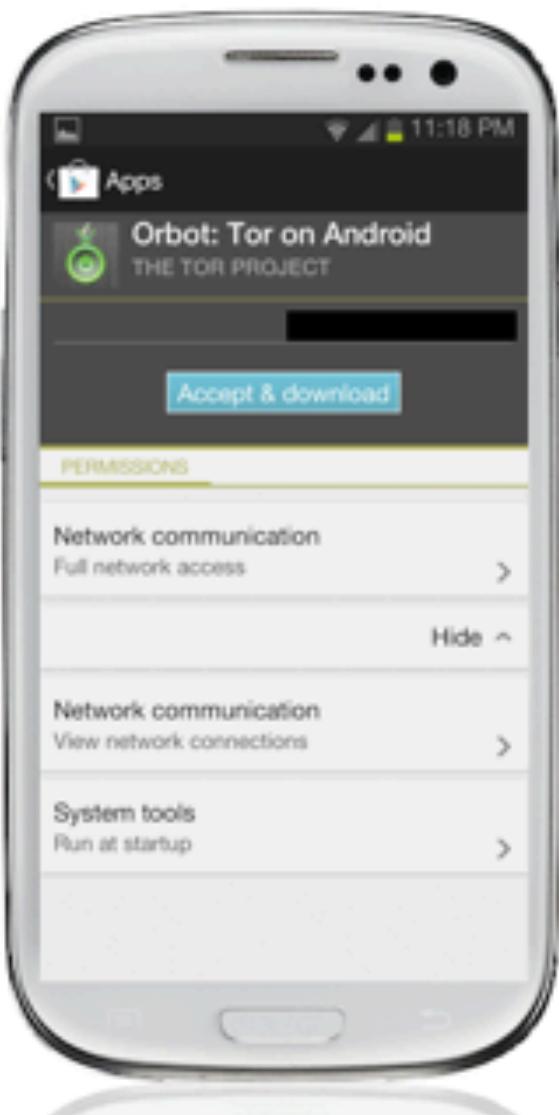
So you want to bypass censorship on Android?

2. Search for *Orbot*. [Got it.](#)



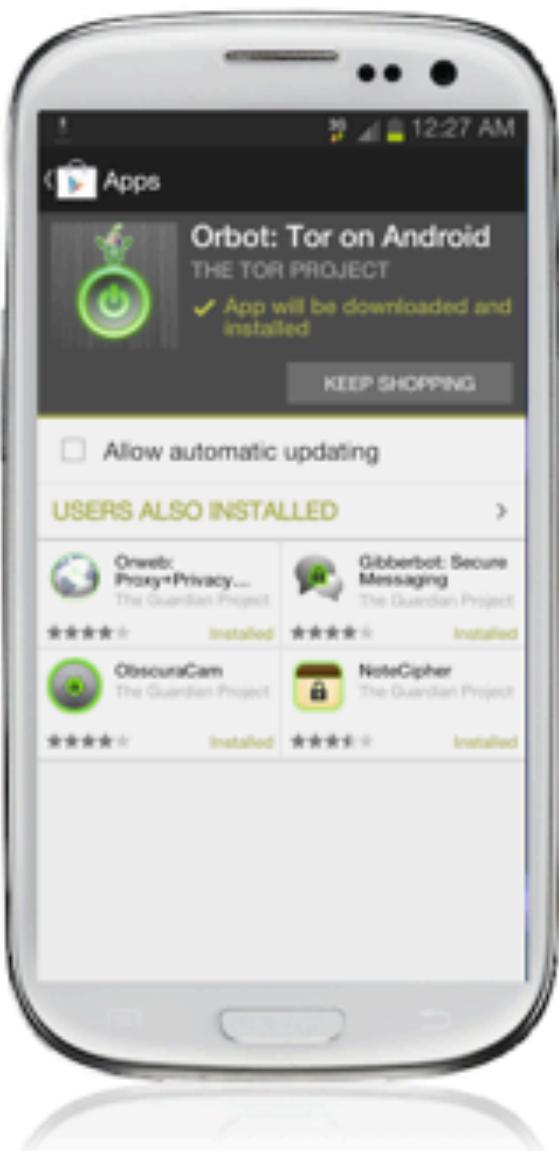
So you want to bypass censorship on Android?

3. Review the permissions. Then, maybe, accept them. [OK, I trust you.](#)



So you want to bypass censorship on Android?

4. Get our sister app, Orweb for anonymous web browsing. Hey look, it's suggested!



So you want to bypass censorship on Android?

5. Open Orbot. Done.



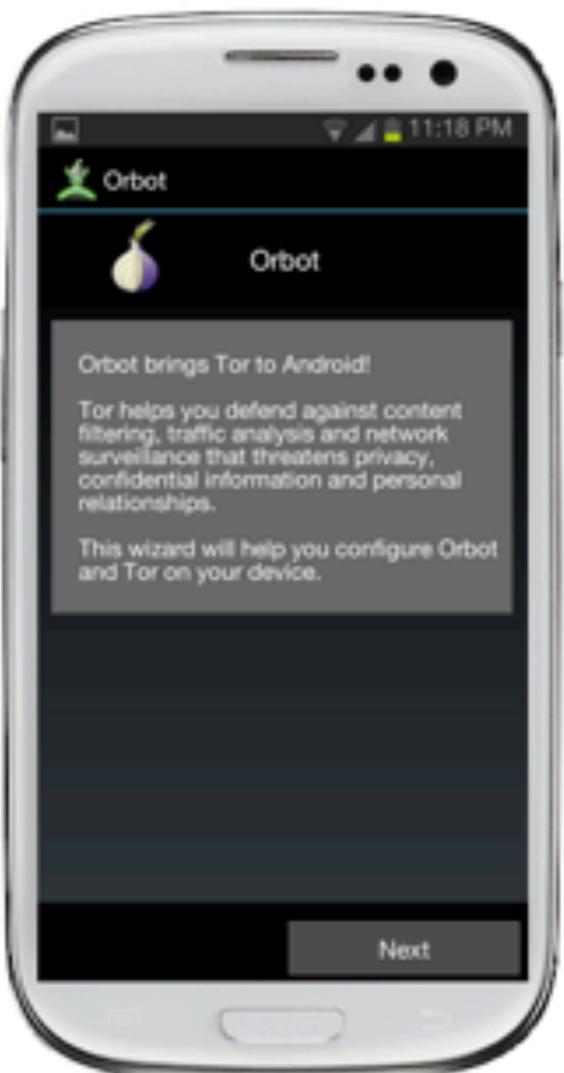
So you want to bypass censorship on Android?

6. Choose your language and get started. [Let's go with English.](#)



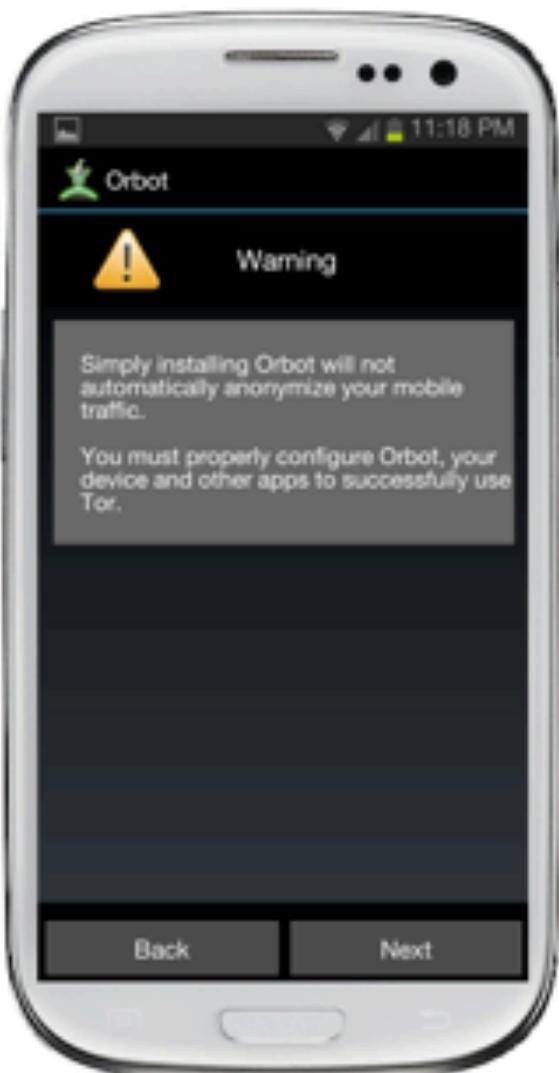
So you want to bypass censorship on Android?

We'll tell you about our project and onion routing.



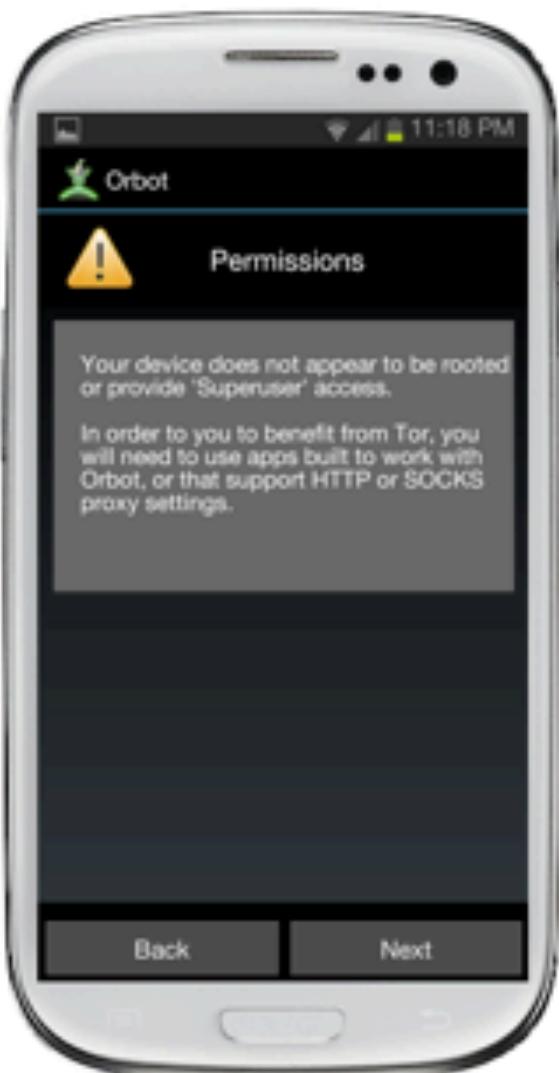
So you want to bypass censorship on Android?

Is it really secure? We break it down.



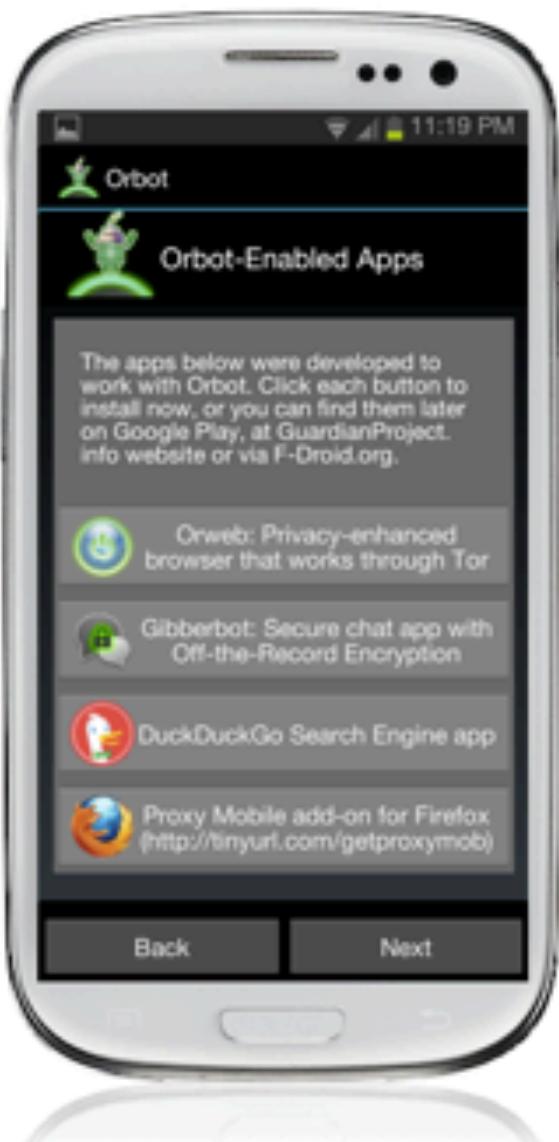
So you want to bypass censorship on Android?

If your phone is jailbroken/rooted then you choose to route all traffic over Tor.



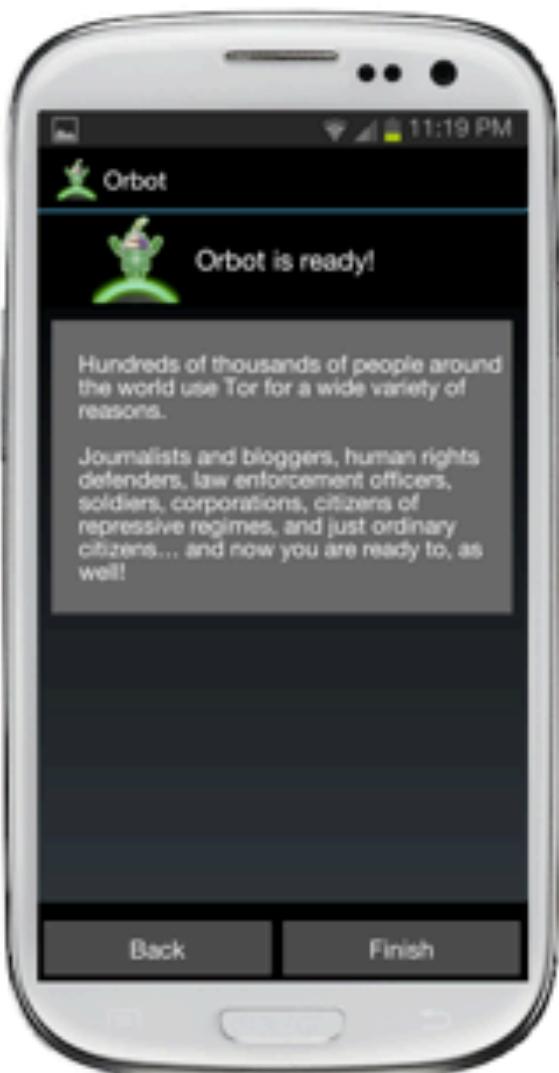
So you want to bypass censorship on Android?

Otherwise you can use these apps over Tor using the proxy feature.



So you want to bypass censorship on Android?

Security is a two way street. Make sure your friends are secure too.



So you want to bypass censorship on Android?

8. Now we long press the button to getting started. [Pressing!](#)



So you want to bypass censorship on Android?

Orbot starts grey



So you want to bypass censorship on Android?

Orbot turns yellow as it's starting



So you want to bypass censorship on Android?

Orbot turns green when it's connected to Tor.



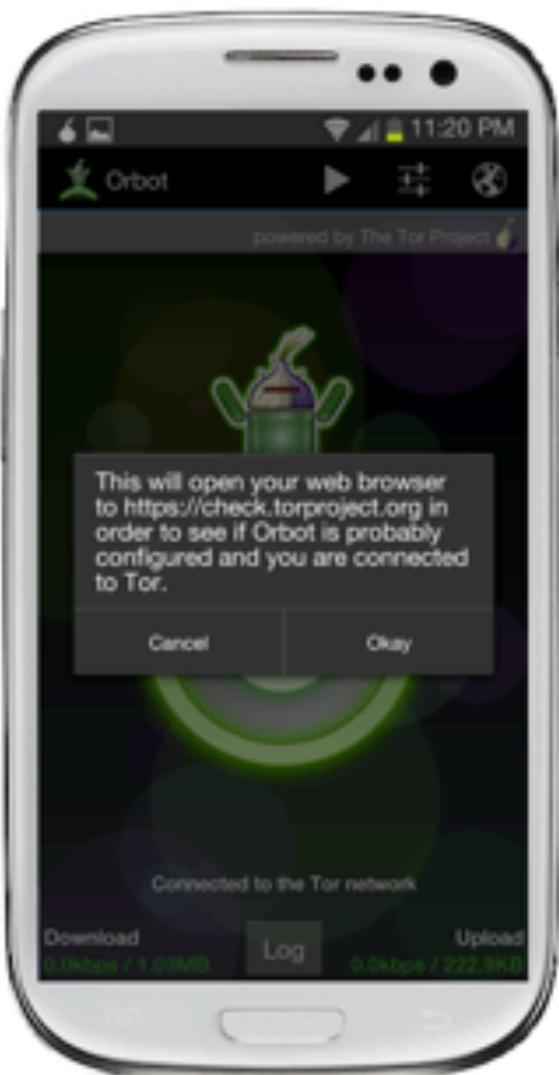
So you want to bypass censorship on Android?

9. Let's confirm we can now bypass the censors. [Ok, how?](#)



So you want to bypass censorship on Android?

10. Press the globe icon to pull up our web browser Orweb. [Opening the app!](#)



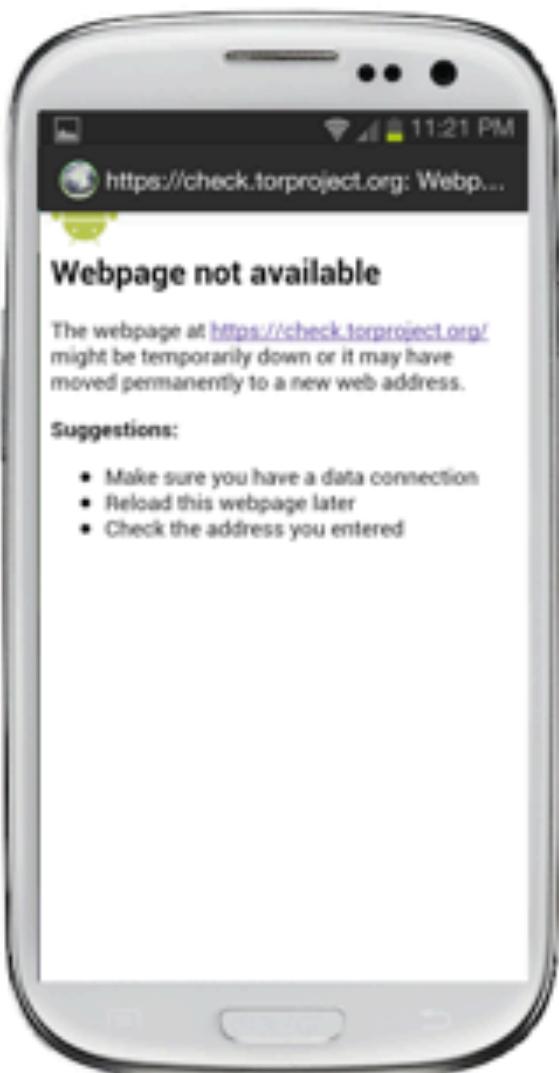
So you want to bypass censorship on Android?

11. It pulls up check.torproject.org to confirm we're surfing anonymously.
[I see congrats.](#) / [I don't see congrats.](#)



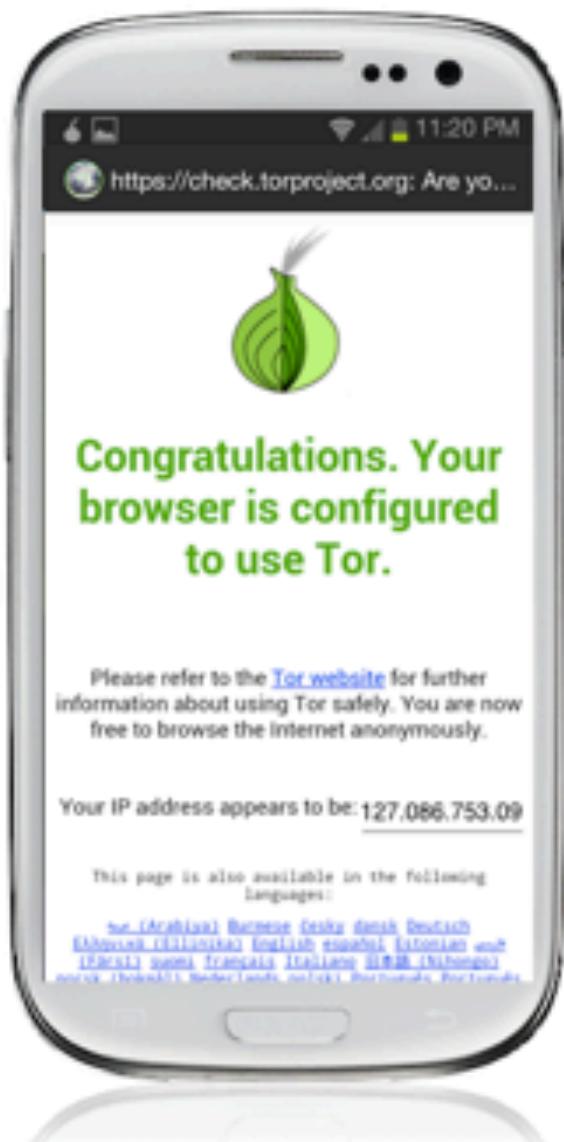
So you want to bypass censorship on Android?

Your configuration is wrong. [Restart Orbot and try again.](#)



So you want to bypass censorship on Android?

You're awesome! [Play it again?](#) - For more info, visit our site:
[The Guardian Project](#)



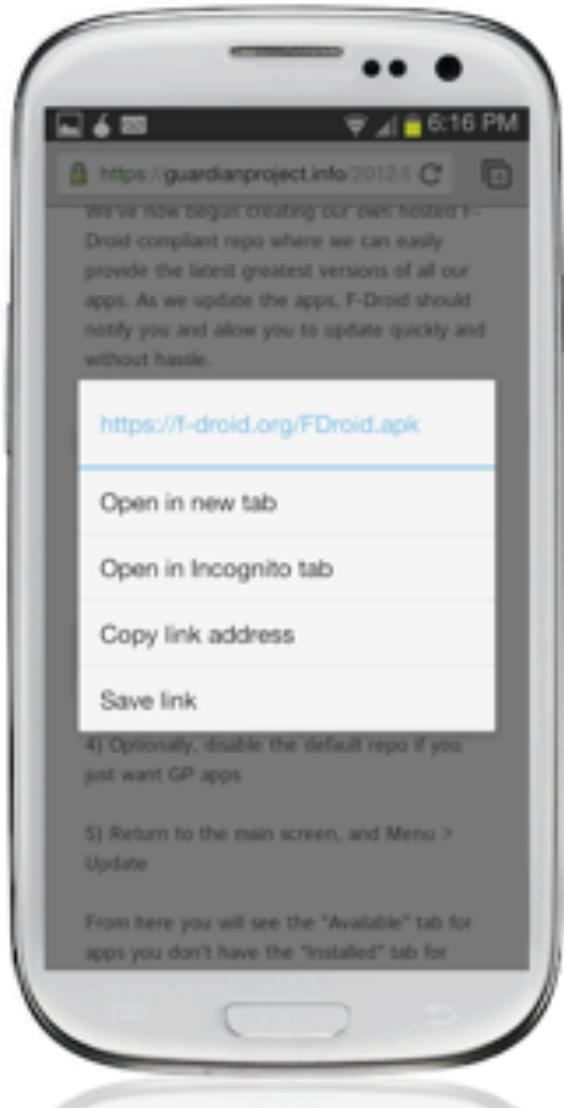
So you want to bypass censorship on Android?

5. Open Orbot. Done.



So you want to bypass censorship on Android?

There's an alternative store. Install F-droid by entering
<https://f-droid.org/FDroid.apk> into the browser. [Done. Next?](#)



So you want to bypass censorship on Android?

Run the app and navigate over to Menu > Manage Repos > New Repository
Cool. What do I enter?



So you want to bypass censorship on Android?

Enter: <https://guardianproject.info/repo/> (don't forget the s!)

[Done. Where are the apps?](#)



So you want to bypass censorship on Android?

Go back to the main screen and you should see the Guardian Project apps.
Click on Orbot to install. [Got it.](#)



So you want to bypass censorship on Android?

Then click on Orweb to install it's partner web browser.

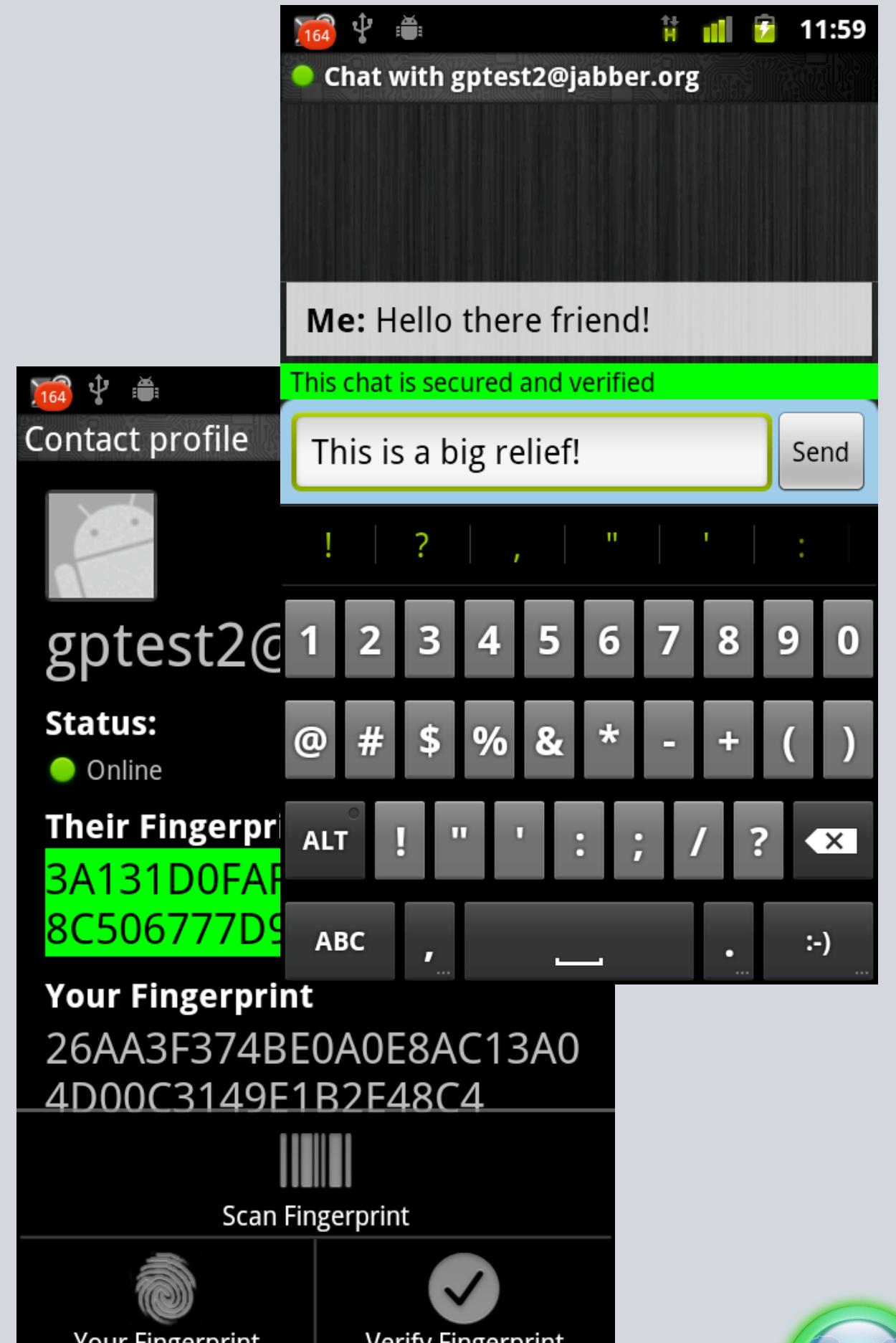
[Got it.](#)



GIBBERBOT

A secure, no-logging instant messaging app for Android, supporting open standard chat and encryption protocols

- Uses industry standard chat encryption scheme (OTR), compatible with Pidgin, Adium, Jitsi and other desktop IM apps
- XMPP protocols enables use with GTalk, Facebook, as well as any self-hosted, secured server
- Can work with Orbot (over Tor) to circumvent firewalls and monitors



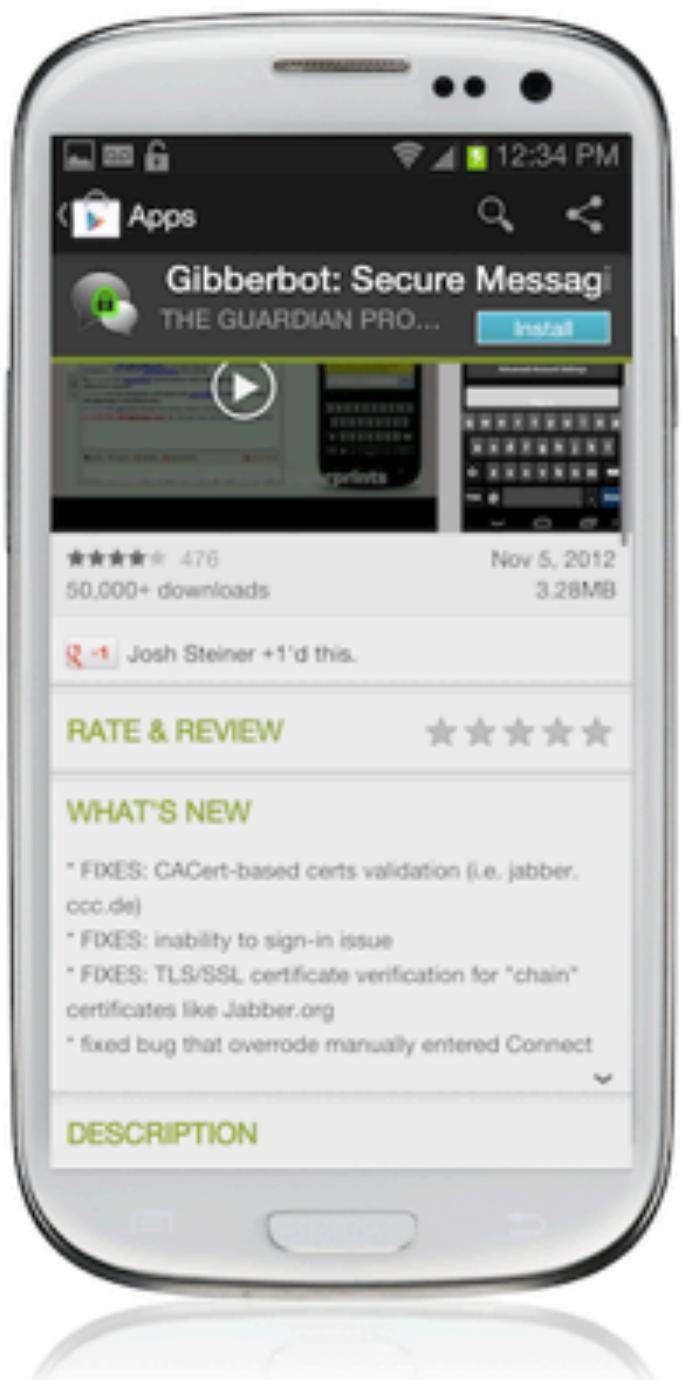
So you want to chat securely on Android?

