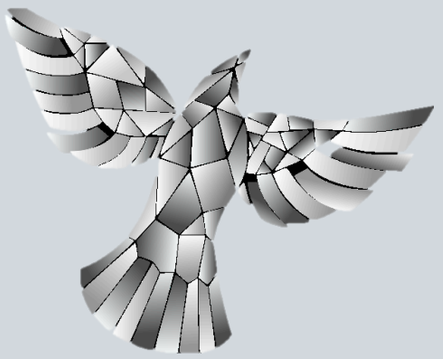
THE GUARDIAN PROJECT

MARCH 2013

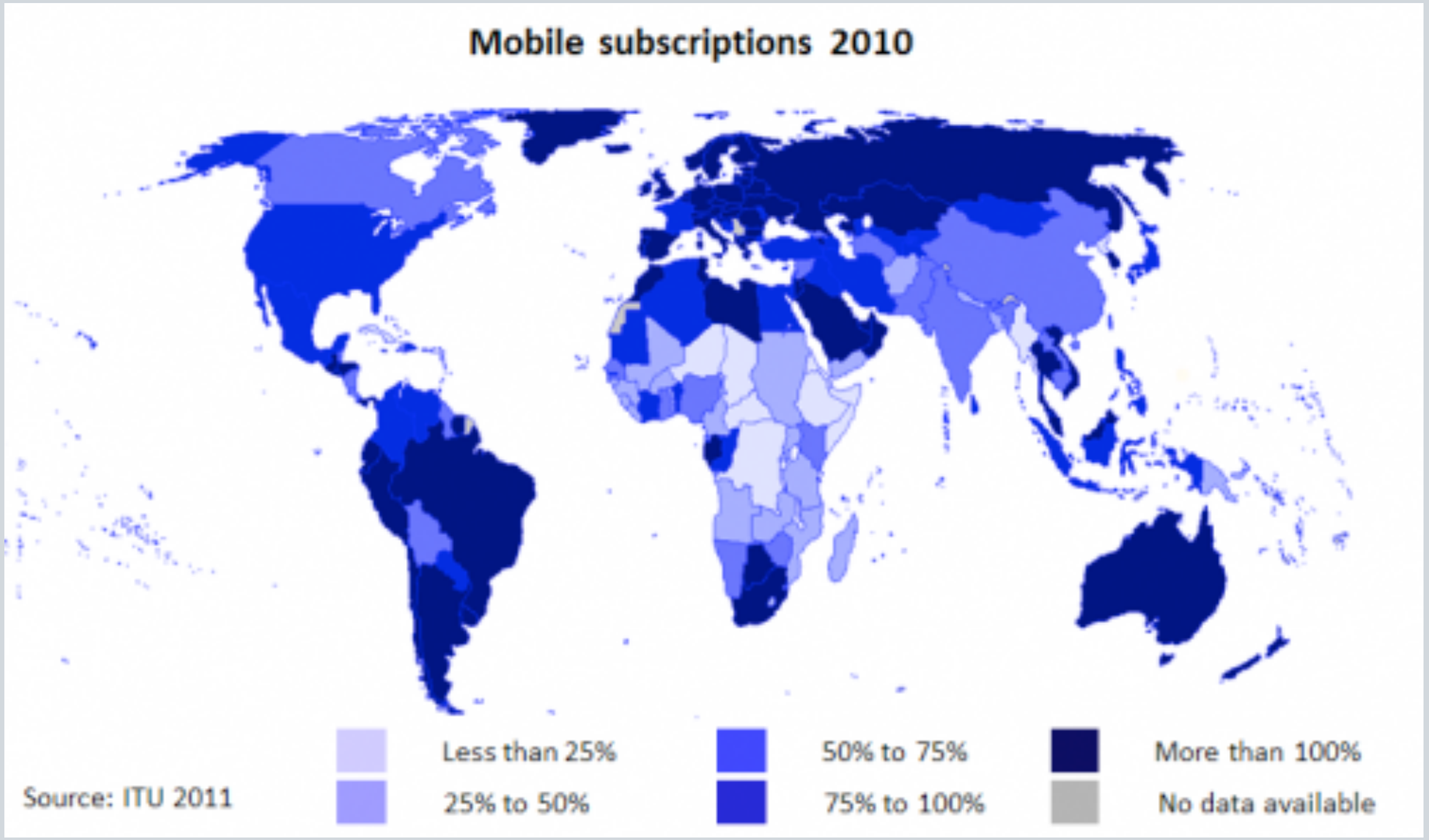
MARK@GUARDIANPROJECT.INFO

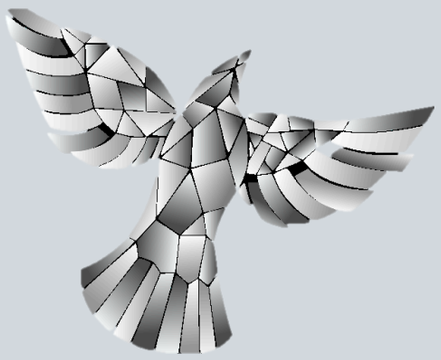
B605 F087 AE87 5CCA 9B76 2A39 EFBF A727 8D8E EFDA