1. Open the Google Play Store. [Easy. Next?](#)
[It's blocked. Help!](#)



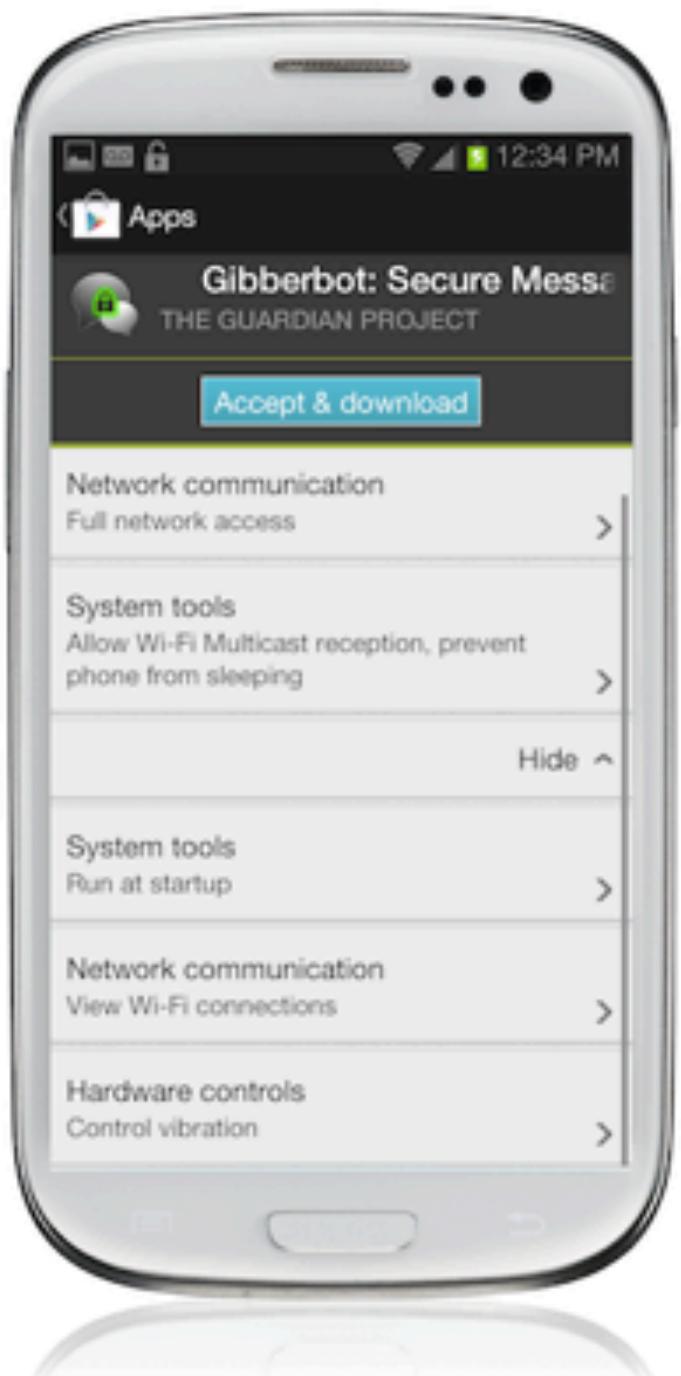
So you want to chat securely on Android?

2. Search for *Gibberbot*. [Got it.](#)



So you want to chat securely on Android?

3. Review the permissions. Then, maybe, accept them. OK, I trust you.



So you want to chat securely on Android?

4. Open Gibberbot. Done.



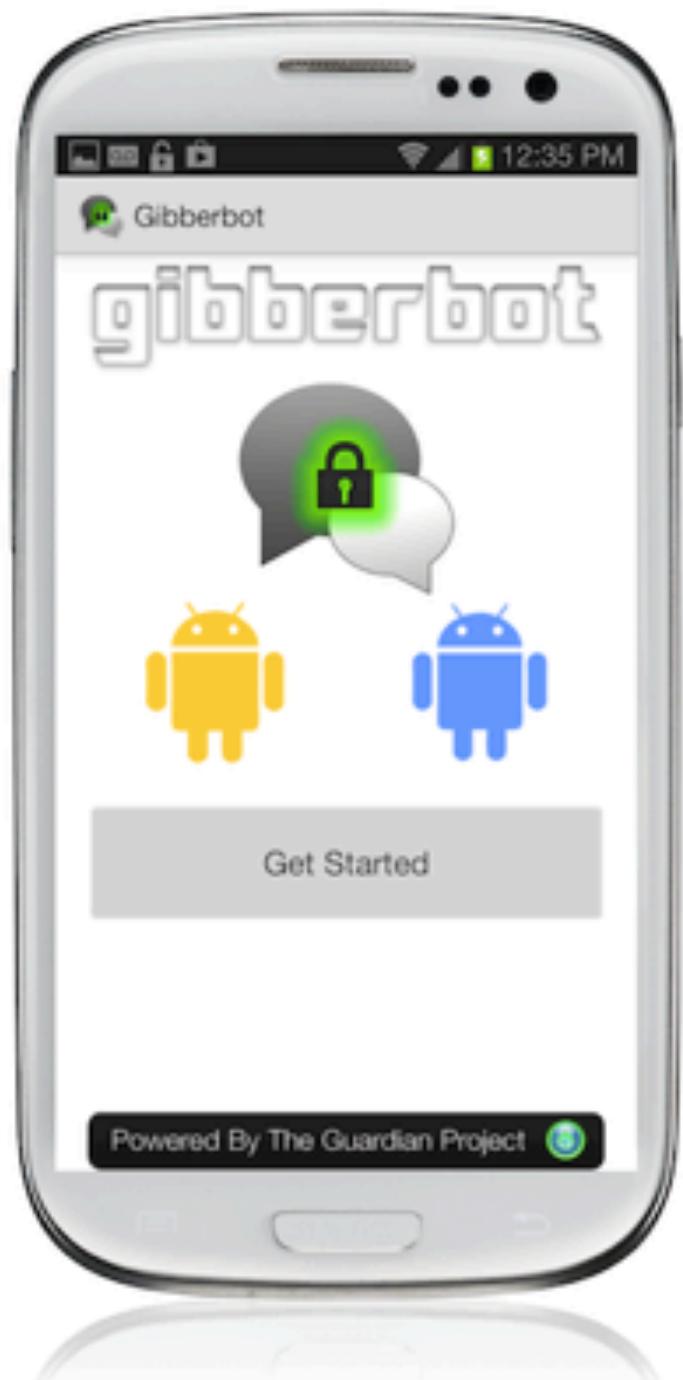
So you want to chat securely on Android?

5. Choose your language and get started. [Let's go with English.](#)



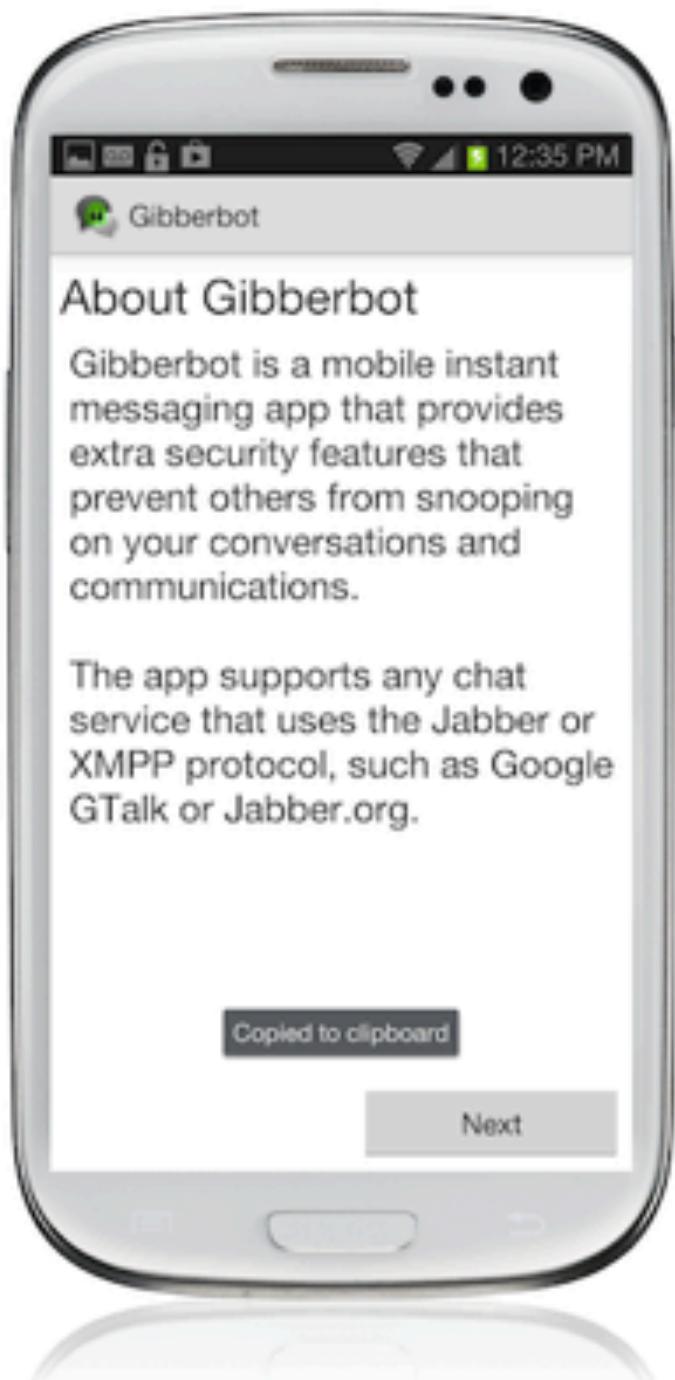
So you want to chat securely on Android?

Now we're getting started.



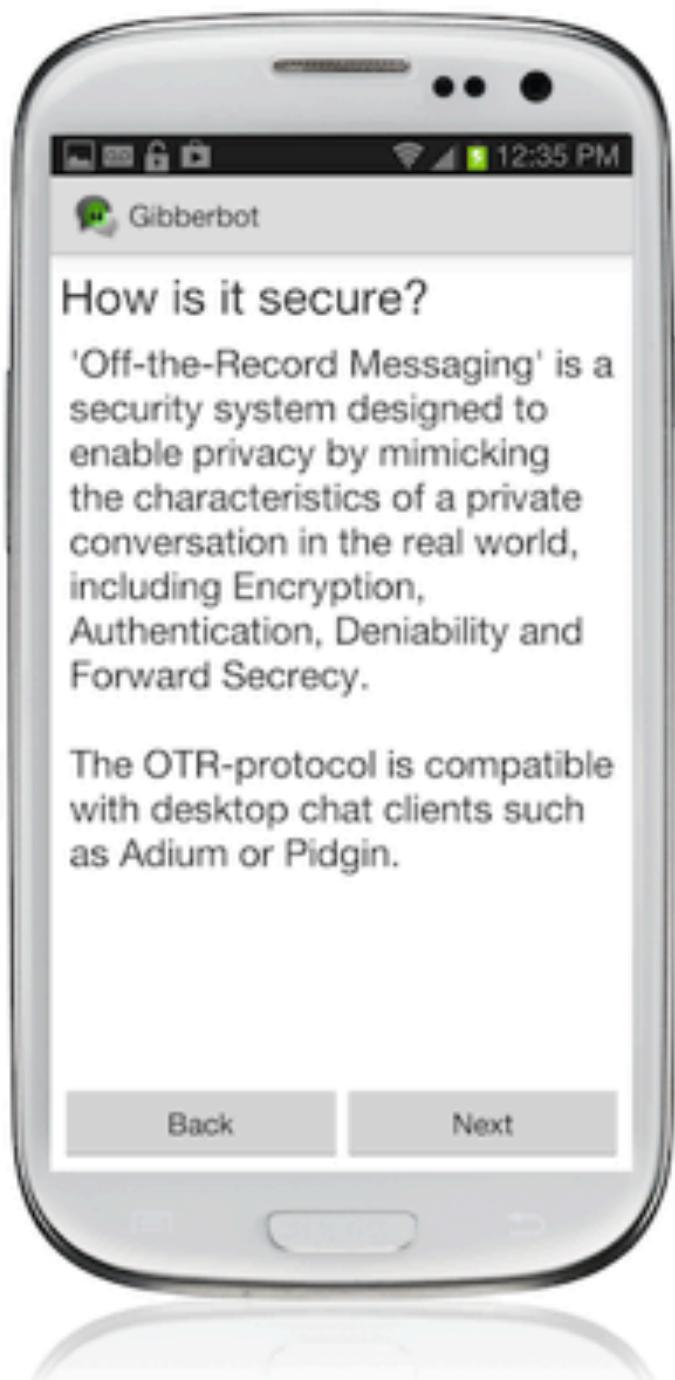
So you want to chat securely on Android?

It will tell you about our project.



So you want to chat securely on Android?

Is it really secure? We break it down.



So you want to chat securely on Android?

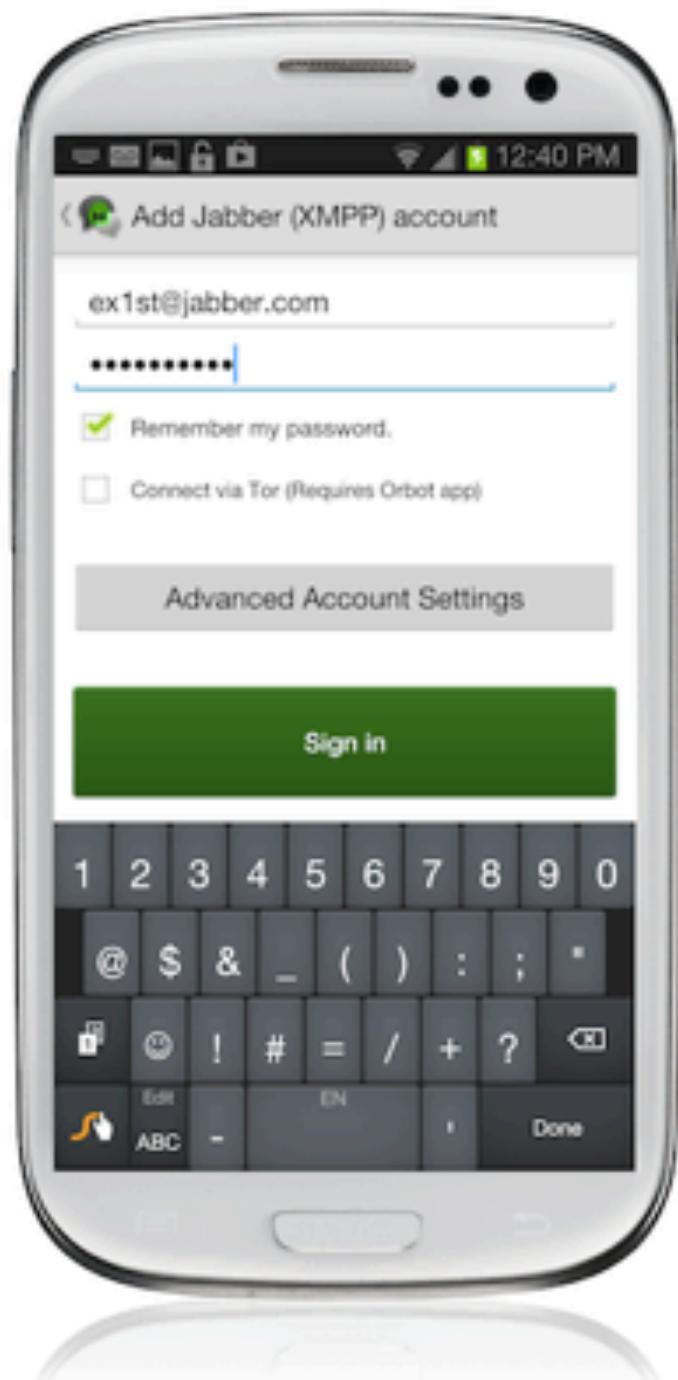
Security is a two way street. Make sure your friends are secure too.



So you want to chat securely on Android?

6. Enter your account info: Gchat, Facebook, DukGo, & XMPP all work.

All set!



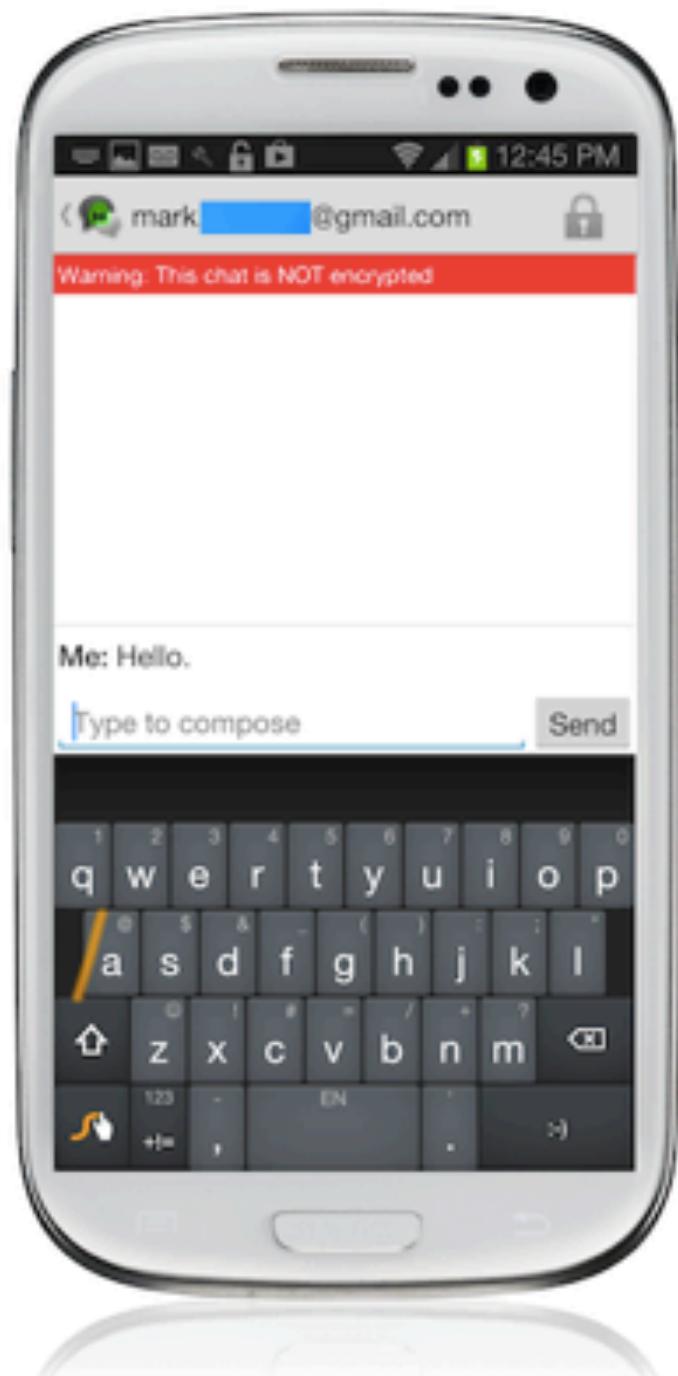
So you want to chat securely on Android?

7. We're in! There's my buddy list. Let's message my friend Mark.



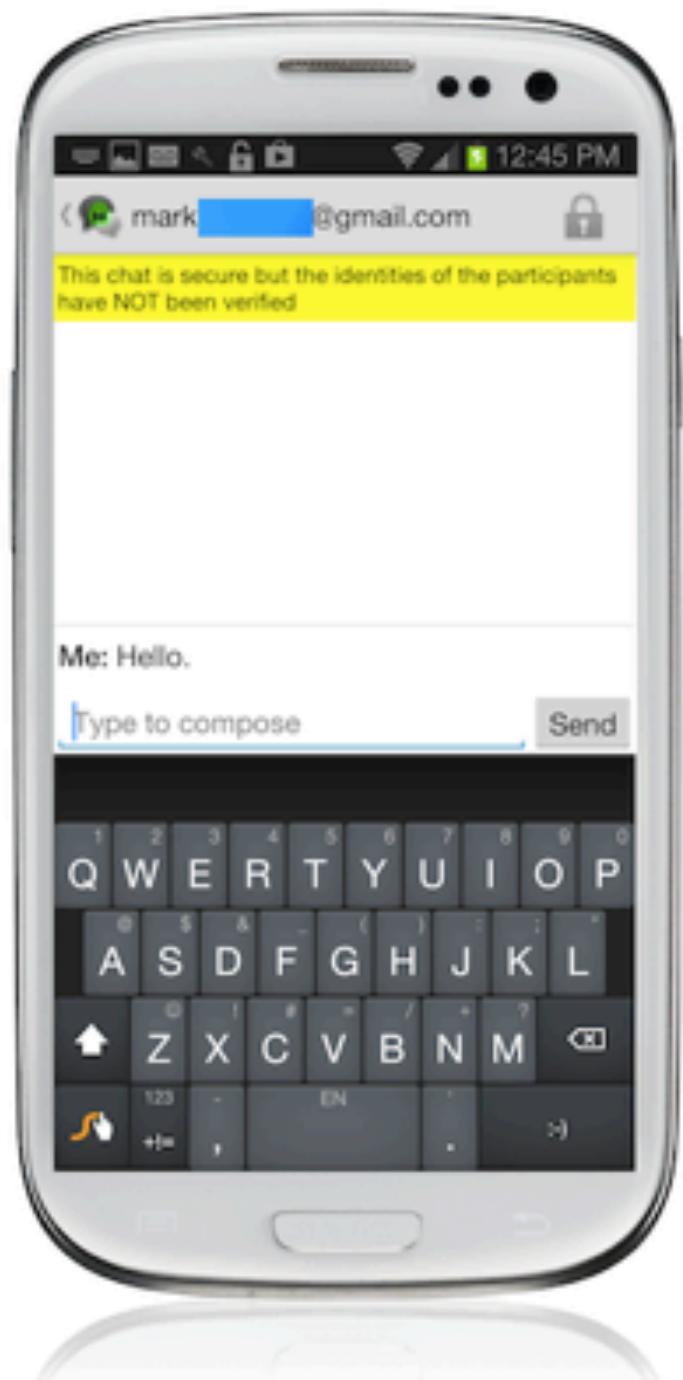
So you want to chat securely on Android?

Uh oh! It's red, so not encrypted yet. Let's wait to see if Mark turns on encryption.



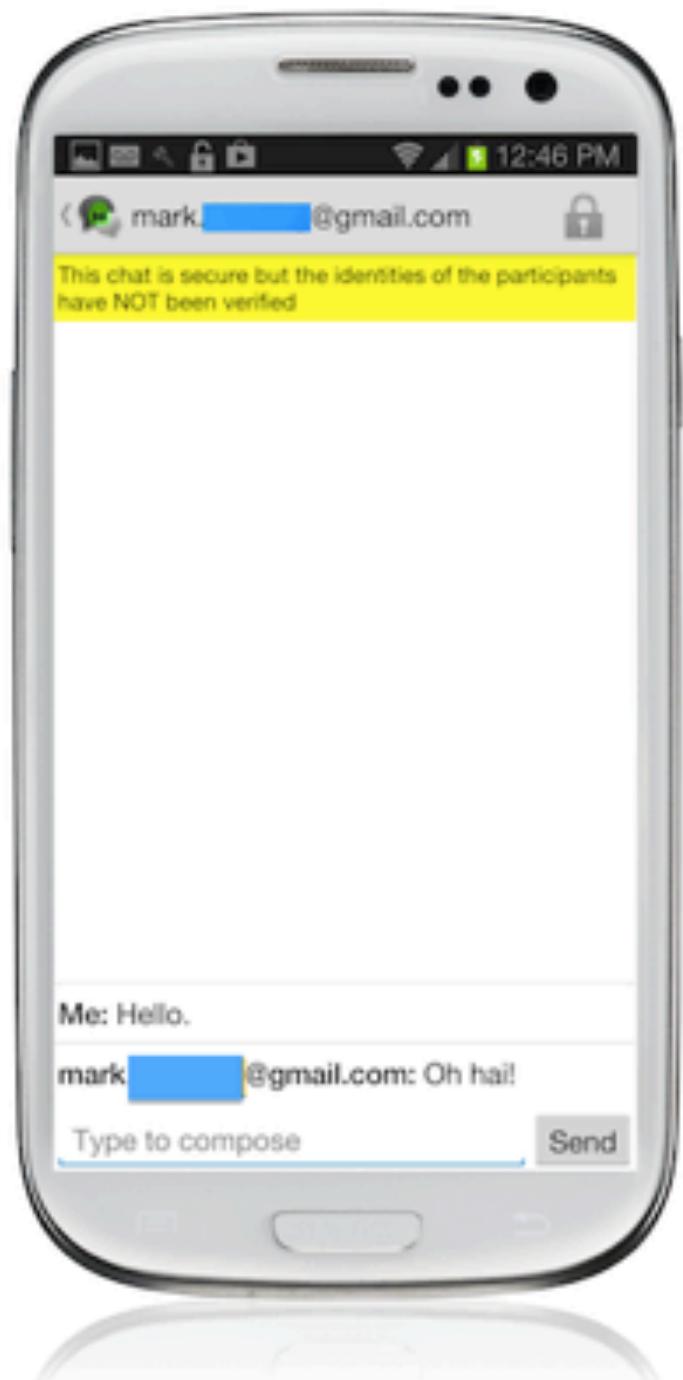
So you want to chat securely on Android?

8. The bar turned yellow! Mark got our chat & turned on encryption.
[Let's verify it's really Mark.](#)



So you want to chat securely on Android?

9. Let's send him an unencrypted message. [Send "Oh hai!"](#)



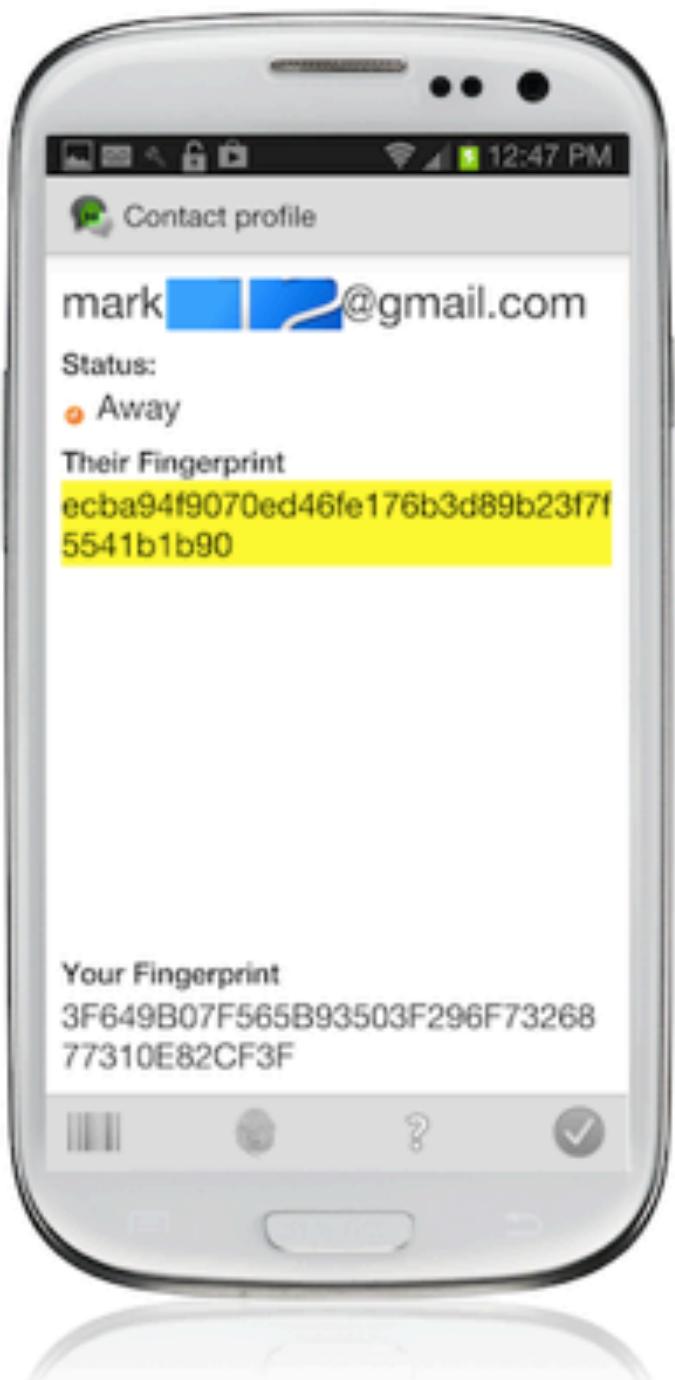
So you want to chat securely on Android?

10. Is that really Mark? Pull up the verify option. [Let's click it to make sure.](#)



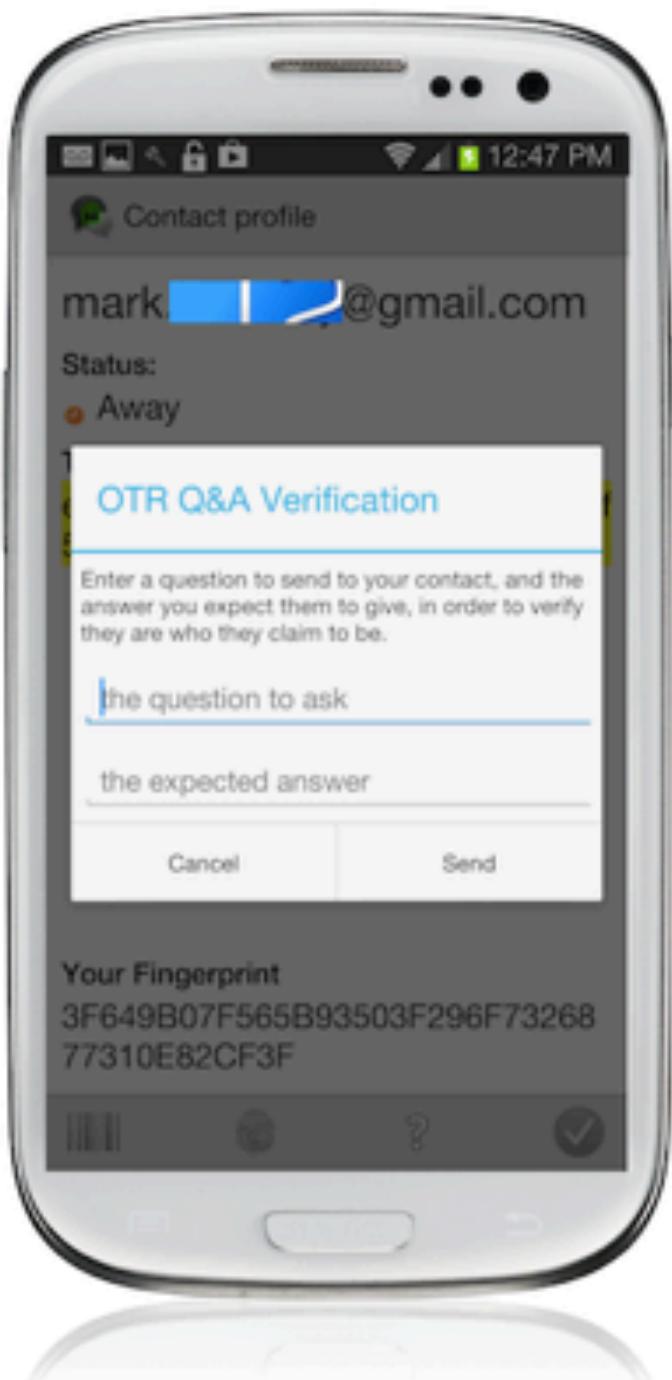
So you want to chat securely on Android?

I can see Mark's fingerprint. Now let me send him a message that only you would know the answer to.



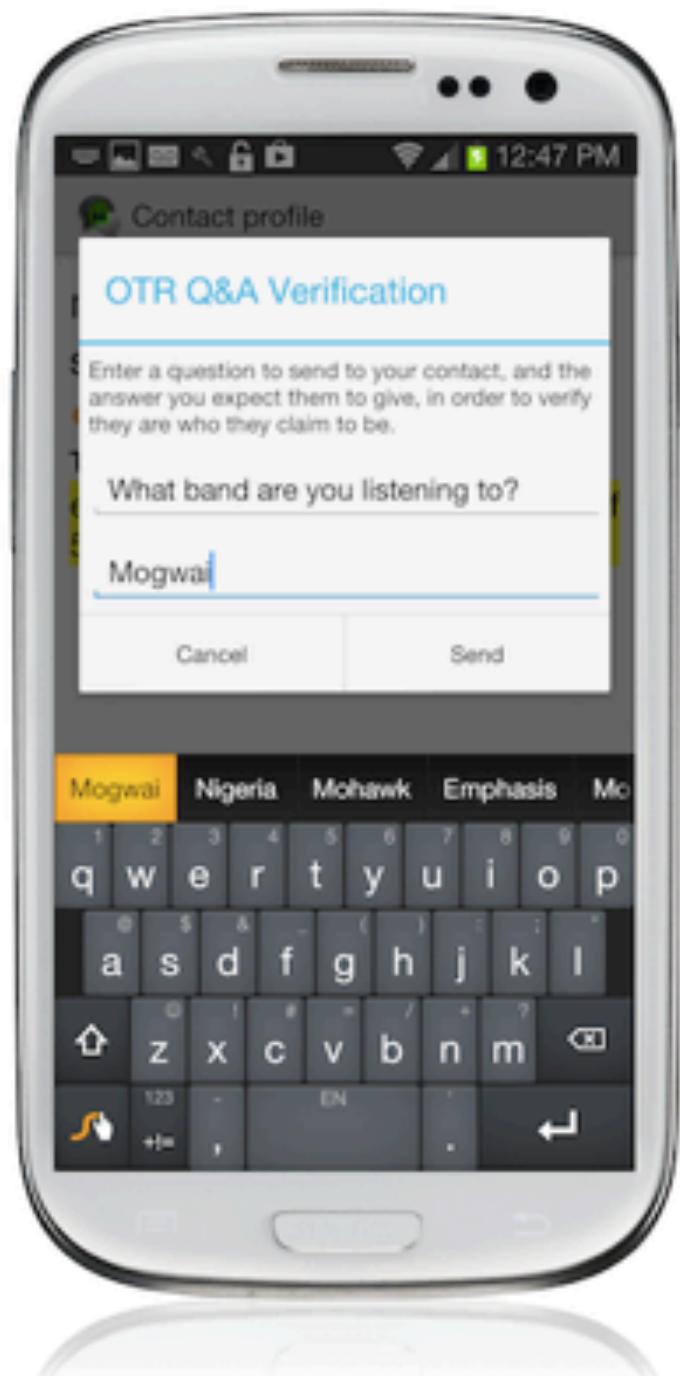
So you want to chat securely on Android?

I'm thinking of a question...



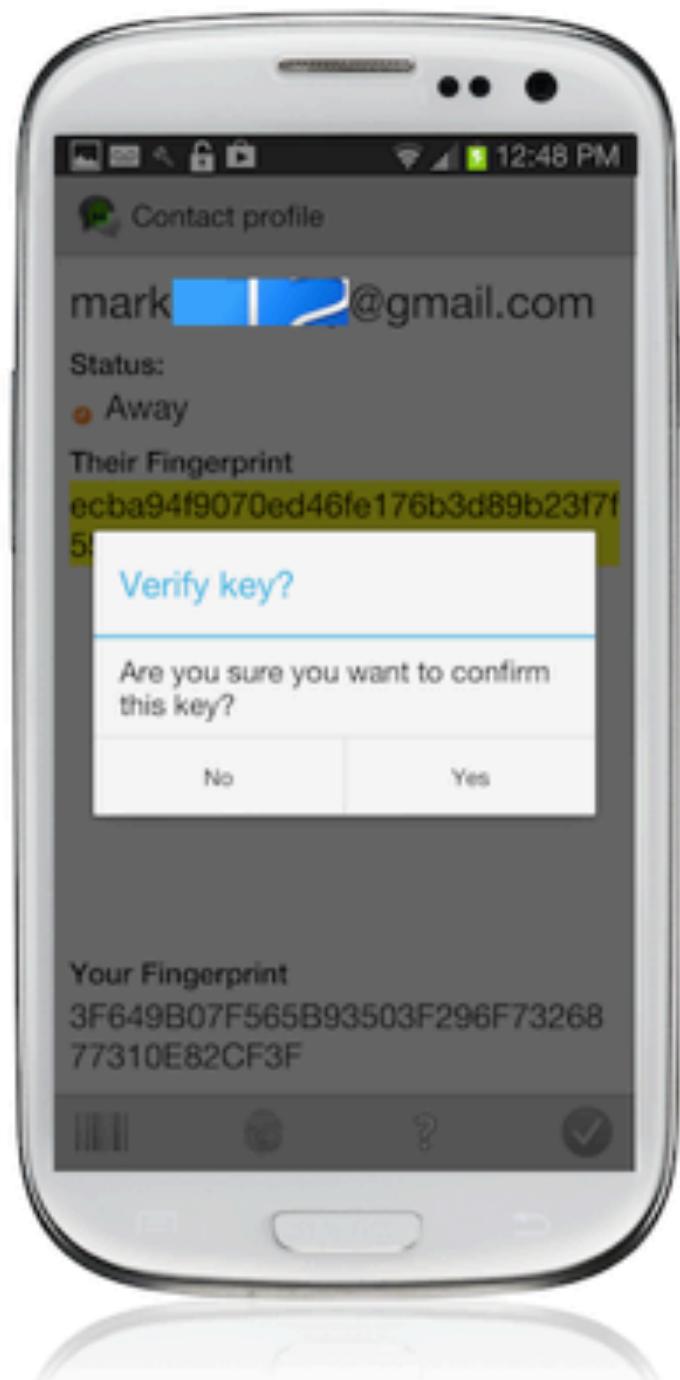
So you want to chat securely on Android?

Got it! I checked on a trusted channel: Spotify. [Send the secret.](#)



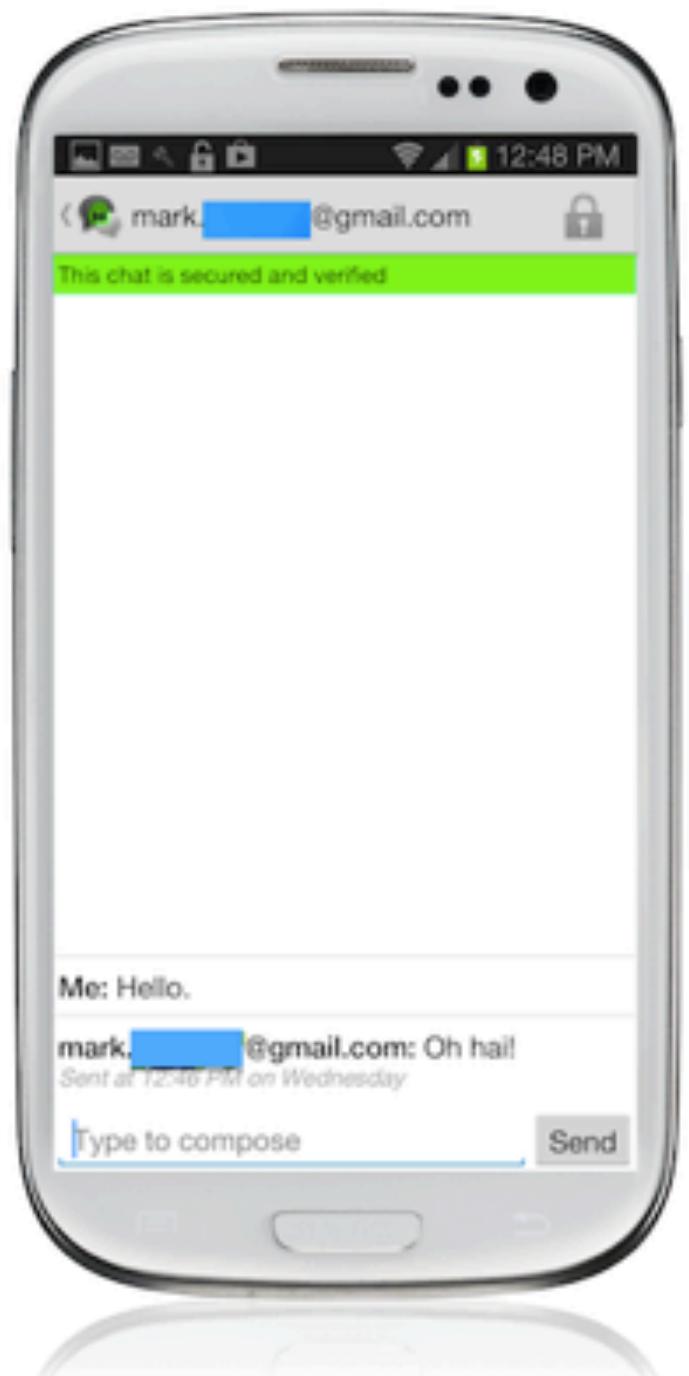
So you want to chat securely on Android?

Mark got the right answer! Well then, let's confirm it's really him.



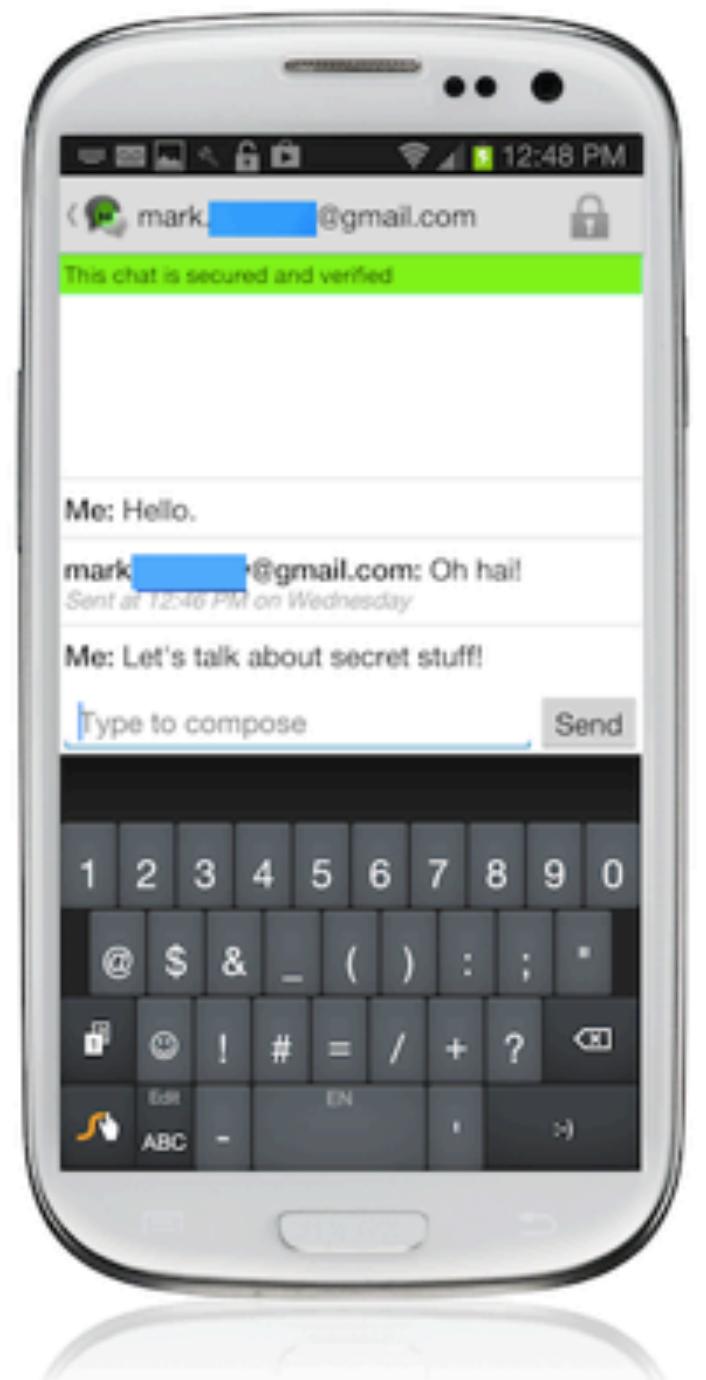
So you want to chat securely on Android?

10. The bar turned green! We're secure.
Let's send him an encrypted message.



So you want to chat securely on Android?

You're awesome! [Play it again?](#)
For more info, visit [The Guardian Project](#)



So you want to chat securely on Android?

1. Open the Google Play Store. [Easy. Next?](#)
[It's blocked. Help!](#)



So you want to chat securely on Android?

There's an alternative store. Install F-droid by entering
<https://f-droid.org/FDroid.apk> into the browser. [Done. Next?](#)



So you want to chat securely on Android?

Run the app and navigate over to Menu > Manage Repos > New Repository
Cool. What do I enter?



So you want to chat securely on Android?

Enter: <https://guardianproject.info/repo/> (don't forget the s!)

[Done. Where are the apps?](#)



So you want to chat securely on Android?

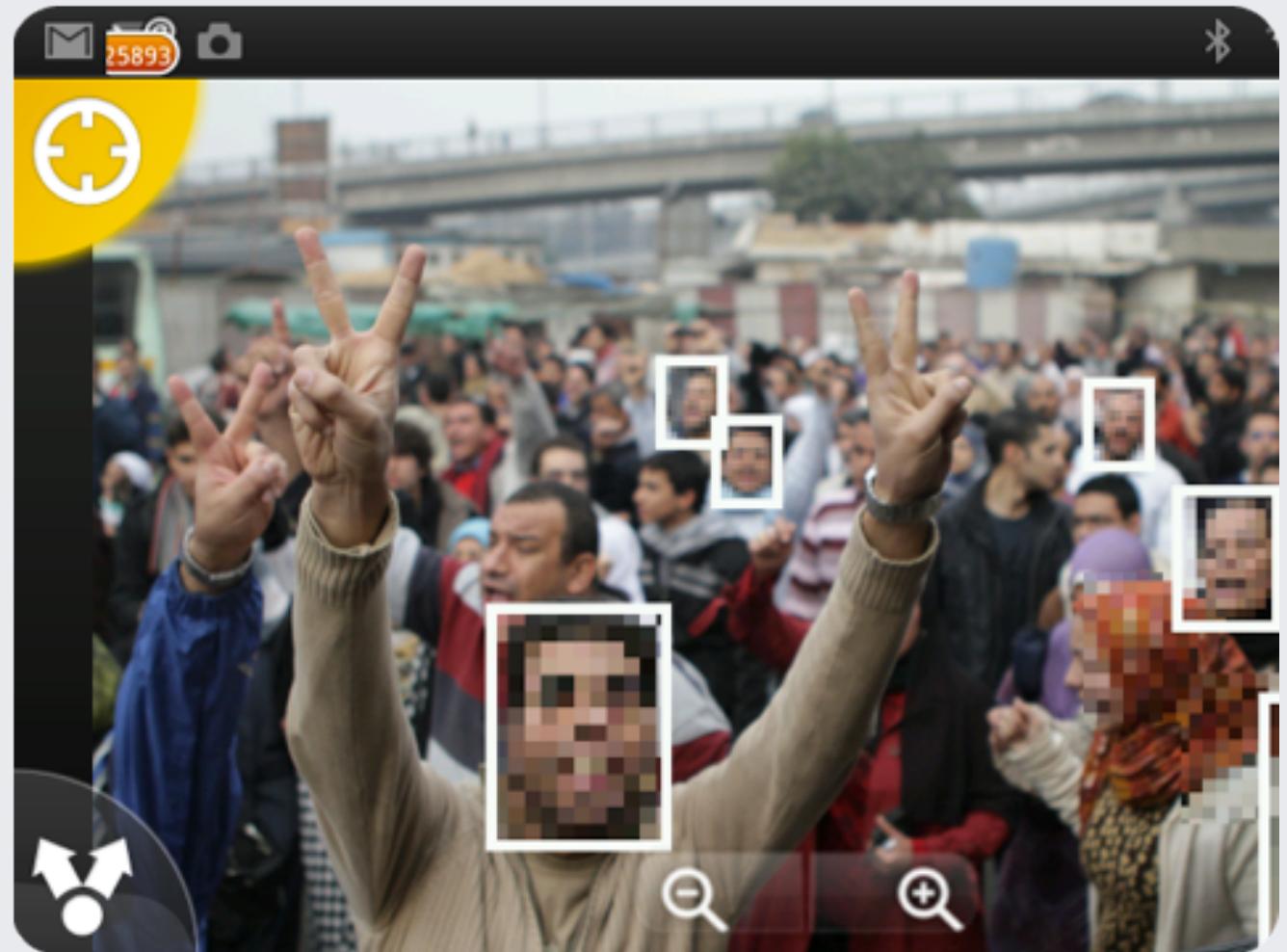
Go back to the main screen and you should see the Guardian Project apps.