Guardian Project is a research and development effort powered by technology-focused activists, concerned citizen users, and open-source security software hackers. We build tools based on real-world experience and feedback. Our process is transparent, inclusive and responsible.



THE GUARDIAN PROJECT
https://guardianproject.info





The number of smart-phones owned almost doubled in one year from 19% in 2010 to 35% in 2011 and is expected to rise over the next 12 months. There are now 4.5 billion mobiles in the developing world alone.

(Source) Worldwide Independent Network for Market Research (WIN) & GALLUP International, United Nations Development Program, USAID

THE GUARDIAN PROJECT
https://guardianproject.info


2012
BIRTHS
ASTEROIDS
1,300,000
300,000

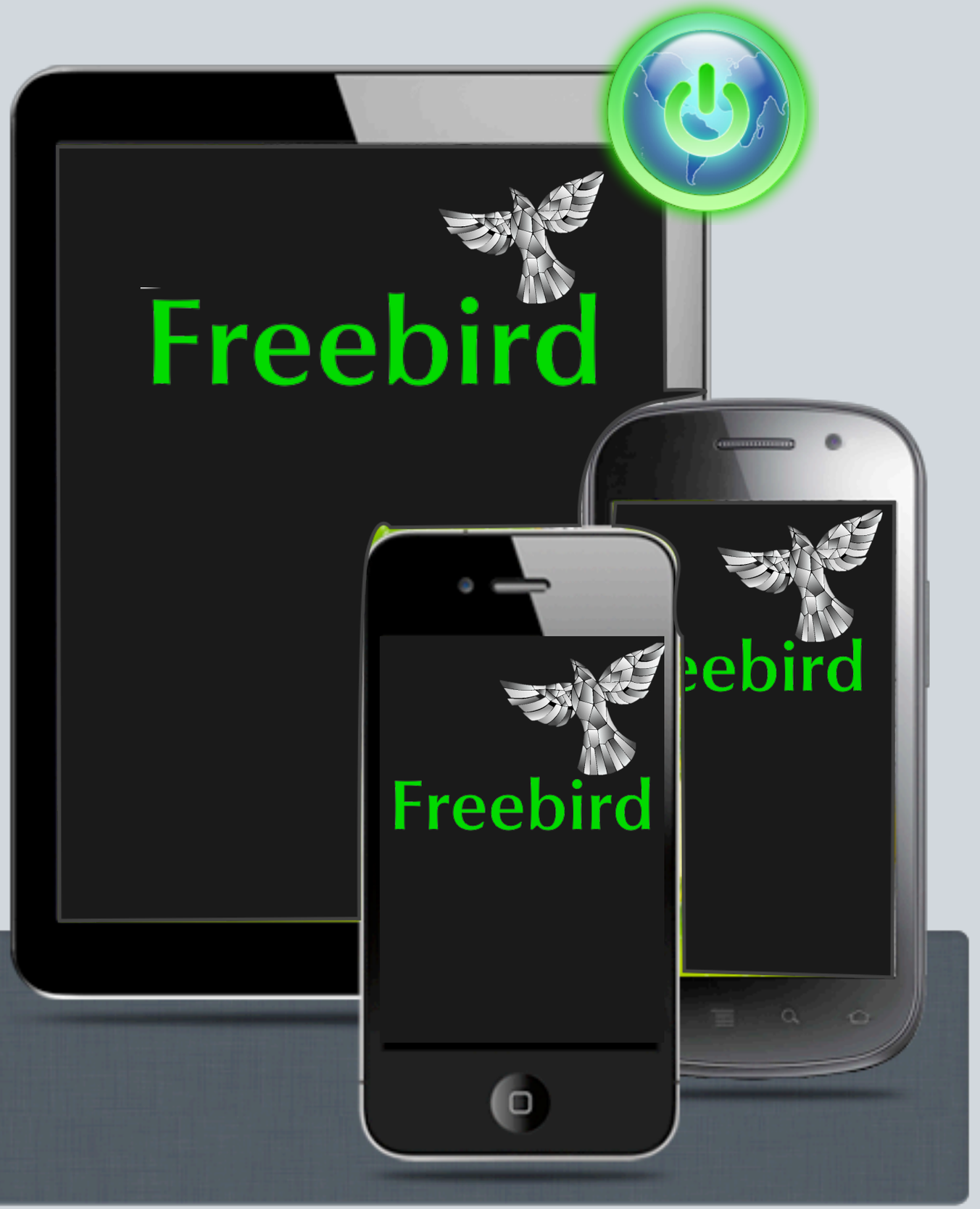
OPEN SOURCE

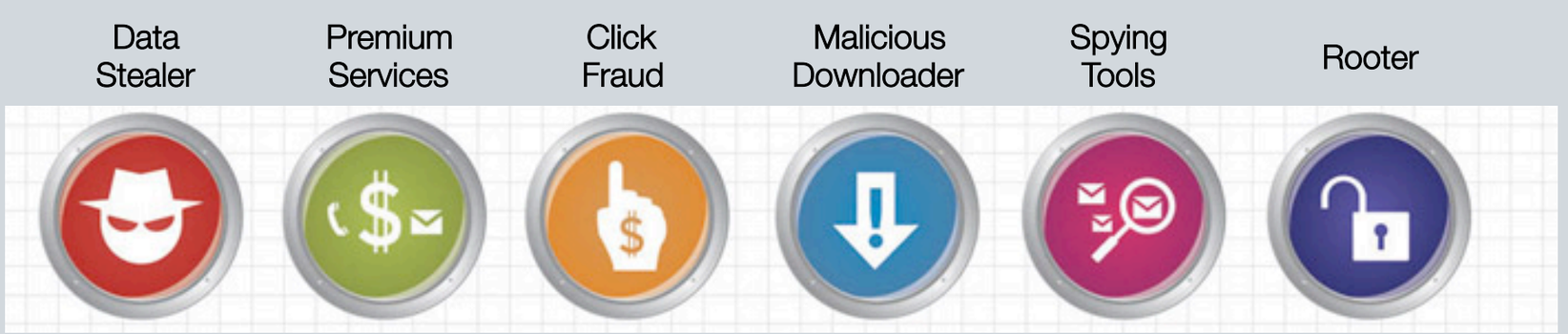
- Participatory
- Accountable
- Efficient
- Truly Secure

github
SOCIAL CODING

PLATFORM AGNOSTIC

Mobile is currently the least secure of all systems. Our goal is to change this. From Android, where we can verify the core to Apple iOS where we can build apps, we are leading the charge.





MALWARE TYPES

Ways to hijack info from apps

On An Average Phone:

31 APPS — Can access your **Identity Information.** *

19 APPS — Can access your **Location.***

5 APPS — Can access your **SMS and MMS Messages.***

lookout™ MOBILE SECURITY

Privacy on Your Phone

91% of consumers have some level of concern with privacy on their phone**

ONLY **7%** of smartphone users are extremely confident they understand private information accessed on their phone**