Click on *Gibberbot* to install. [Got it.](#)



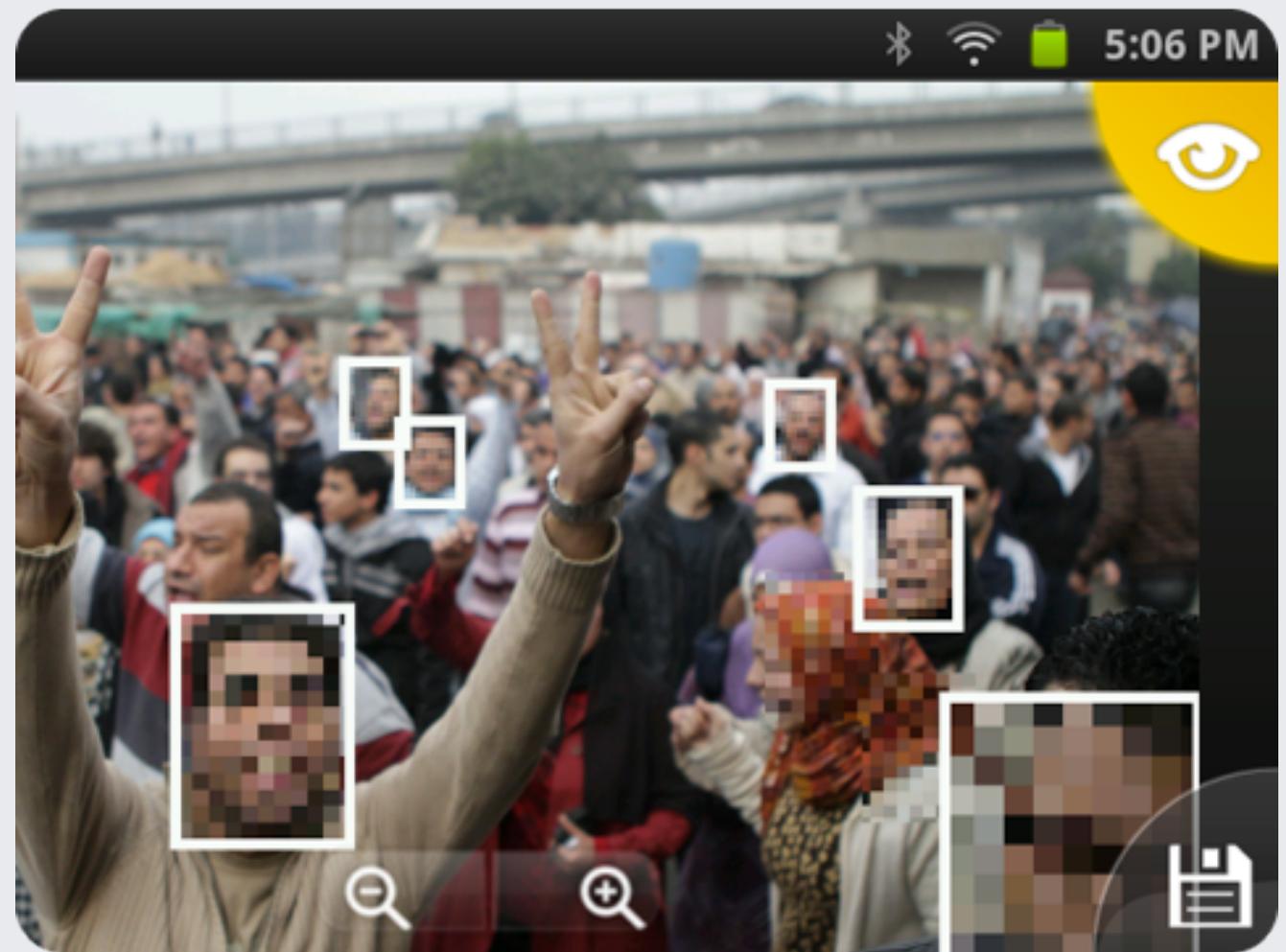
CREATE NEW REGION

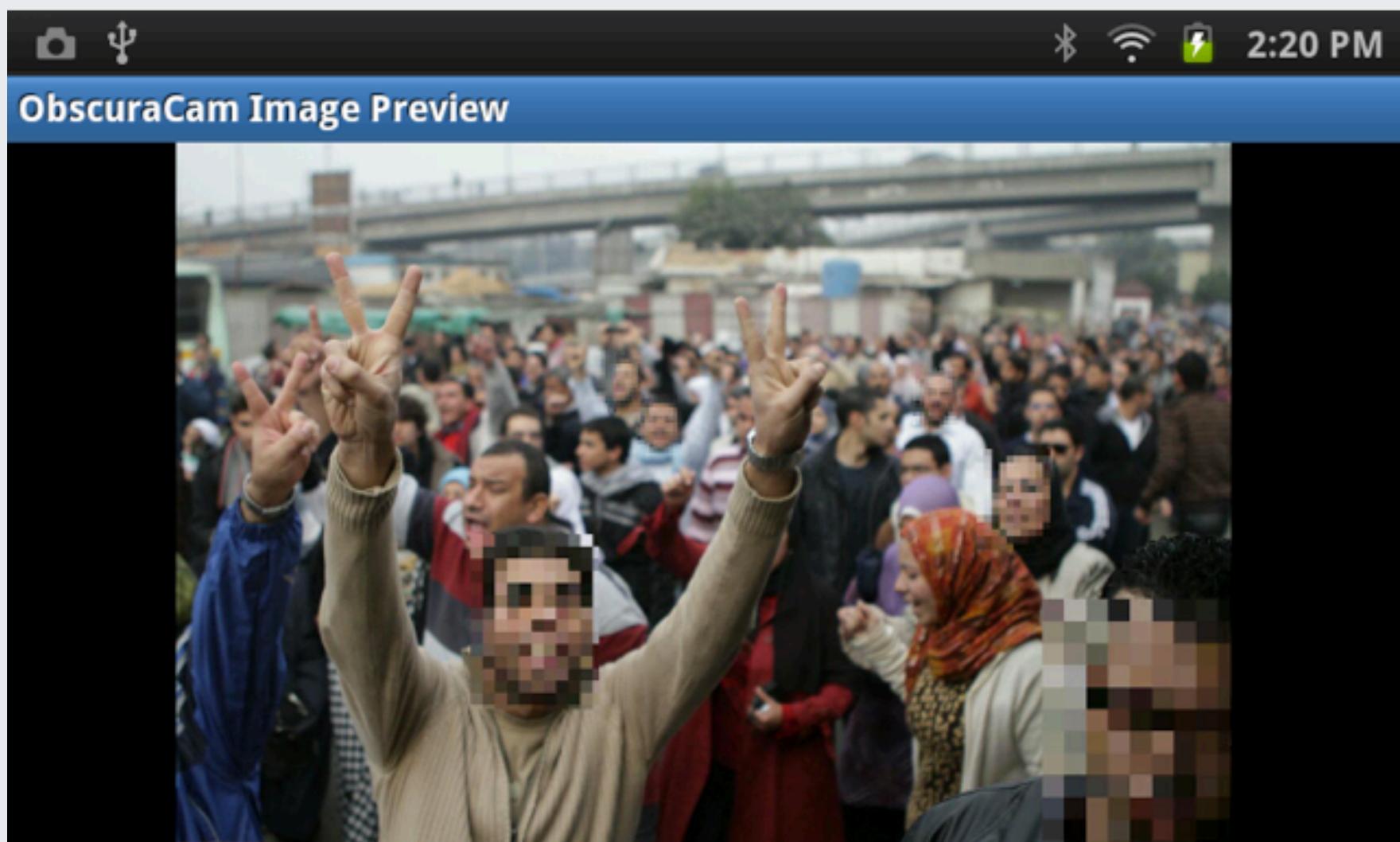
- Tap on the icon in the upper left corner
- Alternately you can tap on the screen to create a new region



PREVIEW

- Tap the icon in the upper right corner

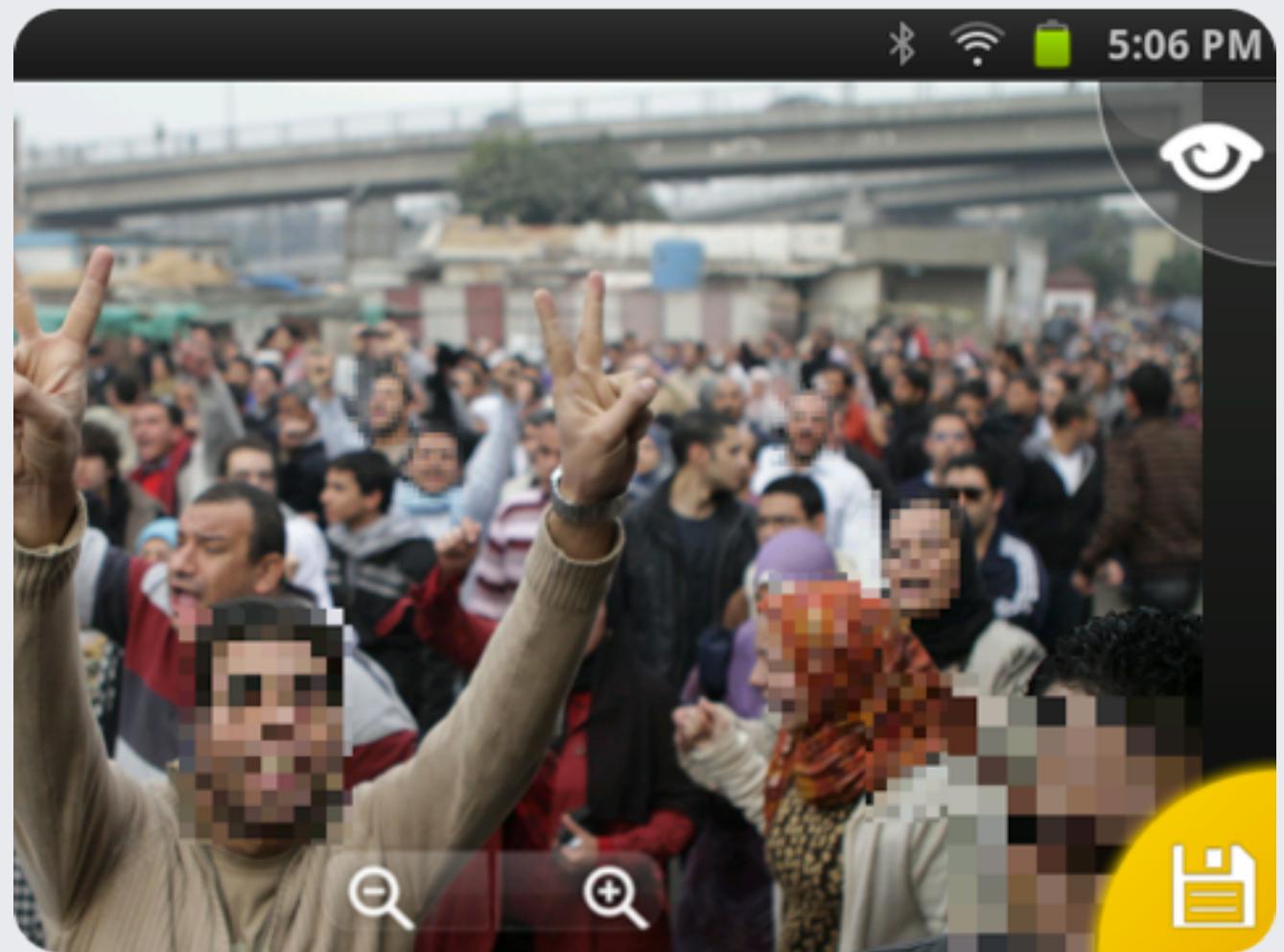




PREVIEW

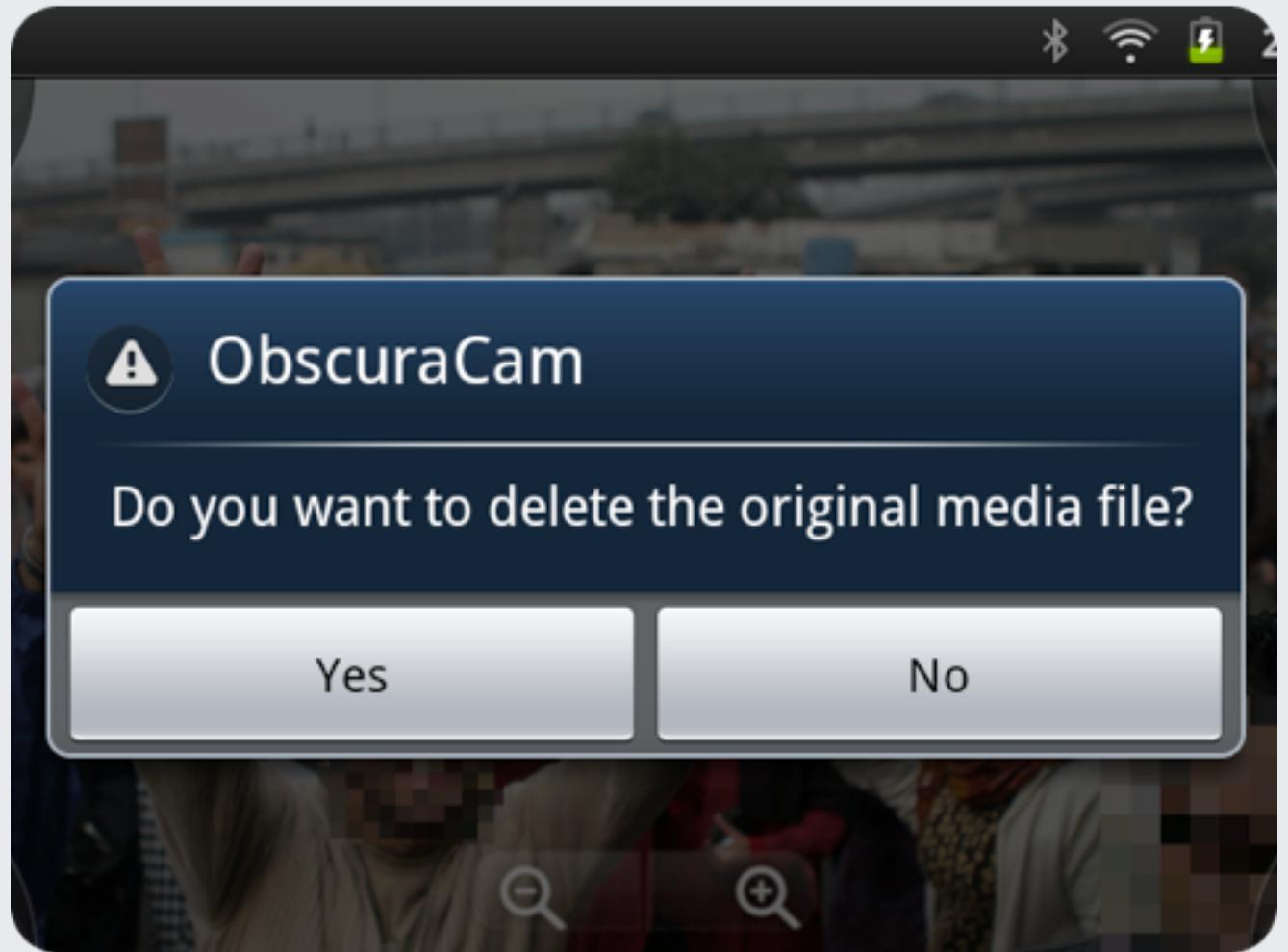
SAVE

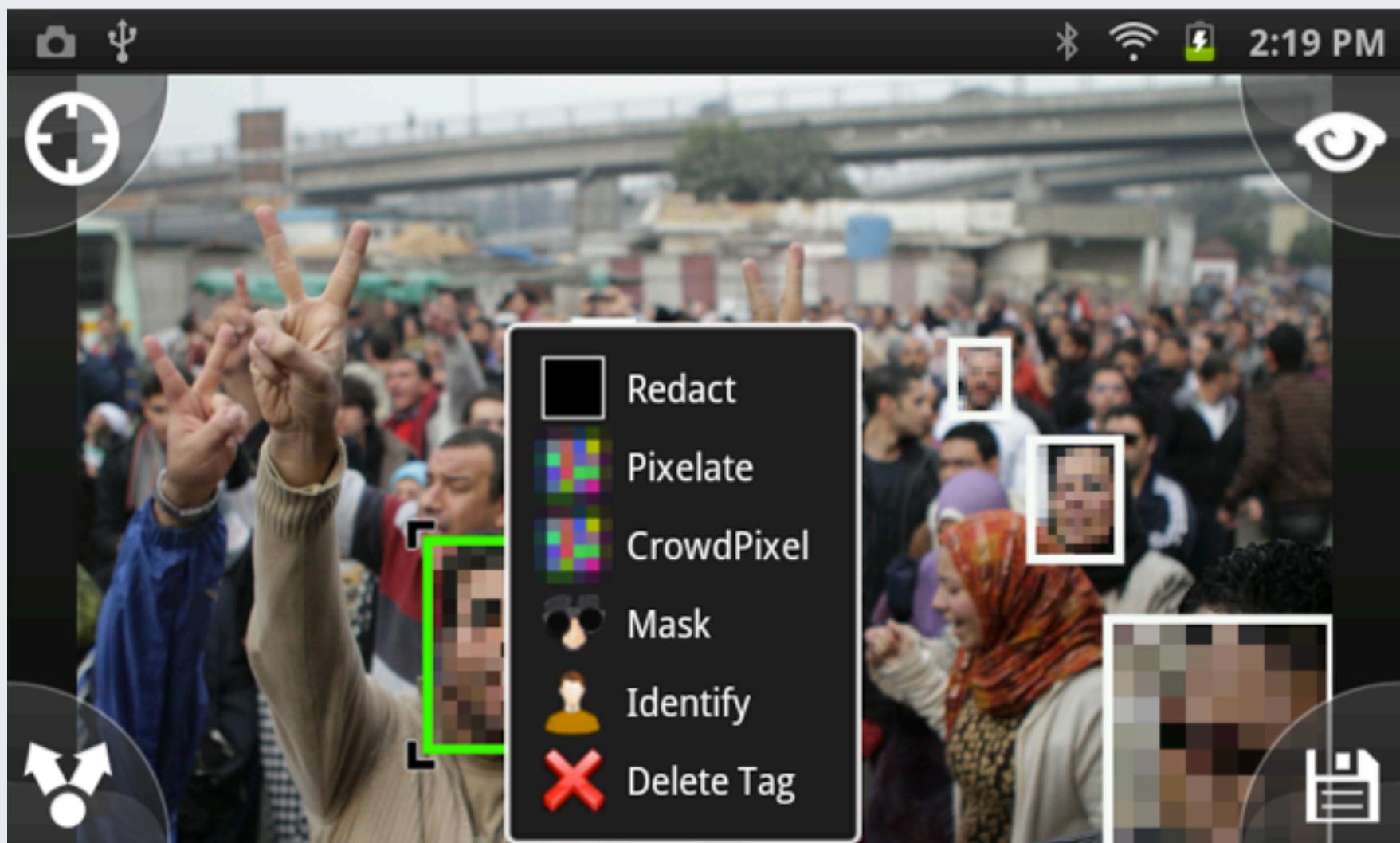
- Tap on the icon in lower right corner



SAVE

- Select option to save or delete original

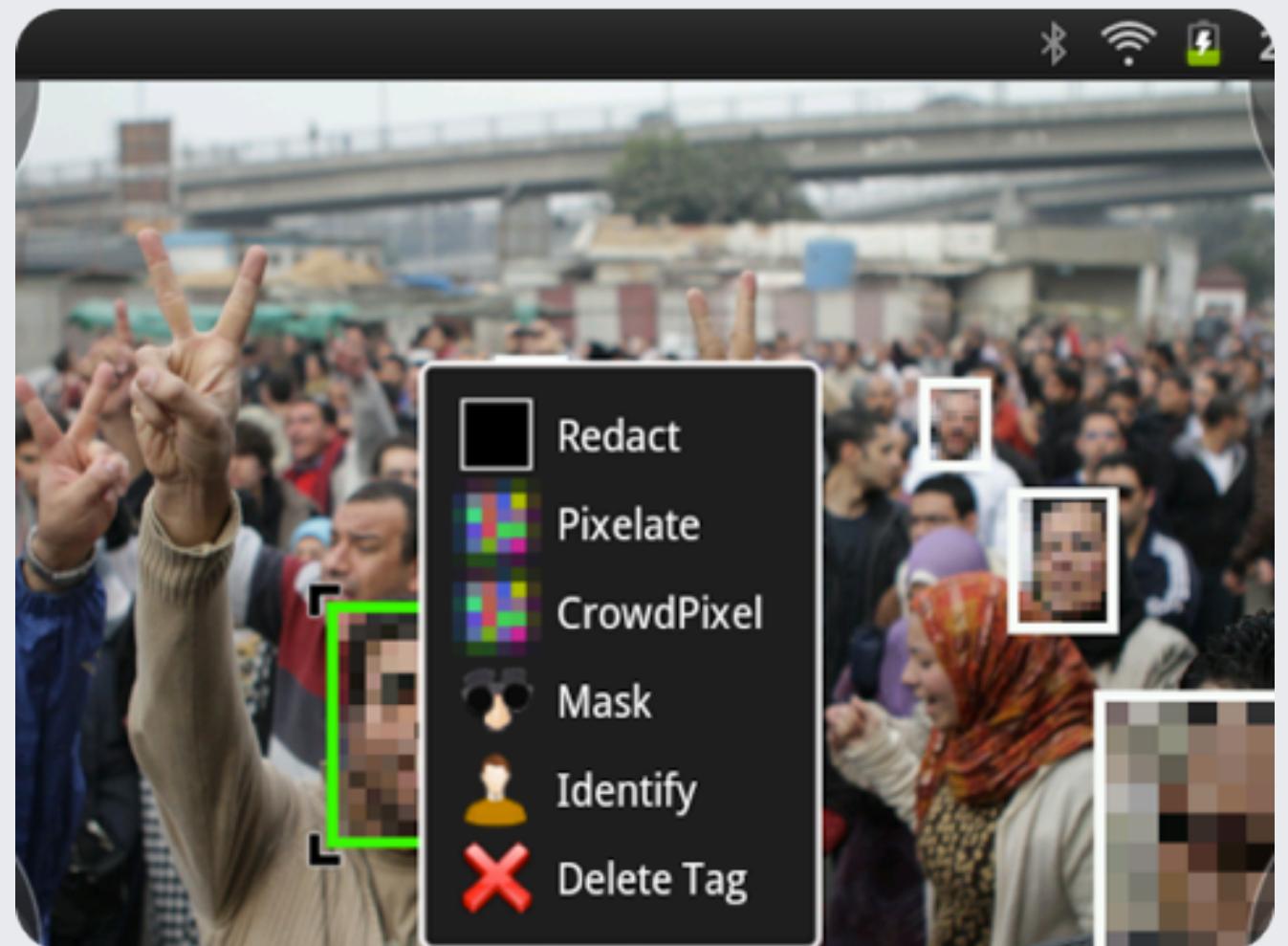




EDIT MENU

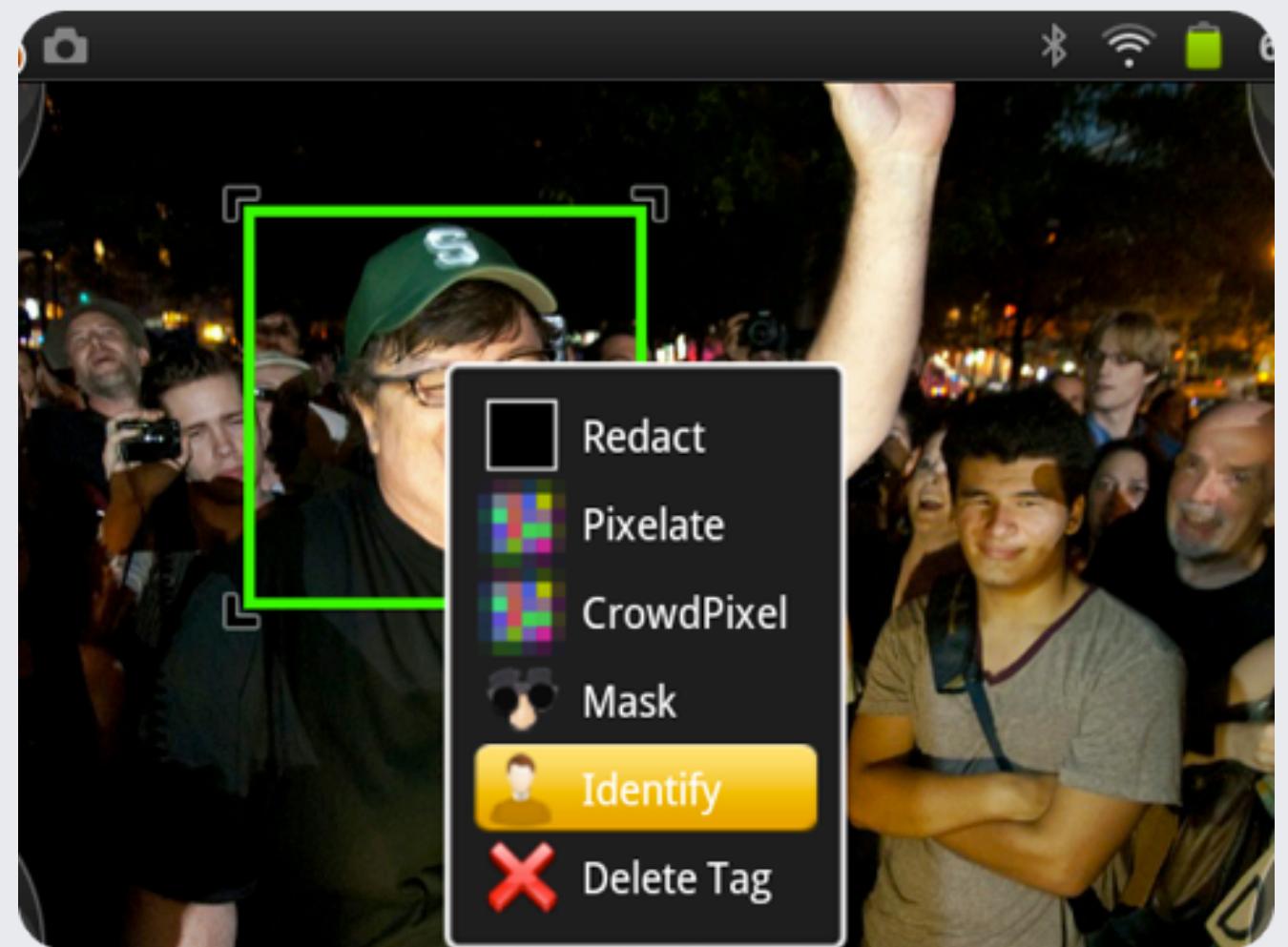
EDIT MENU

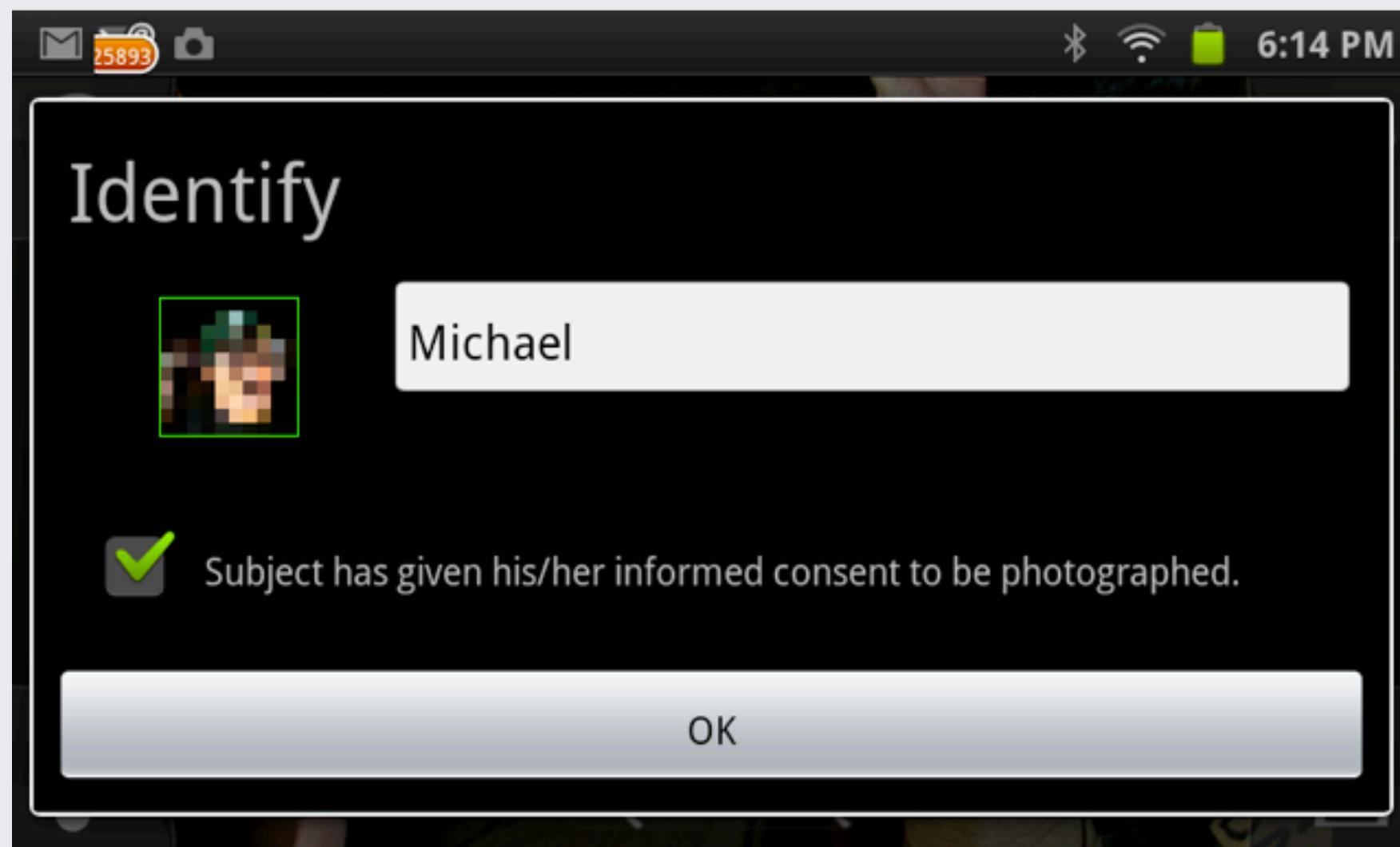
- Redact: Remove completely
- Pixelate: Blur
- CrowdPixel: Blur all but the region
- Identify: Add name and other info
- Delete Tag



IDENTIFY

- Tap region you wish to identify
- Select the Identify option in the popup menu

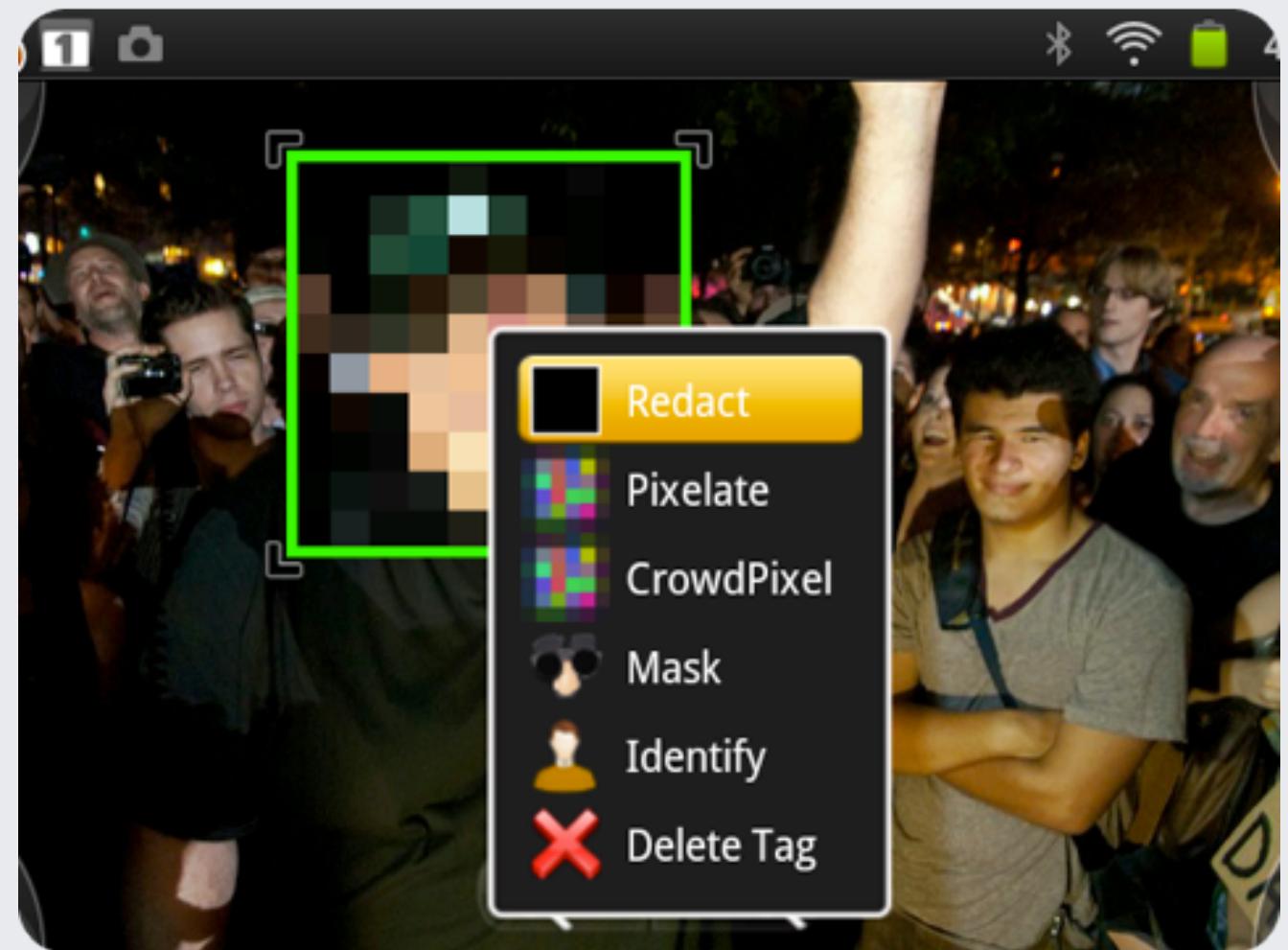




IDENTIFY

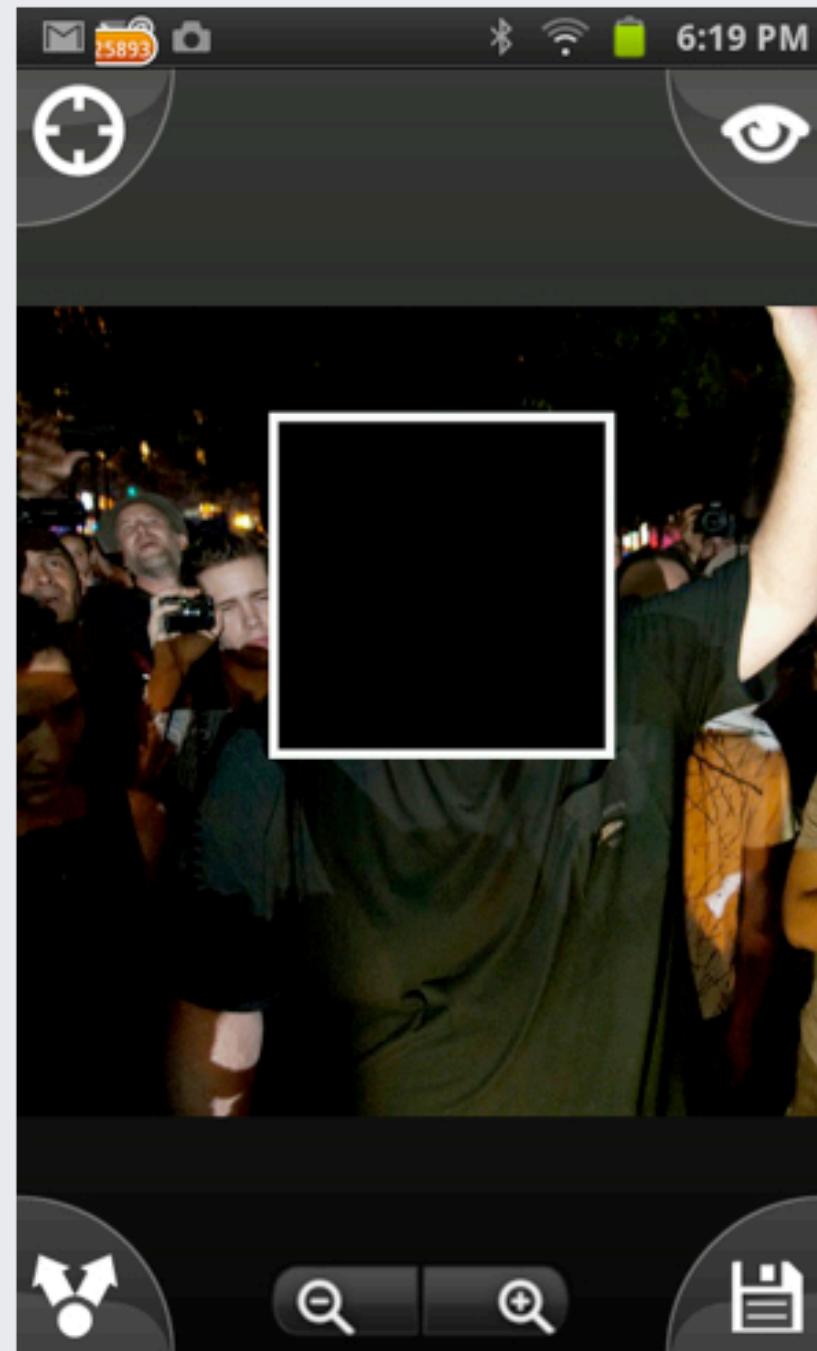
REDACT

- From the edit menu select Redact



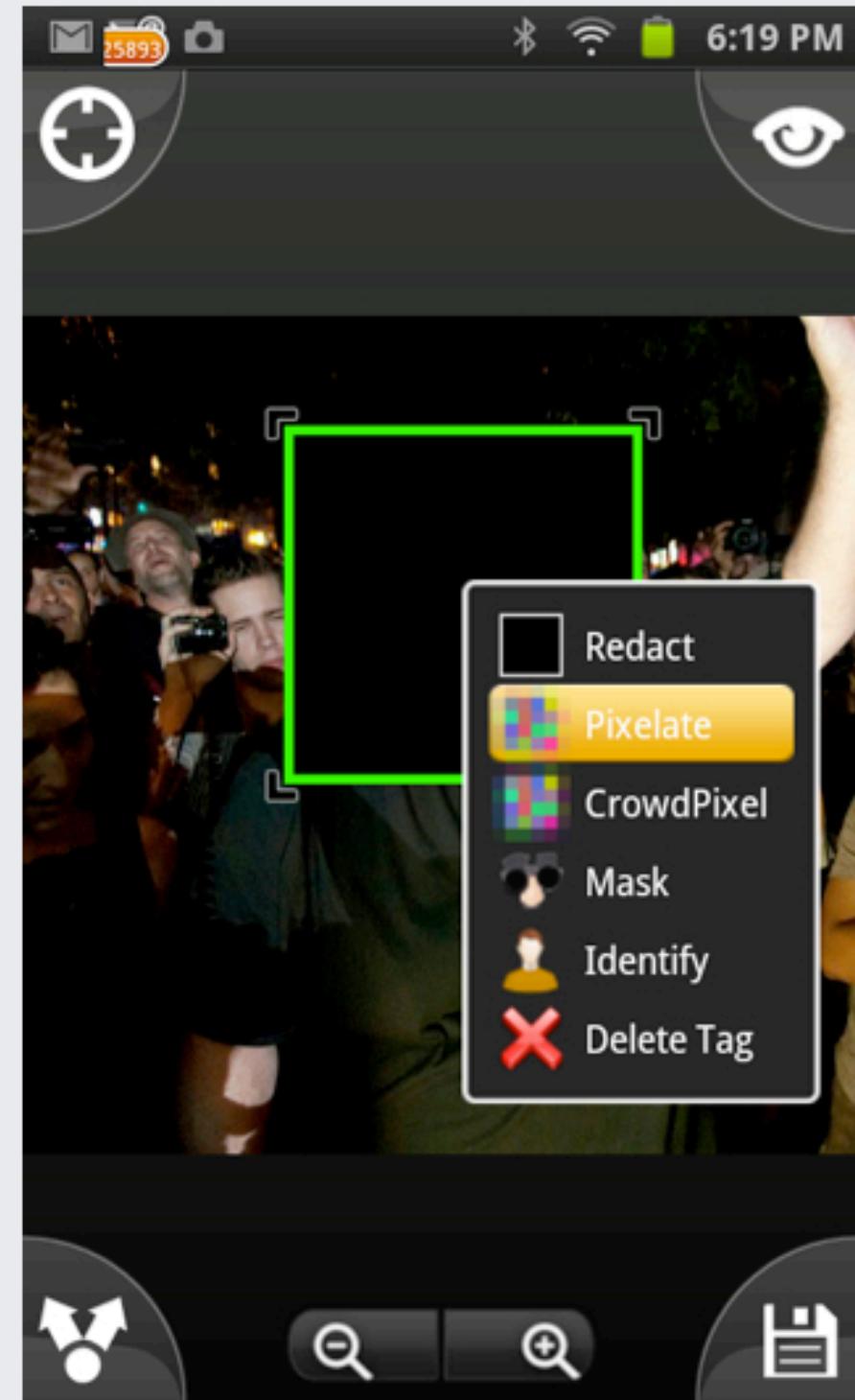
REDACT

- The selected region will be completely removed



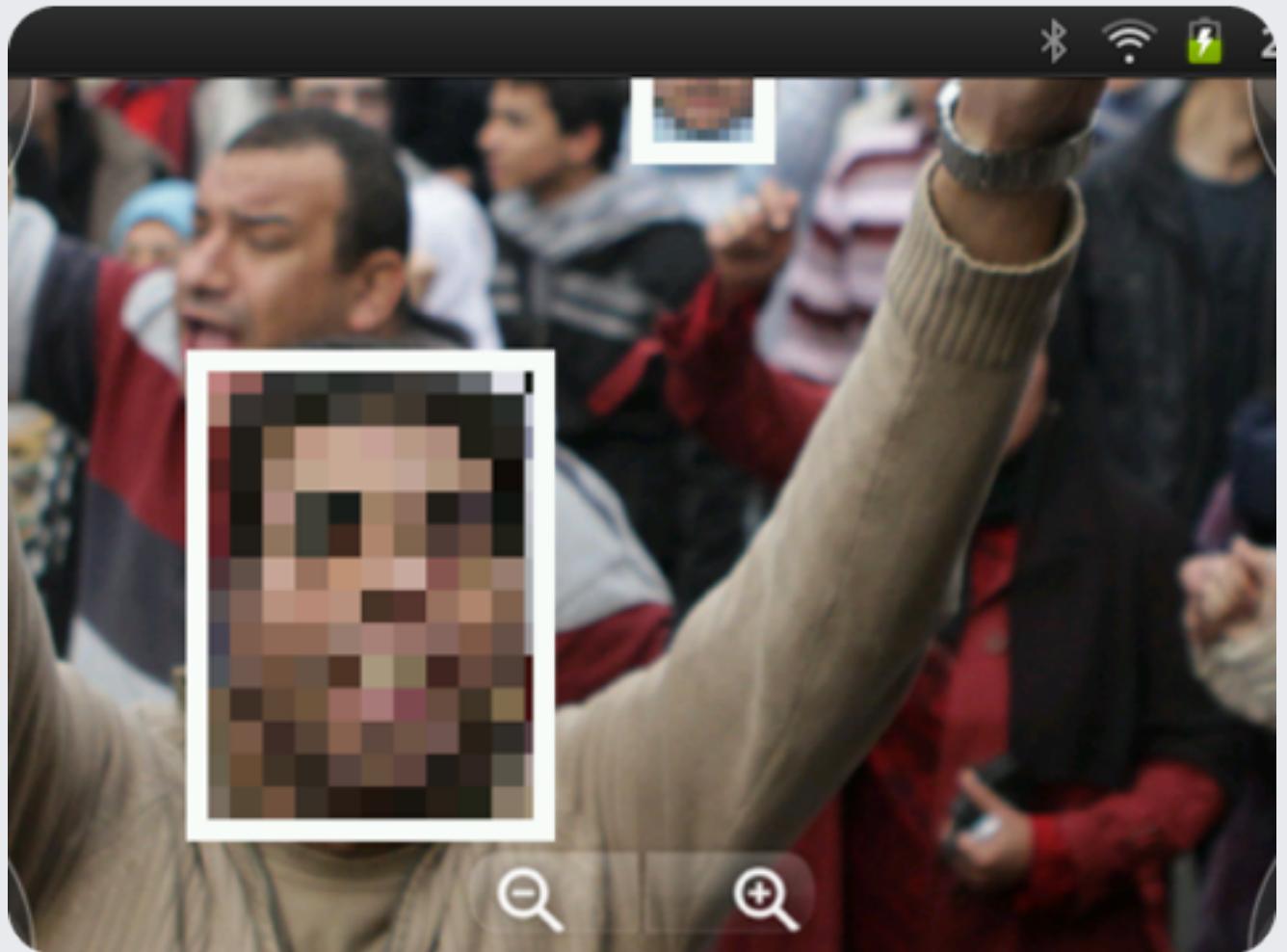
PIXELATE

- From the edit menu select Pixelate



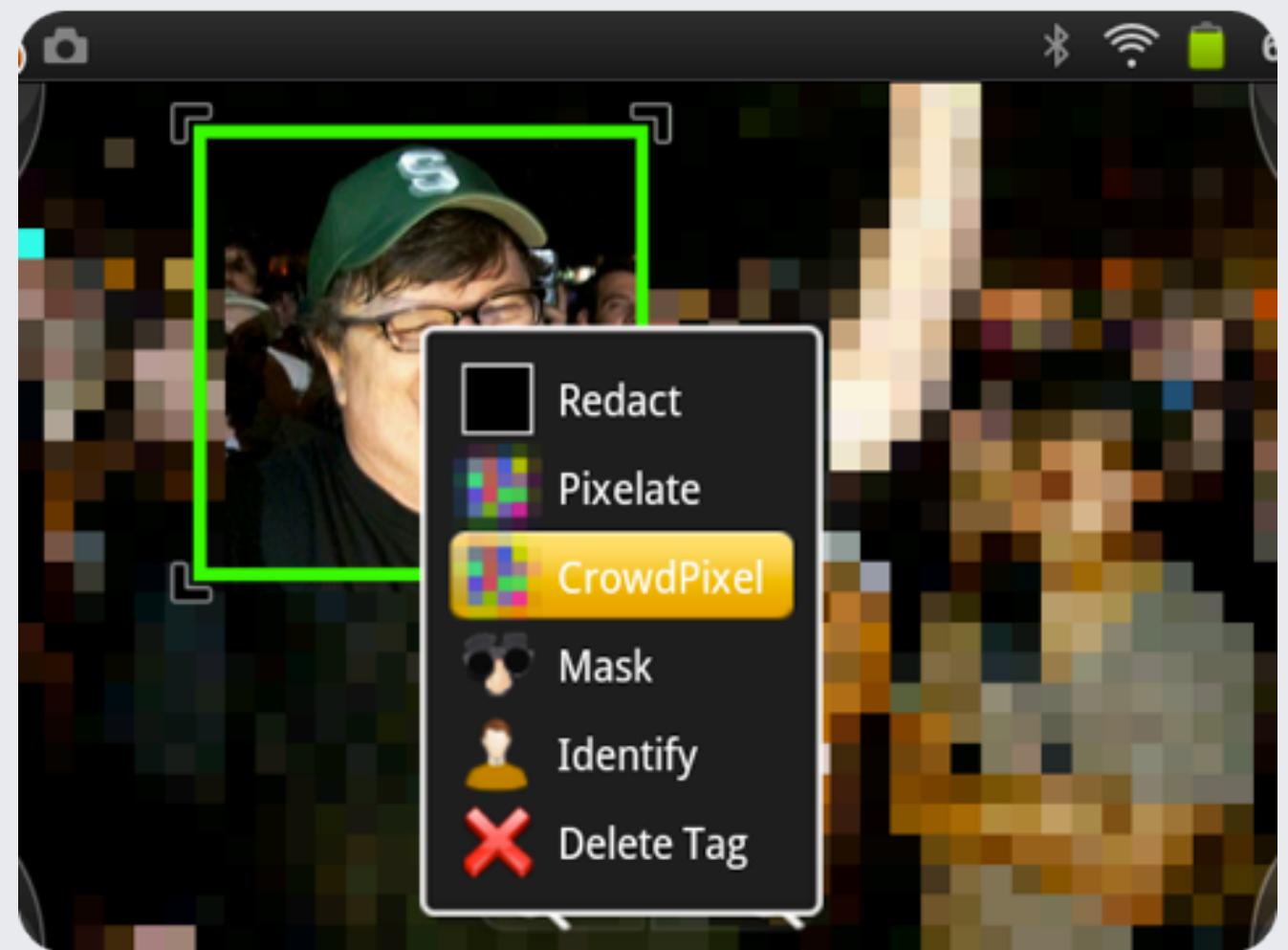
PIXELATE

- The selected region will be pixelated



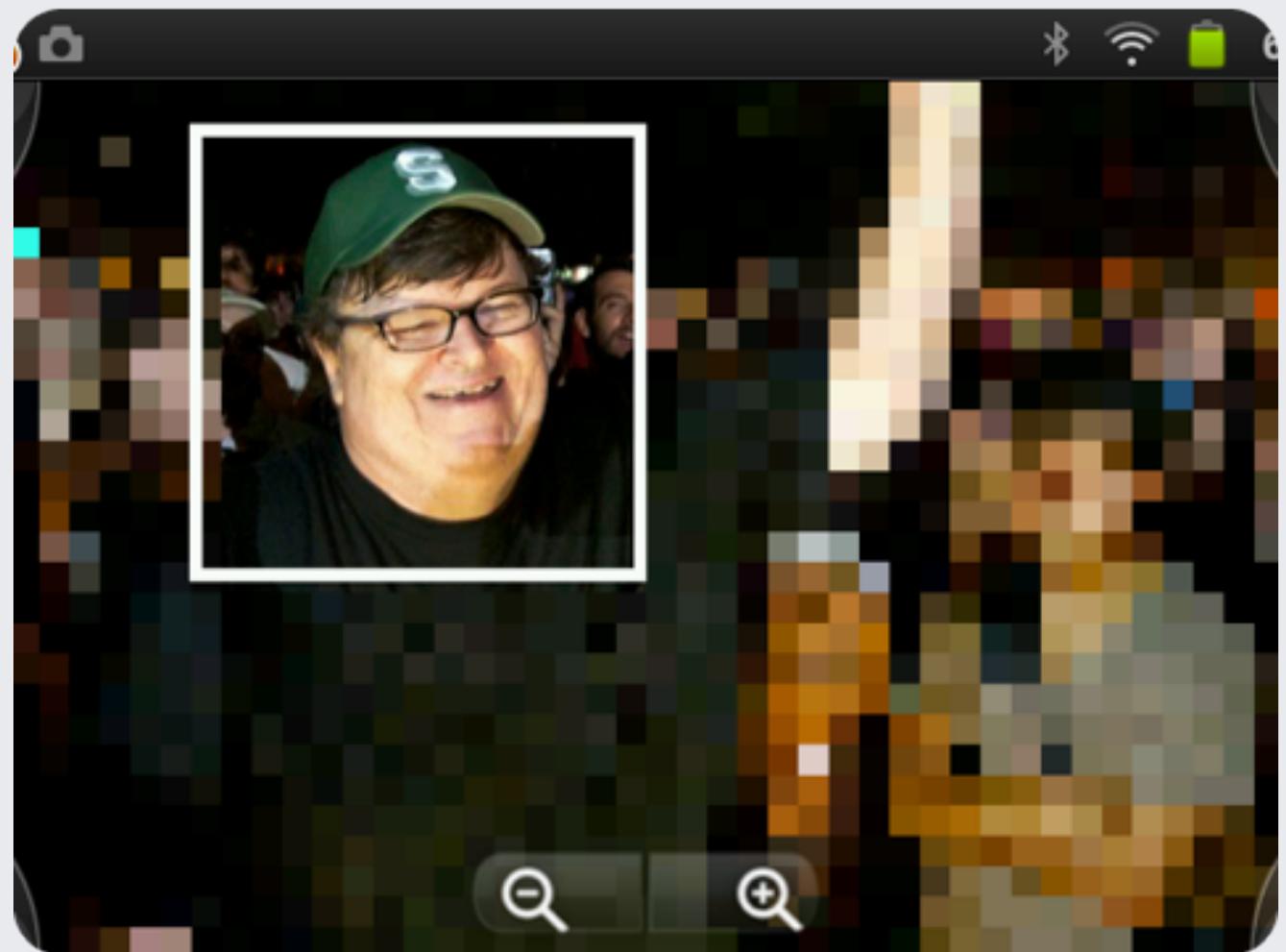
CROWDPIXEL

- From the edit menu select CrowdPixel



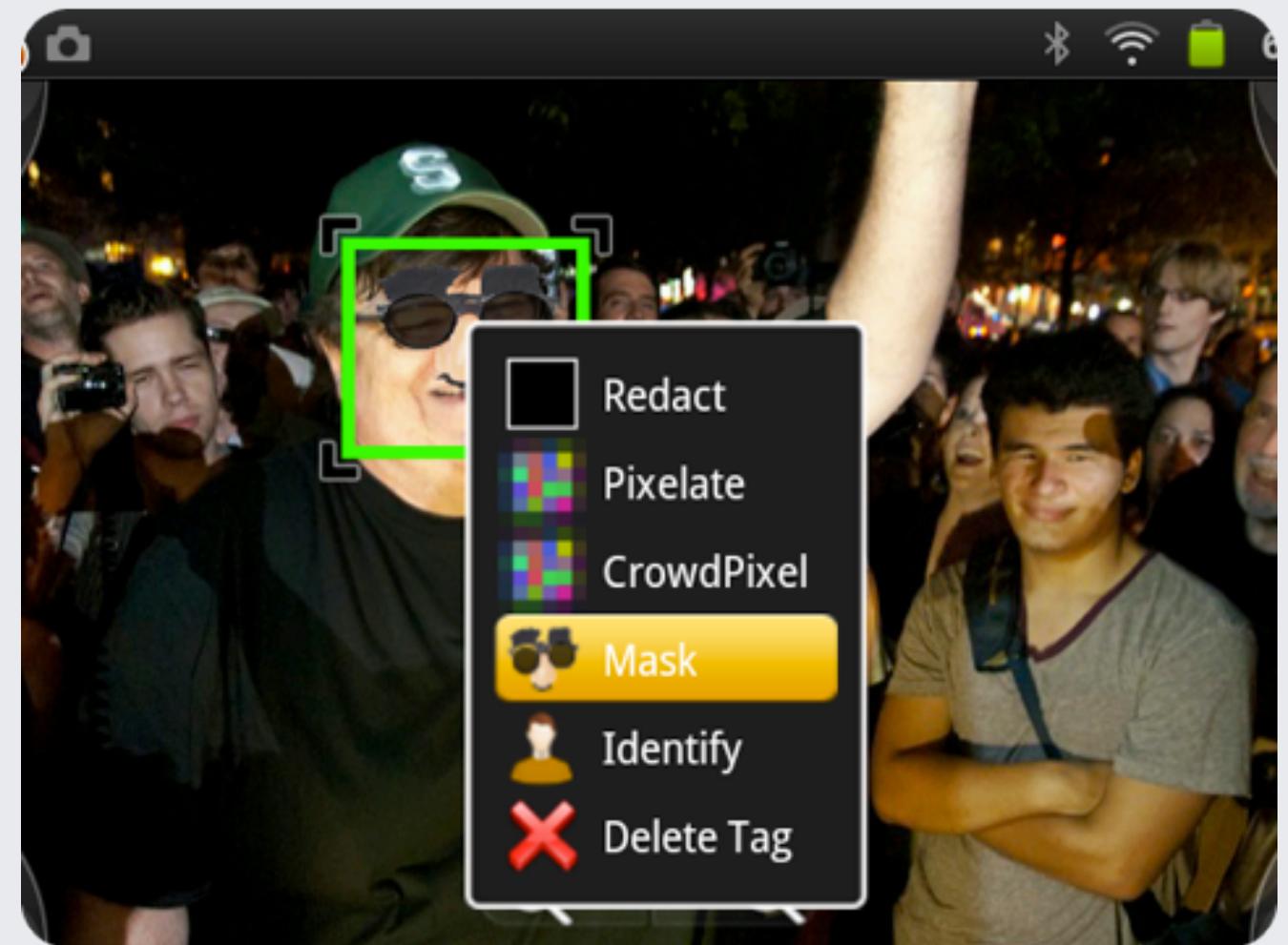
CROWDPIXEL

- Everything OTHER THAN the selected region will be pixelated



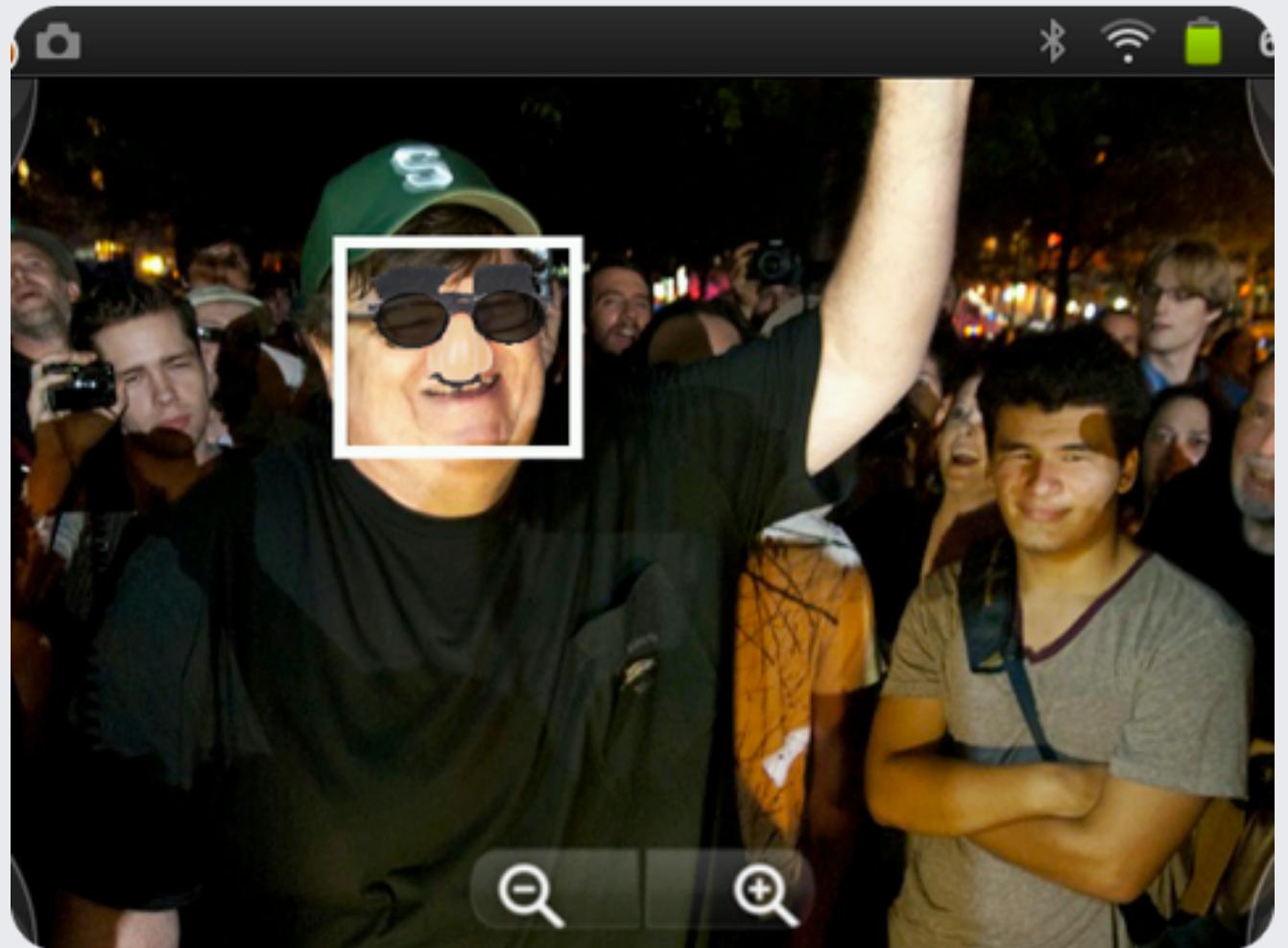
MASK

- From the edit menu select Mask



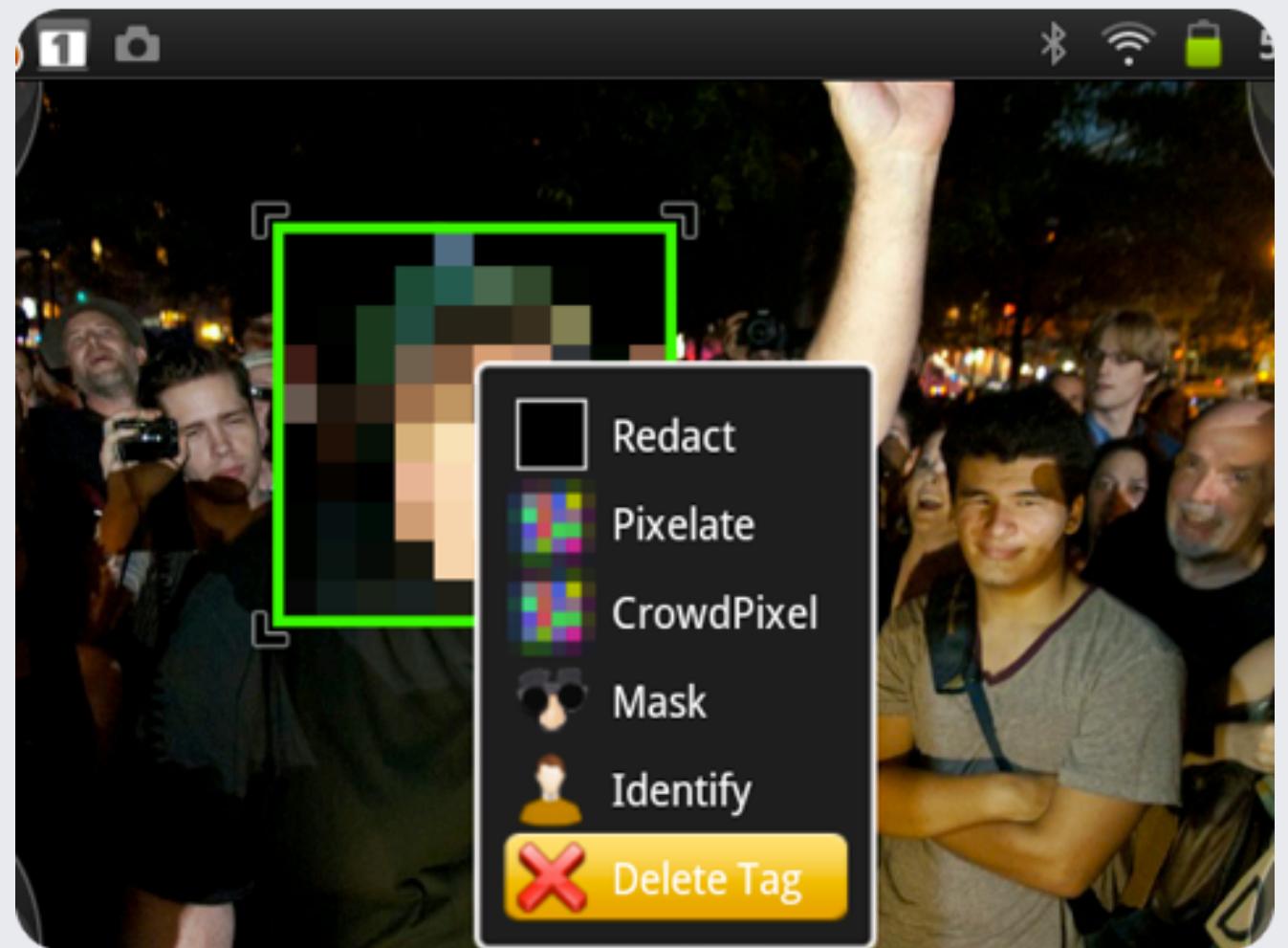
MASK

- A mask will partially cover the center of the selected region
- NOTE: Mask will NOT protect anonymity but will defeat automatic face recognition i.e. Facebook



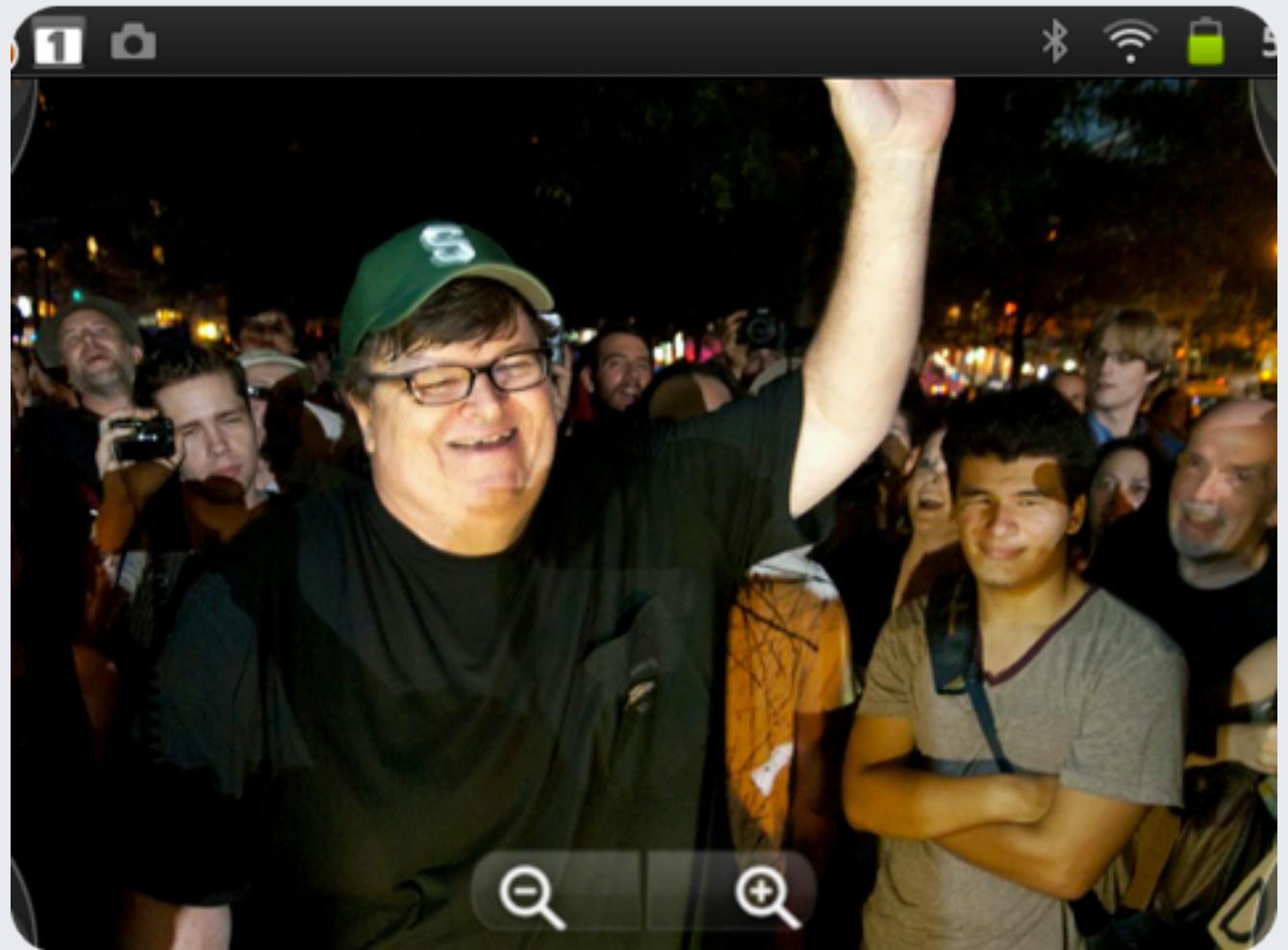
DELETE TAG

- From the edit menu select Delete Tag



DELETE TAG

- Deleting Tag will remove the selected region and leave it un-obfuscated





- witness.org
- guardianproject.info



Hurricane Sandy?



INFORMACAM

The screenshot shows the InformaCam application interface. At the top left is the logo "InformaCam" with a lock icon. Below it says "Powered by The Guardian Project". At the top right are links for "SUBMISSIONS", "SEARCH", "ADMIN", and "HELP". A navigation bar at the bottom has tabs for "Views", "Options", "Add Annotation", and "ImageRegion Tracing: On / Off". The main area displays a photograph of a brown dog sitting on a bed. A white tracing box highlights a portion of the dog's body. To the right of the image is a detailed metadata panel:

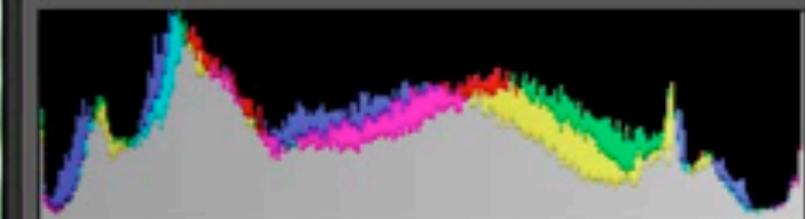
- Intent**: Submitted by: [REDACTED] (Ownership type: Individual)
- Genealogy**: Media created on: 19 Dec 2012, 14:14
Acquired by submitting device on: 19 Dec 2012, 20:50
- About the device submitting this media:**
 - Bluetooth Name: [REDACTED]
 - Bluetooth Address: 1[REDACTED]0
 - Handset IMEI: 3[REDACTED]7
- Device Integrity**: InformaCam is 100 % certain that this media was captured by the device with the above IMEI.

On the right side of the screen, there is a mobile phone interface showing the "InformaCam" app. It has two buttons: "Camera" and "Camcorder". Below the phone are three menu items: "Media Manager", "Message Center", and "Address Book".

A secure camera application being developed with WITNESS, to help improve visual privacy, secure human rights media content, and innovate in software camera tools for activists.



Histogram



ISO 640 95 mm f / 3.5 1 / 500 sec

Jeffrey's View Metadata

Preset None

File JEF_031786.NEF

Folder 10-Nanzenji-Walk

Rating • • • • •

View Name

Title

Caption Anthony looks for goodies in Fumie's purse while visiting Nanzenji.

Scene Stroll at Kyoto's Nanzen Temple

Blog URL <http://regex.info/blog/2007-06-10/486>

Artist Jeffrey Eric Francis Friedl

Copyright Copyright 2007 Jeffrey Eric Francis Friedl

Date June 10, 2007

9:43:11 AM

Size 3872 x 2592

Exposure 1 / 500 sec at f / 3.5

ISO 640

Bias 0 EV

Flash Did not fire

Metering Pattern

Focal Length 95 mm

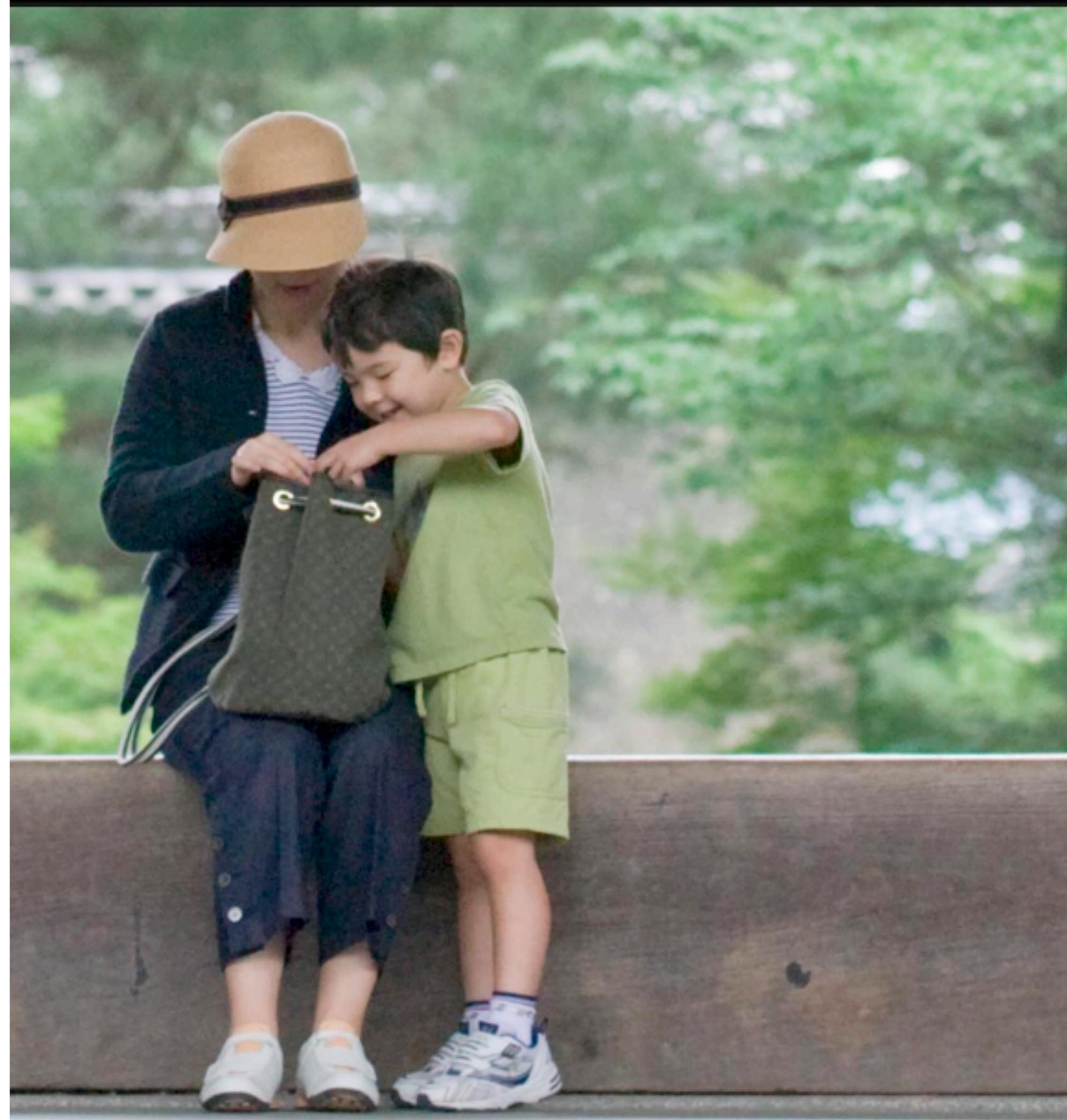
Lens 70.0-200.0 mm f/2.8

Distance 19.95 m

Make NIKON CORPORATION

Model NIKON D200

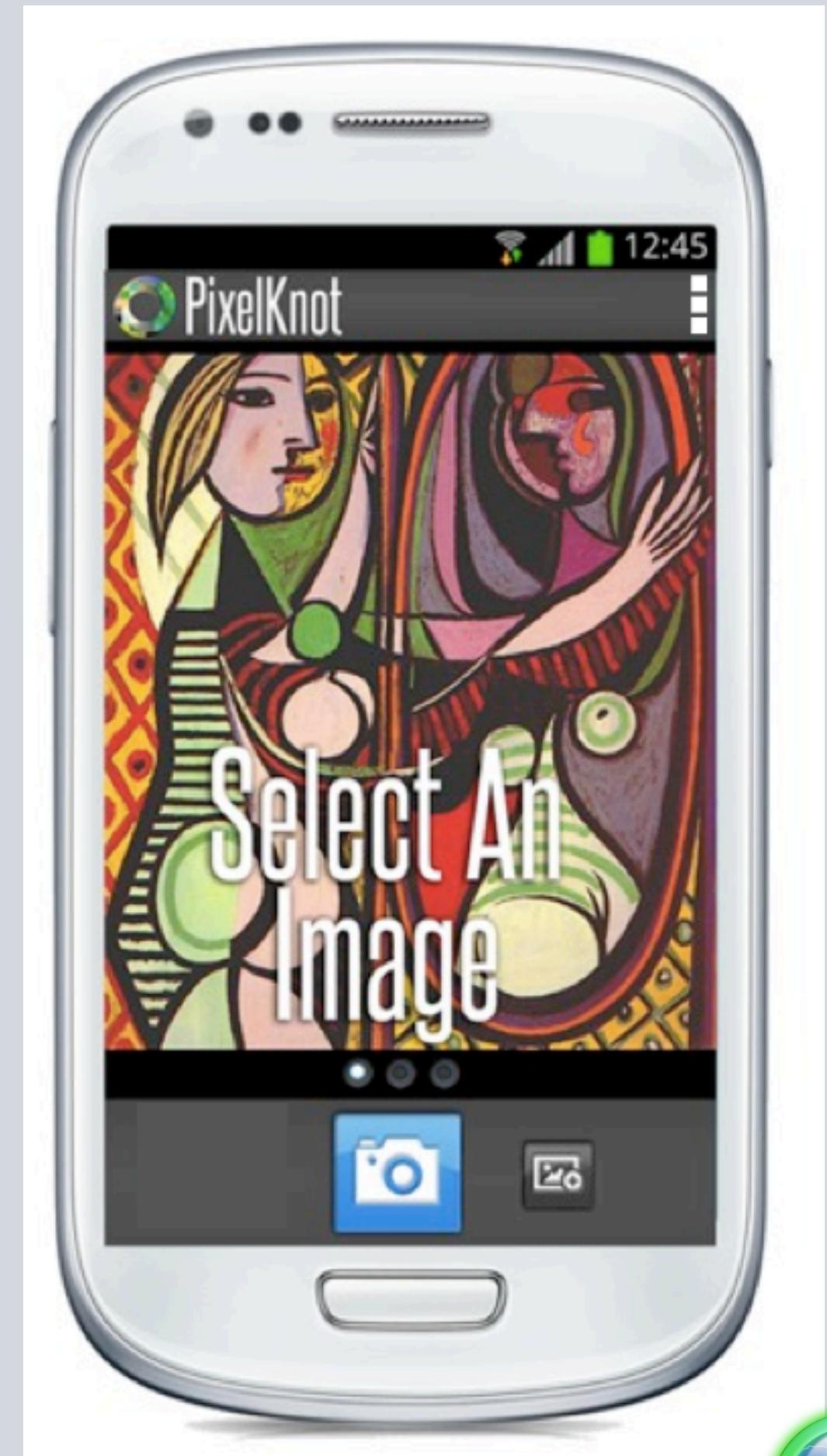
Sync Settings Sync Metadata



PIXELKNOT

Image steganography:
The practice of embedding secret
messages into a piece of media so that
no one, apart from the sender and
intended recipient, know that the
secret message exists.

- Secure & Encrypted messages
- F5 Steganography algorithm





MODERN IMAGE STEGO

The secret message in an image, or ghost in the machine, must:

1. Have the original image appear, to the trained human eye, **unedited**.
2. Have the bytes of the image appear, to a trained analyst, **undistorted** so much so as to arouse suspicion.
3. Have the complete message be **recoverable** no matter how it is transmitted.

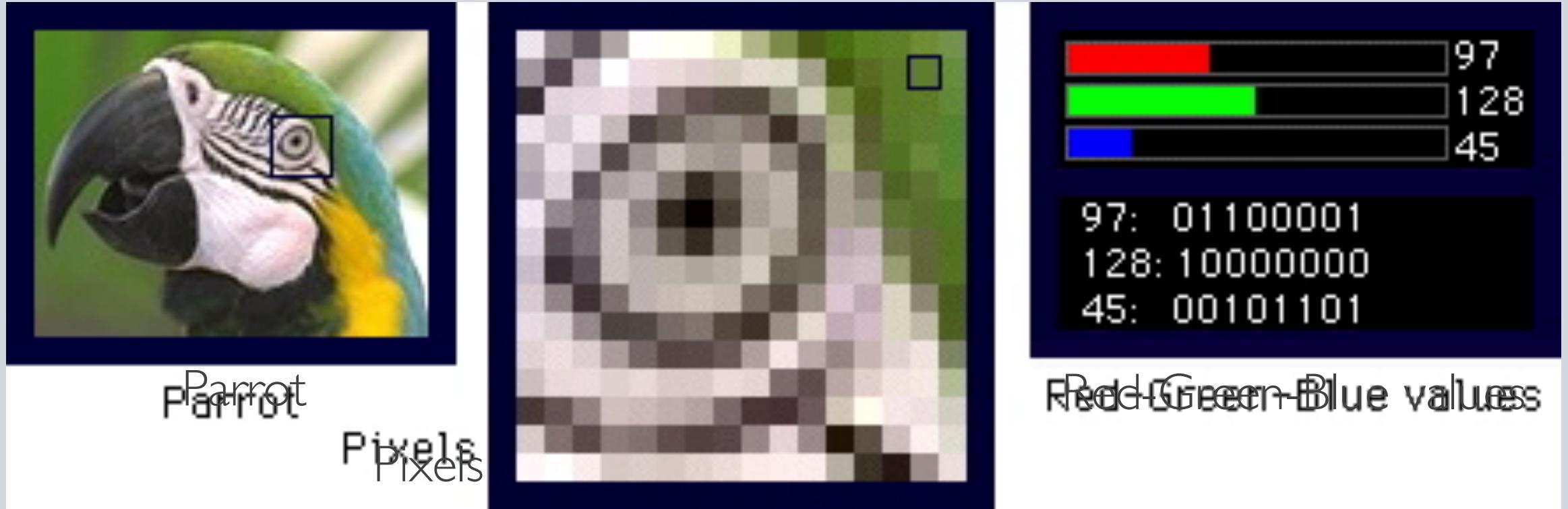




MODERN PROBLEMS

What was cutting edge a couple of years ago, no longer
is.





LEAST-SIGNIFICANT-BIT STEGO

Problems with making slight alterations to certain parts of an image:

1. **Distortion:** Forensic analysts are now accustomed to this trick. The footprint of an image treated this way can be obvious to a professional, so it can be found-out.
2. **Unrecoverable:** This tactic requires that the image never deviate in its size or quantization. This happens across most modern image-sharing medium, such as social networks & MMS.



FUTURE SOLUTIONS

An app that manipulates the image at the "compressed domain," at the quantization tables of the jpeg, and embeds the secret message as a DCT coefficient in the chrominance channel of each 8x8 pixel block of the image

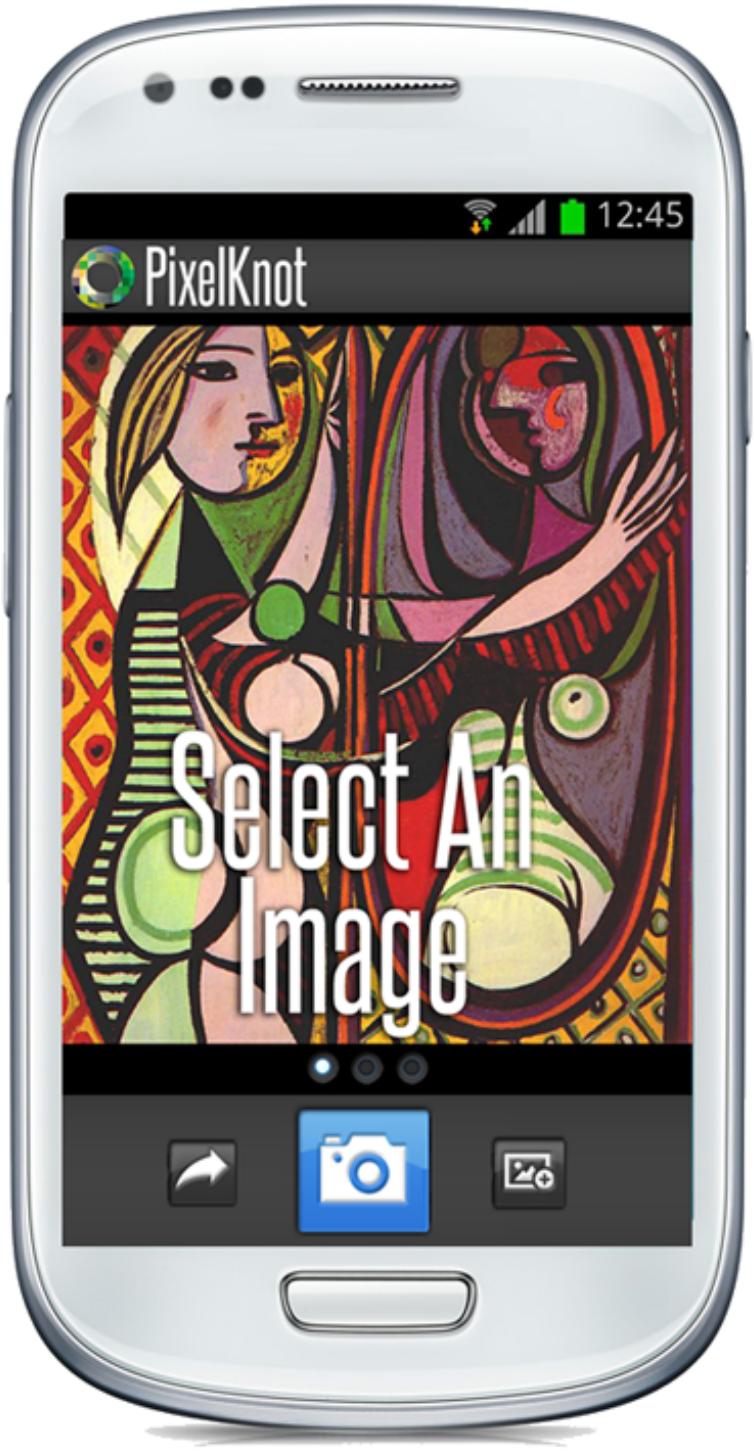


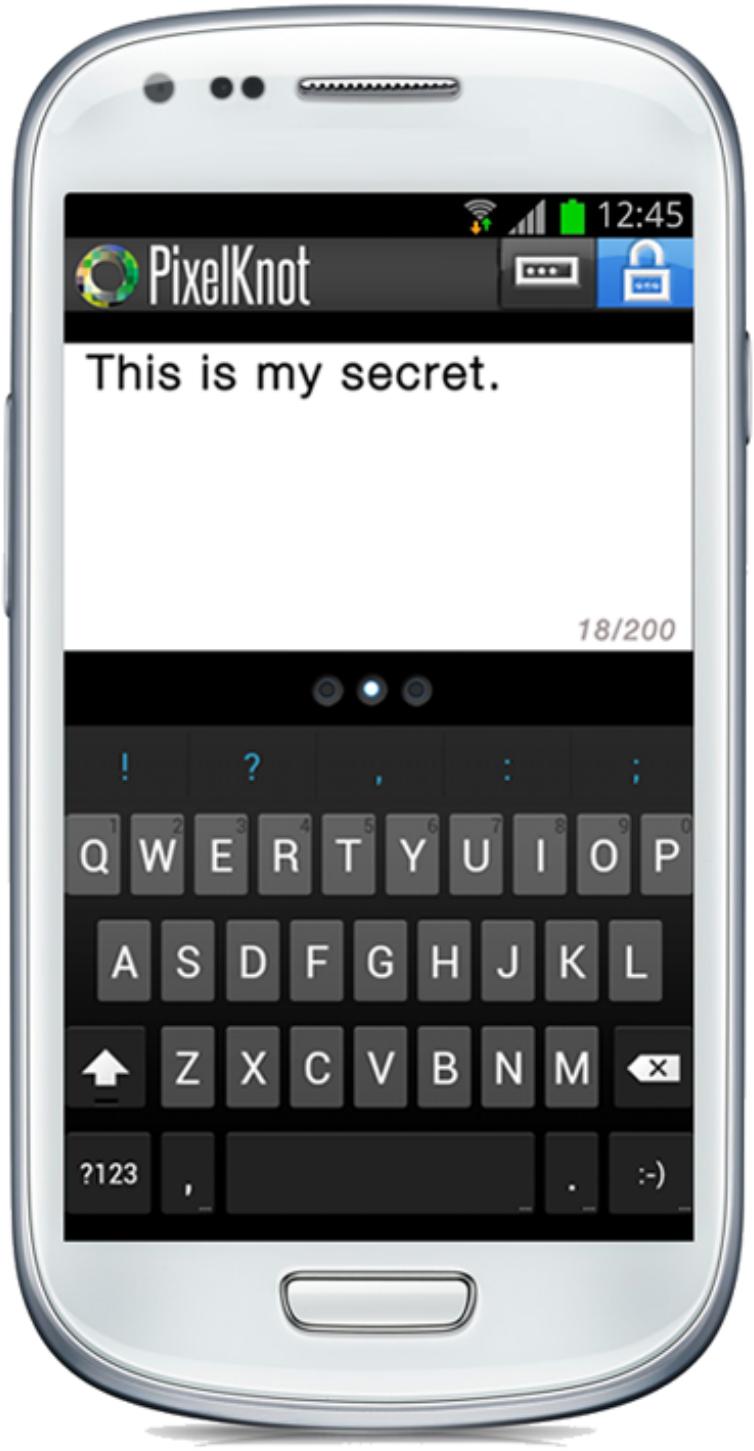


SOCIAL MEDIA INTEGRITY

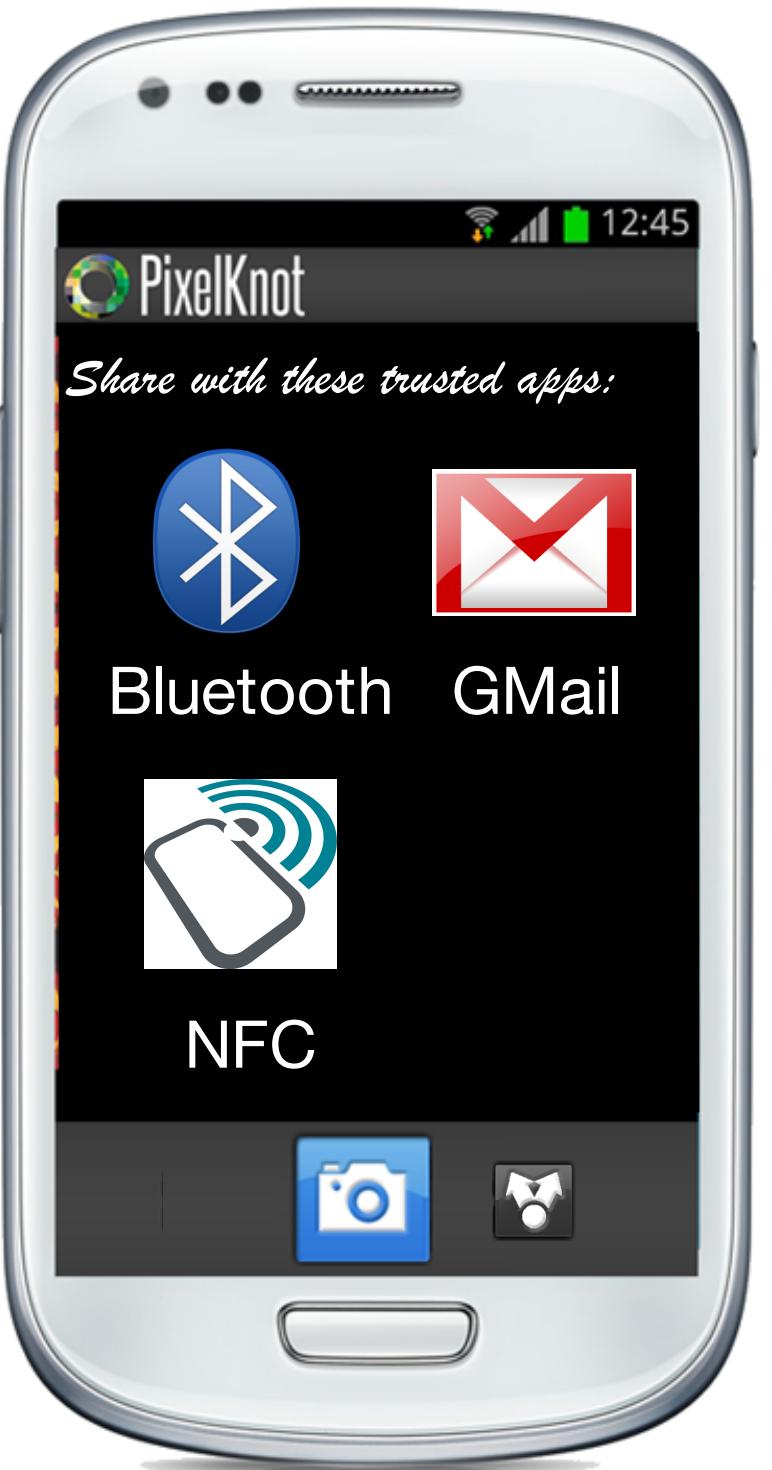
The quantization stego method purportedly resists certain transformations to the image. However, this is as long as the image itself is not re-quantized by another actor, which could be the case with certain web and mobile services like Facebook. This approach already is popular in the use of watermarking copyrighted material.







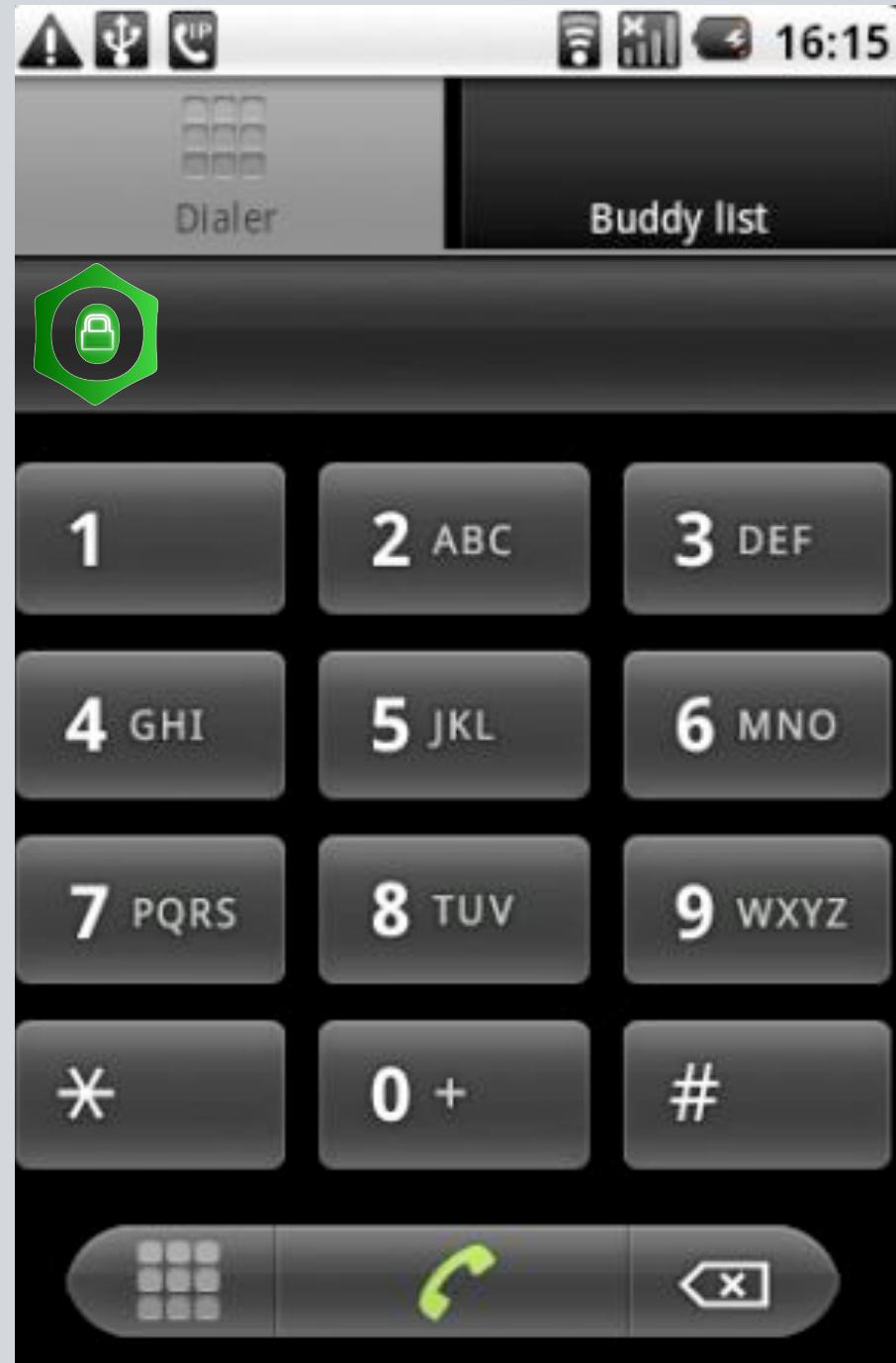




OSTEL

Secure and free phone calls. A defacto standard by which a voice over internet protocol service can be considered end-to-end secured, with verifiable encryption, minimal logging, and a decentralized model of deployment and use.

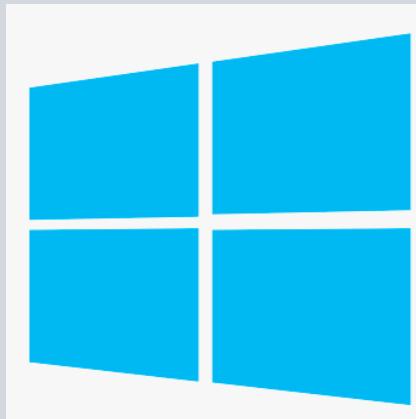
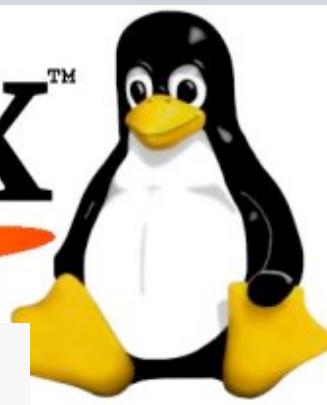
- Built-in public key encryption with ZRTP
- A network of compliant server/service instances
- Client software on mobile and desktop
- Currently functioning on Android, iPhone, Blackberry, PC & Linux
- <https://ostel.me>





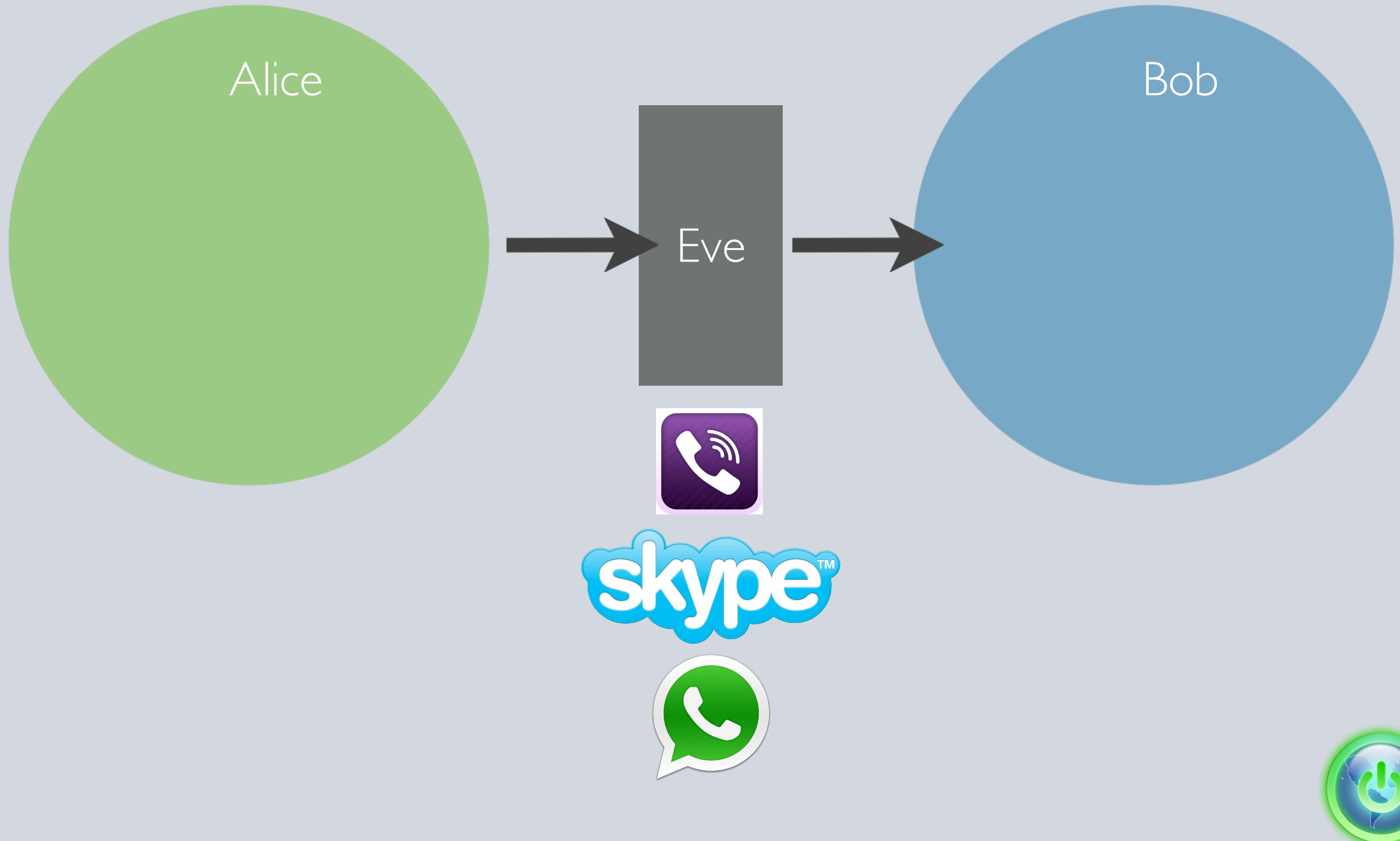
NOKIA

Linux™



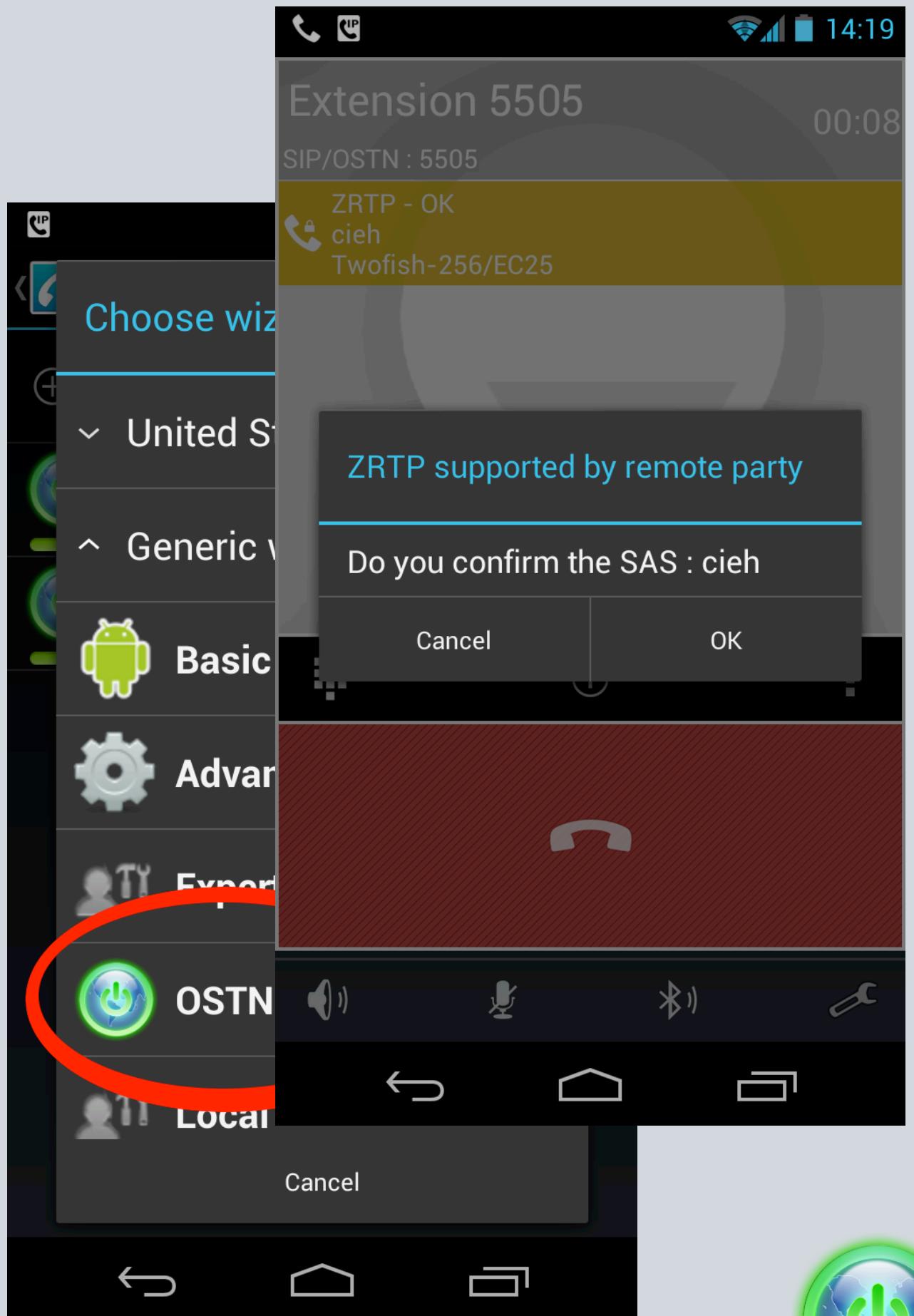
Windows®

END TO END ENCRYPTION?



CSIPSIMPLE

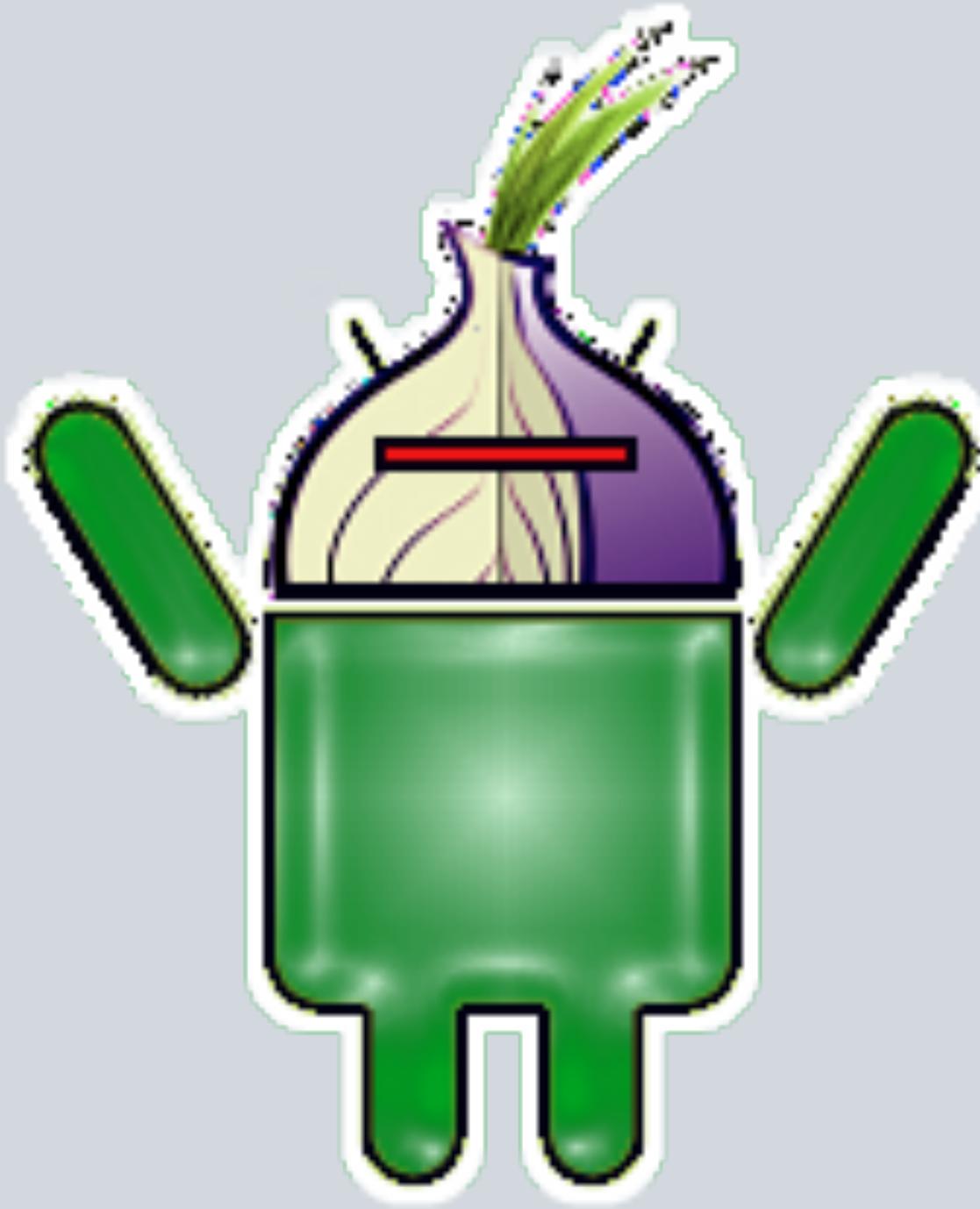
CSipSimple is a program for Android devices that allows for making encrypted calls. Naturally the calling software isn't enough on its own and we need a communication network to enable us to make calls.





OSTEL.ME





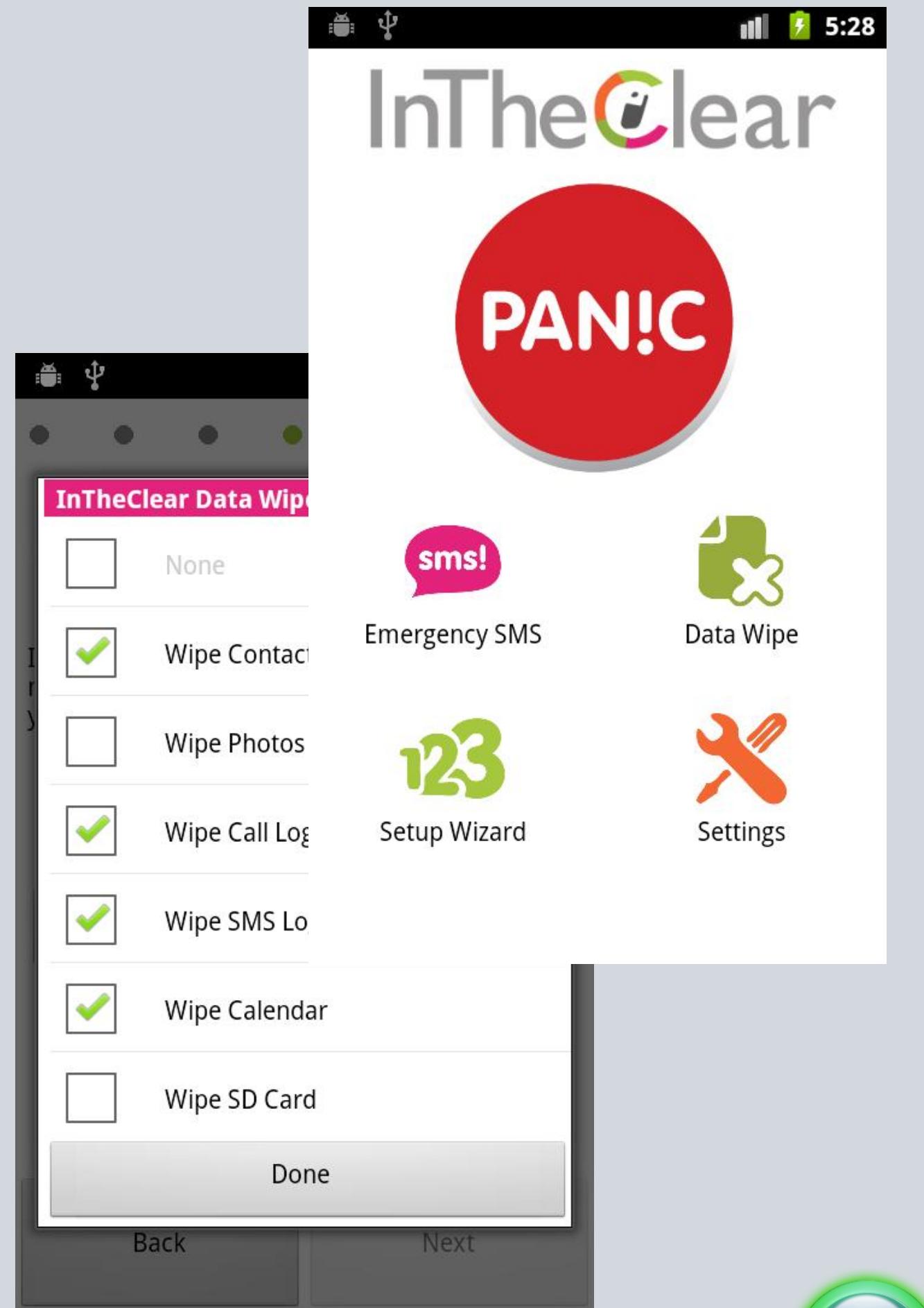
TOR AND OTHER PROBLEMS



IN THE CLEAR

A “poison pill” app data wipe and emergency SMS distress beacon.

- Quick, one-touch activate
- Wipe data across different Android apps and external storage / SD Card
- Emergency SMS sends in background repeatedly with location and cell network dataAlso available on Blackberry and Java (Nokia, etc) phones



K-9 MAIL

K-9 Mail is an open-source e-mail client with search, IMAP push email, multi-folder sync, flagging, filing, signatures, bcc-self, PGP, mail on SD & more!

- Open Source
- <http://k9mail.googlecode.com>



The screenshot displays the K-9 Mail application's user interface. At the top, there is a status bar with icons for signal strength, battery level, and time (22:14). Below the status bar, a message is shown: "Hallo. Thialfihar To: Oliver". A "Decrypt" button is located in the bottom right corner of this message area. The main interface consists of several panels:

- Accounts (Next poll @ 2010-08-14 22:14)**: Shows two accounts: BT (423.5KB) and Hotmail (610.5KB). Each account entry has a downward arrow, a trash can icon, and an upward arrow.
- Integrated Inbox**: A list of messages under the heading "All messages in integrated inbox".
- All messages**: A list of messages under the heading "All messages in search results".
- Compose**, **Search**, **Add account**: Buttons in the top row of the main panel.
- About**, **Check mail**, **Settings**: Buttons in the bottom row of the main panel.

The central part of the interface shows a large amount of encoded PGP message content, starting with "-----BEGIN PGP MESSAGE-----" and "Version: APG v1.0.6".





POSTCARD

Vs.

LETTER





YAHOO!



POSTCARD

Vs.

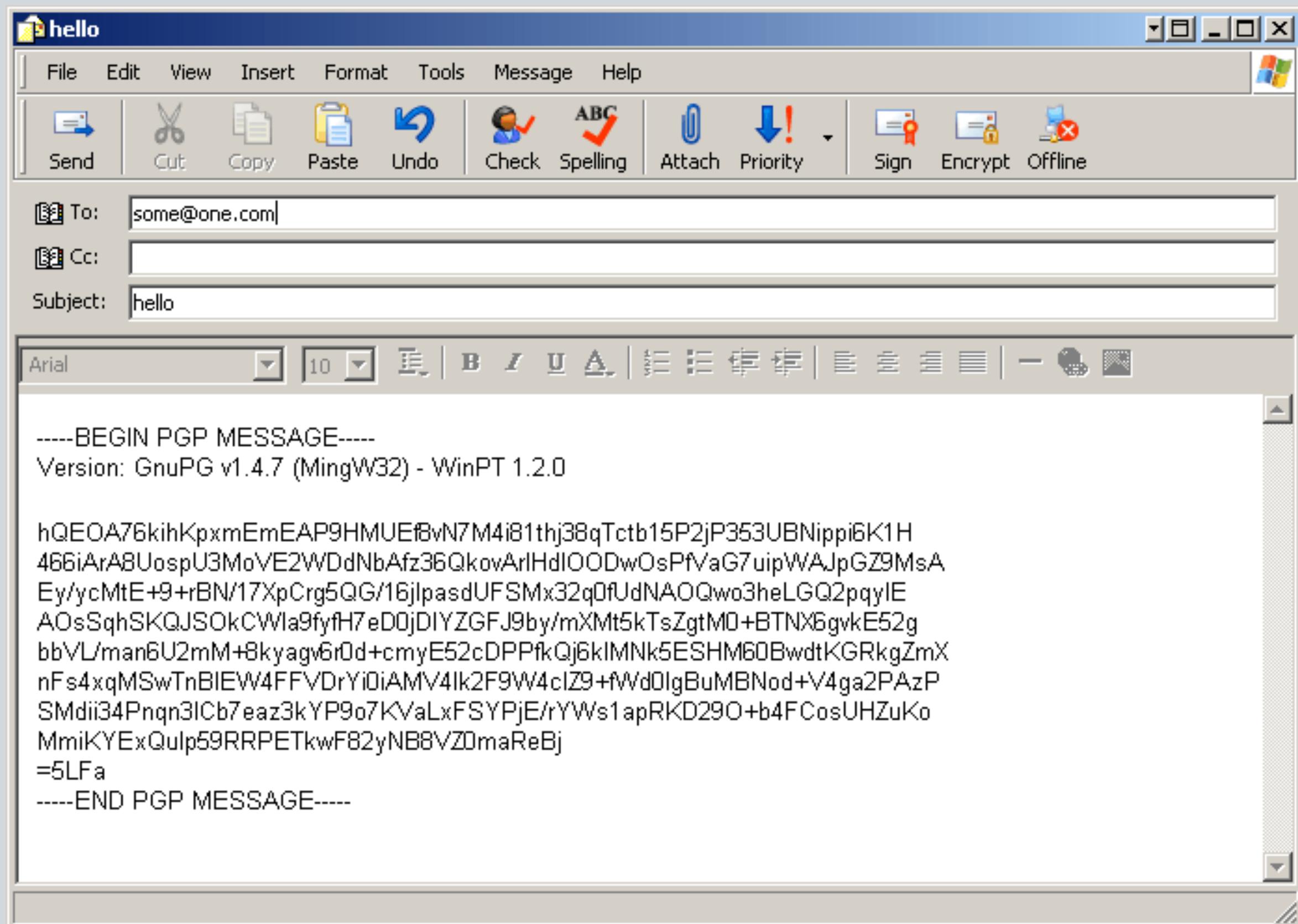
LETTER





WAX SEAL





WAX SEAL

+

CYPHER

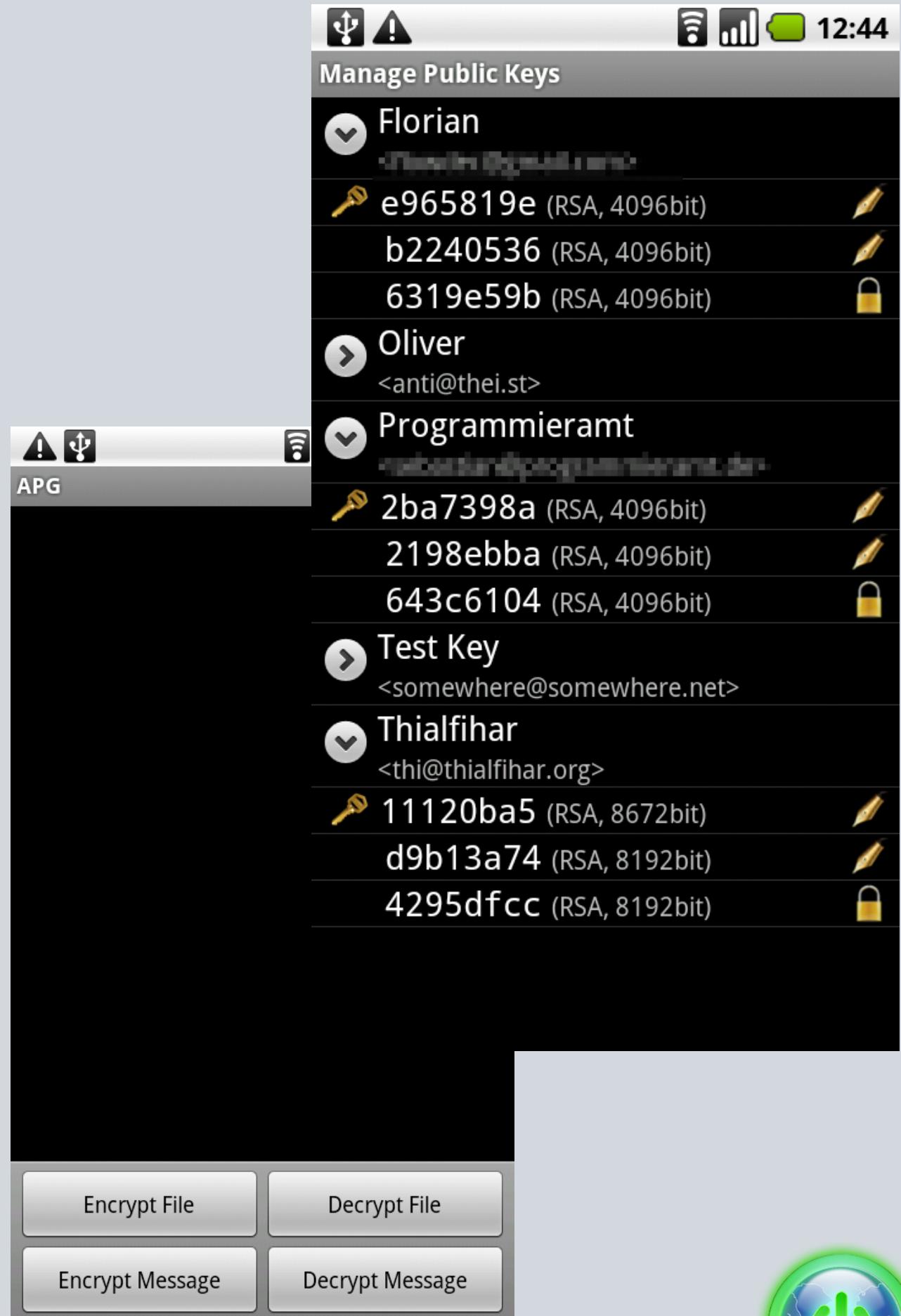


AGP



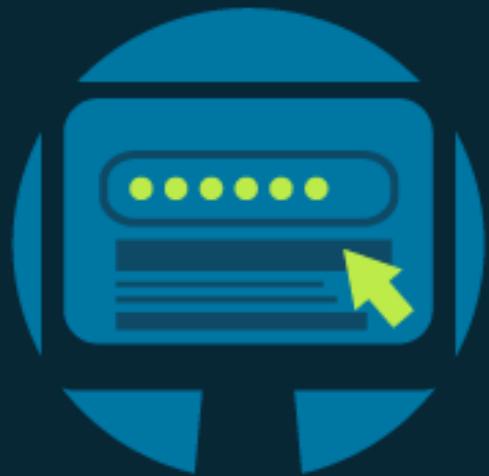
Manage OpenPGP keys on mobile to encrypt, sign, decrypt emails and files. Android Privacy Guard tries to fill that void of no public key encryption for Android.

- import/export of GPG key rings and exported keys from/to the SD card
- encrypt and sign messages, then send them via your preferred email app
- decrypt messages and verify signatures
- reply to decrypted messages with quoting and automatic filling of receiver key and signature, based on the keys used to sign/encrypt the received message
- list the most recent emails in the inbox of your Google Mail accounts on the phone
- support file managers for easier file selection where necessary
- file encryption/decryption with asymmetric and symmetric ciphers
- key management (import, create, edit, export)



8 SIMPLE PRIVACY TIPS TO PUT YOUR MIND AT EASE

Here are a few simple things you can do to protect your privacy:



Always create unique passwords.



Set a strong password and frequently change it.



Update your phone and third party application software.



Look for signs of trust and read reviews and ratings of applications before purchase.



Be careful clicking on links within emails, SMS or social networking sites that ask for your personal information.



Only enter your account or credit card information on a site that begins with "https://" or has the lock symbol.



Take a minute to read the application's privacy policy.



Take note of pop-up notices/alerts.



HOT OR NOT?

If your phone is hotter than you, you might have a problem.





TRANSLATION

Help us speak your language.
transifex.com



A photograph of two young girls playing tag on a grassy field. One girl, wearing a pink shirt and denim shorts, is running towards the right. The other girl, wearing a white t-shirt with a graphic and dark shorts, is running towards the left, reaching out with her right hand as if to catch the other girl. In the background, another girl lies on the grass. An orange traffic cone is visible in the top left corner.

CREATE GAMES



DEVELOPER TOOLS

Software routines and utilities to help programmers understand and code application with security and privacy by default





CIPHER SUITE

A Growing Number Of Tools For Securing Apps &
Communication on Android



IOCIPHER

Transparent encrypted virtual disks for Android. This allows Android app developers to use the familiar and well documented android.database.* API to build in encrypted storage into their apps

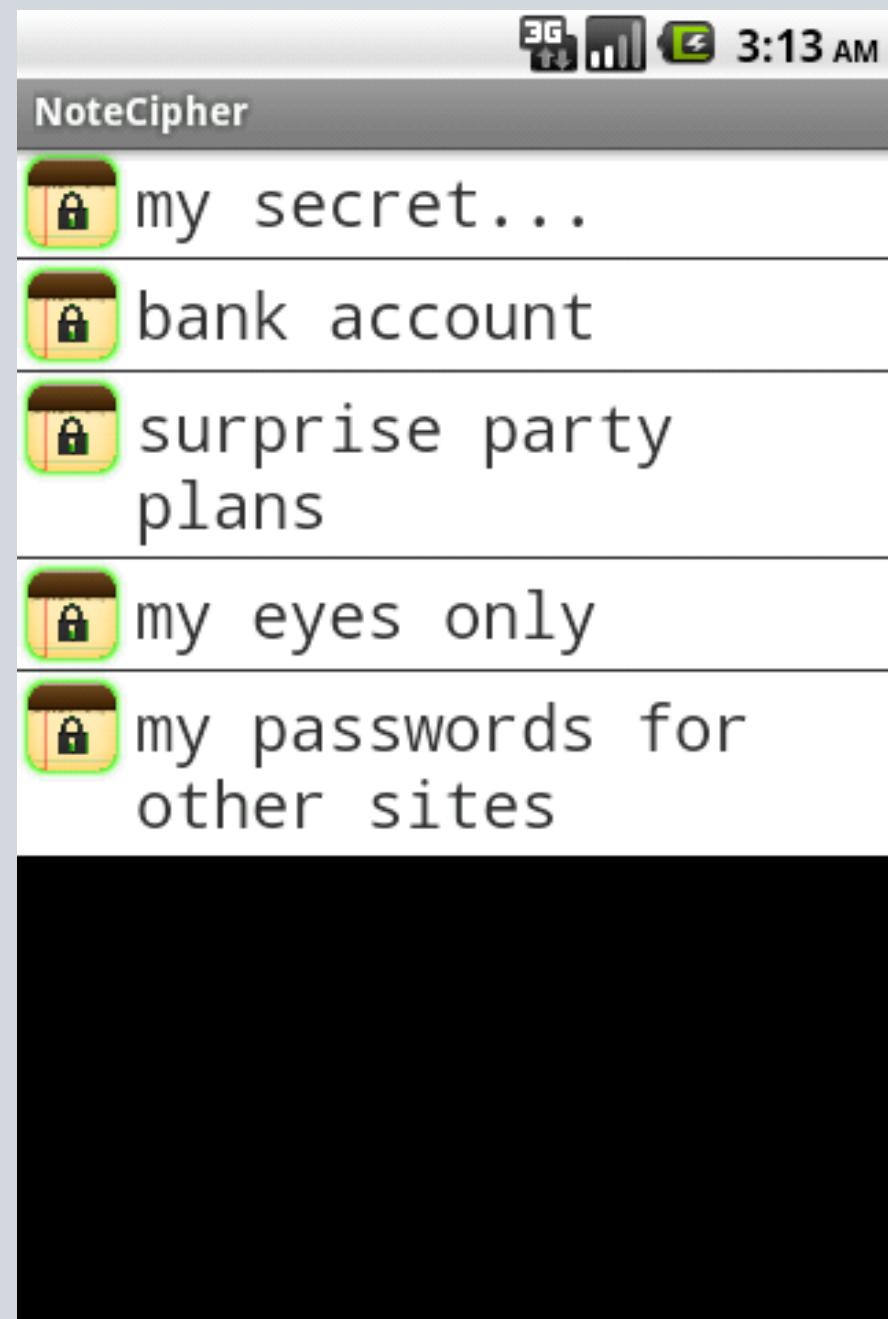
- libsqlfs+SQLCipher built on top of SQLite, which gives a single, very portable file that is the whole filesystem
- libsqlfs is a FUSE module
- Successful alpha of IOCipherServer/SpotSync app



SQLCIPHER

SQLCipher is an SQLite extension that provides encryption of per-app database files.

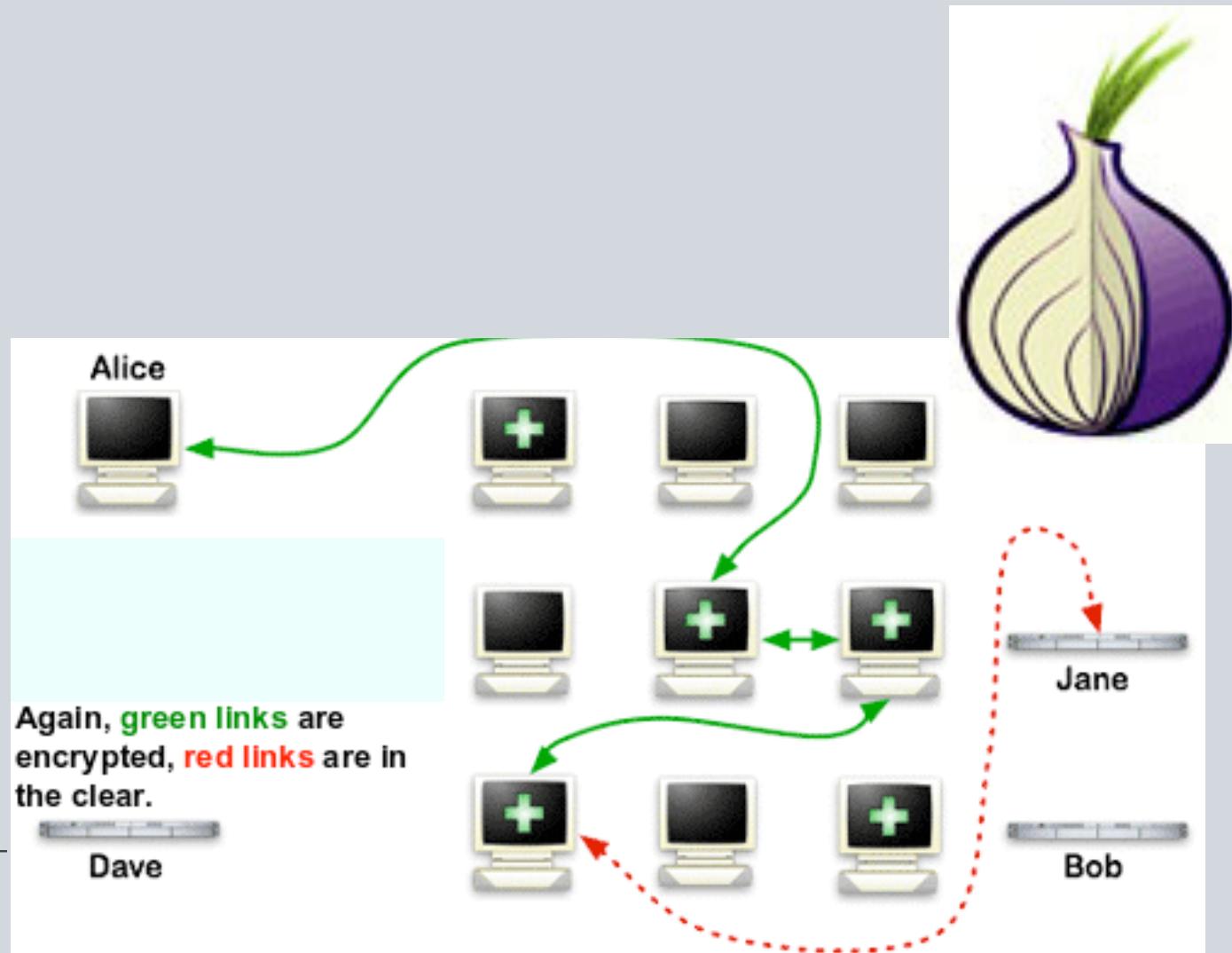
- Symmetric, 256-bit AES
- Existing open-source project, ported to Android
- Simple process to enable encryption on existing apps
- Cross-device and desktop portable data compatibility
- Robust, tested and performs well on mobile devices



NETCIPHER

Enabling secure and anonymous network proxying. This is an Android Library for use by any application that wishes to route its network traffic through Orbot/Tor.

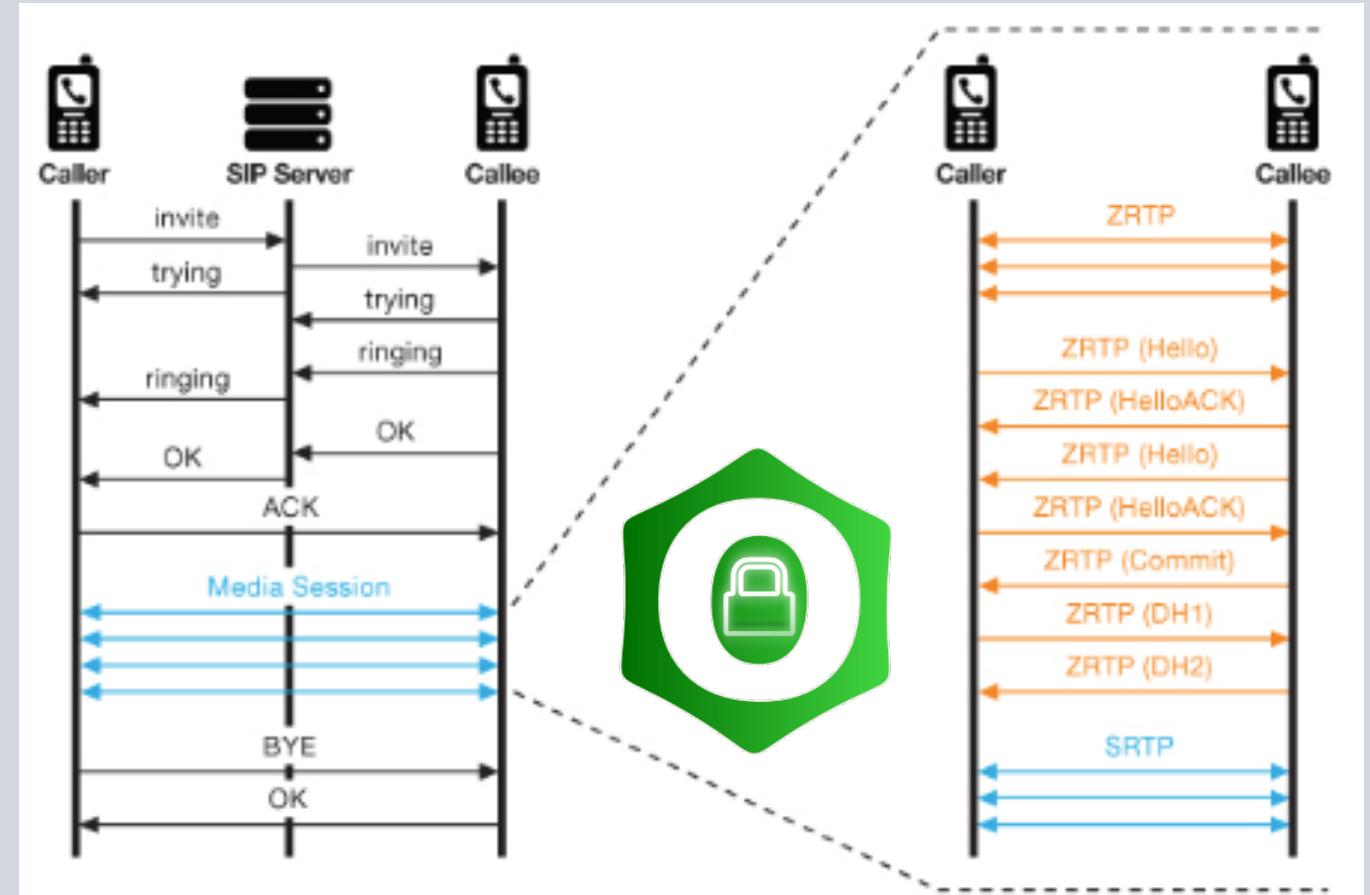
- StrongTrustManager: a robust implementation of an TLS/SSL certificate verifier, that can be customized with any set of certificate authorities
- Proxied Connection Support: HTTP and SOCKS proxy connection support for HTTP and HTTPS traffic through specific configuration of the Apache HttpClient library
- OrbotHelper: a utility class to support application integration with Orbot: Tor for Android. Check if its installed, running, etc.
- Transparent proxying of application data traffic on rooted devices
- Applications that provide traffic proxying to Orbot's local HTTP and/or SOCKS proxies can access the Tor network on non-rooted devices
- Successful integration with official Twitter app



OPEN SECURE TELEPHONY NETWORK

Secure voice communications schematics featuring an open client and server for a federated network. Standards development for VOIP end-to-end security, with verifiable encryption, minimal logging.

- Built-in public key encryption standards with ZRTP
- Coordinating a network of compliant server/service instances
- Coordinating client software on mobile and desktop, including PrivateWave, Redphone, Groundwire, Keywe, and Debian





CAN WE REPLACE THE TELEPHONE
COMPANY?



	Android + Guardian	RIM BlackBerry + BES	WinMo / iPhone + ActiveSync / Lotus
Open-Source / Peer Review	Apache and GPL licensed open-source code, extensive public review	Closed-source	Closed-source
Encryption Standards Support	OpenPGP, AES-256, ECC-56 bit (SMS)	FIPS-Certified, AES message encryption	No message encryption. TLS transport encryption.
Anonymity	All data traffic can be routed through Tor anonymity network	User identified by host/IP address of BES	User identified by host/IP of ActiveSync server / VPN
Circumvention	Restrictive FW can be passed using Tor network with bridges	RIM Network / BES may be accessible via restrictive fw	Corporate VPN may be accessible via restrictive fw
Customization	Completely customize down to Android ROM image up to apps	Add on apps / J2ME / BlackBerry SDK	Add-on apps / .NET
Device Management	GPS tracking, locking, wiping, backup and ROM update via network download or SDCard	BES support for device authentication, remote erase and more	Remote lockout / auth for ActiveSync / remote erase of Exchange data

CAPABILITY COMPARISON



PARTNERSHIPS & SERVICES

Partner with other organizations for joint research, development and solution creation

Contract to customize and integrate open-source code for specific needs

Provide auditing, review and advice on mobile security architectures and deployments

Plan, purchase, and configure off-the-shelf mobile hardware solutions for a nominal fee

Provide general and specialized mobile security training and curriculum development

Partner in advocacy and awareness campaigns on mobile security & privacy

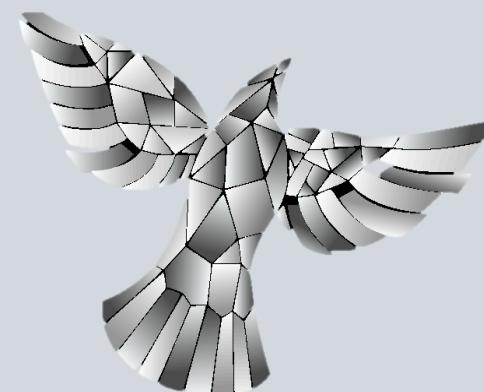


The Guardian Project is under active development, with beta stage deployments of software and hardware with partner organizations underway.

Our apps are available through our site, through partners sites and in the Android Market, and in total have been downloaded over 750,000 times.

We are actively seeking developers, designers, users, partners and funders for our work.

Please visit <https://guardianproject.info> for more information.



**THE GUARDIAN
PROJECT**
<https://guardianproject.info>



THE GUARDIAN PROJECT

WWW.GUARDIANPROJECT.INFO

INFO@GUARDIANPROJECT.INFO