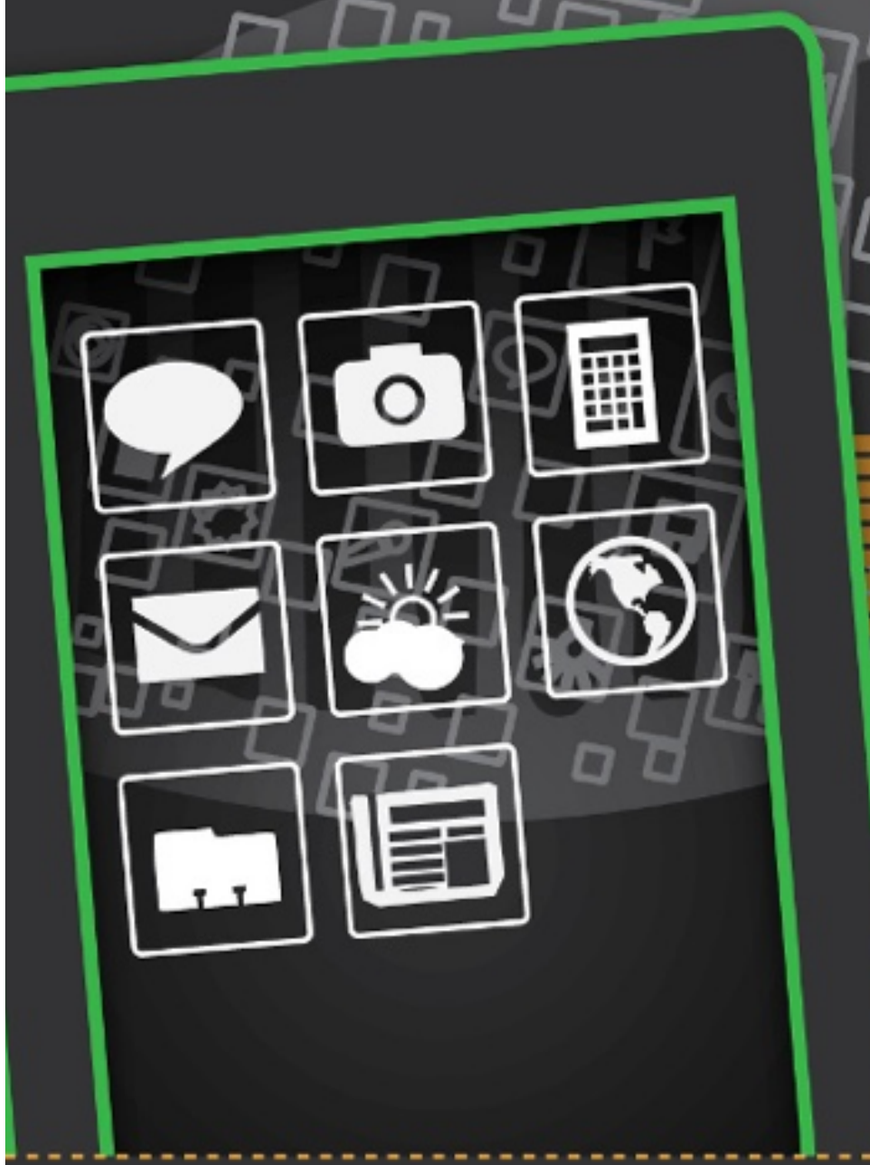
project

obile applications
applications are
mobile threats.

300,000
TOTAL APPLICATIONS

28% OF APPS IN THE APP STORE ARE FREE

64% OF APPS IN THE ANDROID MARKET ARE FREE



APPS CAN ACCESS:

- LOCATION
- CALL HISTORY
- TEXT MSGS
- EMAIL
- CONTACTS
- WEB HISTORY
- YOUR PHONE #
- PHOTOS
- DOWNLOADS

ACCESS YOUR LOCATION
33%
29%

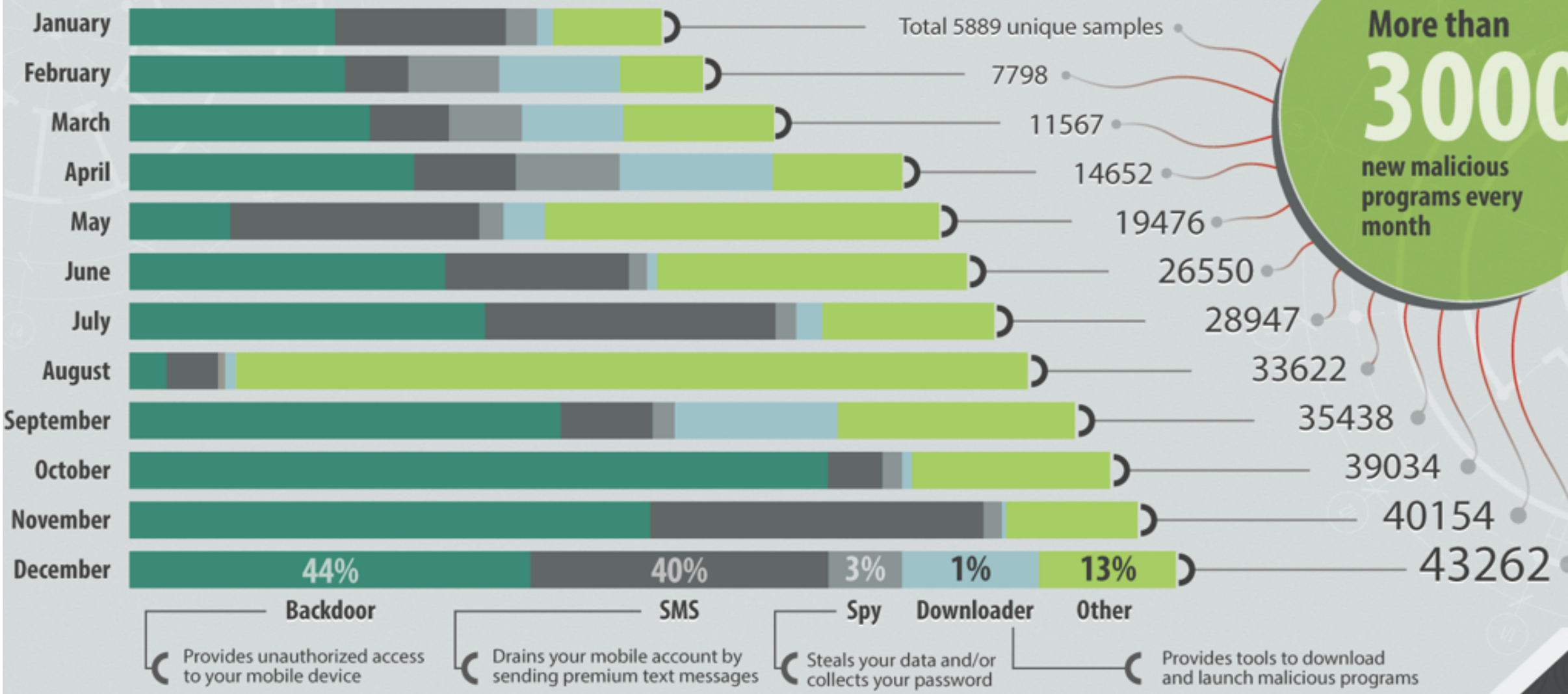
ACCESS YOUR CONTACTS
14%
8%

INCLUDE 3rd PARTY CODE*
23%
47%

lookout™

OOGLE ANDROID MARKET * Third-party SDK's like mobile advertising and analytics DESIGN BY: mikewirthart.com

Android Threats in 2012



More than 3000 new malicious programs every month

NOTABLE MALWARE BY REGION

USA

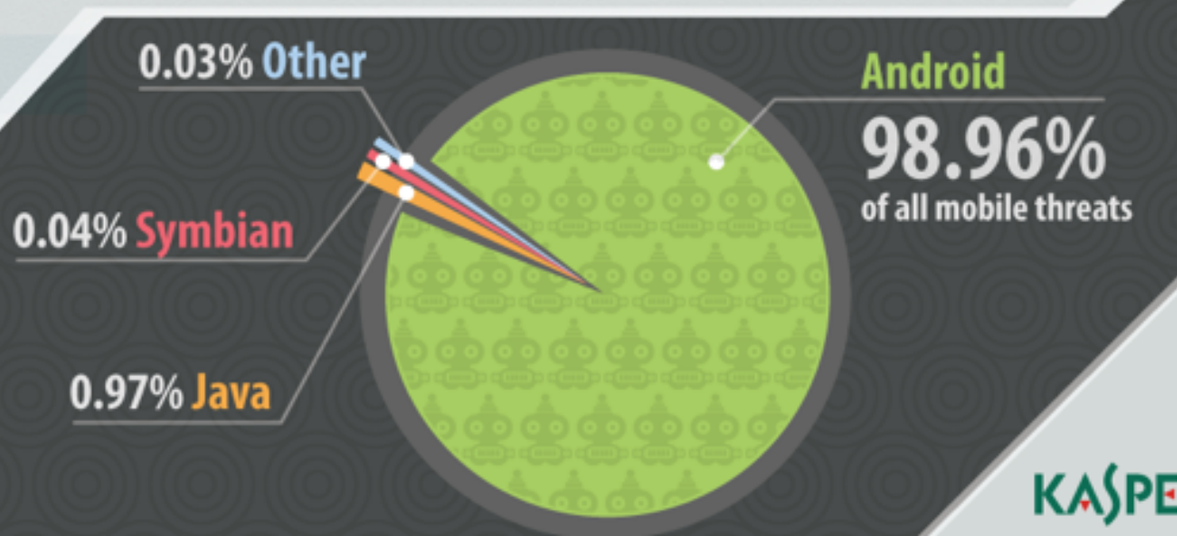
Trojan
AndroidOS.FakeRun.a
displays annoying ads instead of promised game or useful software

Europe

Trojan
AndroidOS.Plangton.a
displays ads and modifies browser bookmarks. Exposes victims to online scams as well

Russia

Trojan
SMS.AndroidOS.Opfake.bo
sends texts to premium-rate numbers, directly stealing victims' money



KASPERSKY lab

Freebird

Open Mobile Technology Workshop

Rio ⟷ NYC

May 30, 2012

INSTITUTE FOR THE FUTURE

Internet at Liberty 2010

The promise and peril of online free expression

Budapest, 20-22 September

PERSONAL DEMOCRACY FORUM

Technology is changing politics.

CDDRL STANFORD

MARCH 9–13, 2012 AUSTIN, TX

SXSW INTERACTIVE

EVENTS

"We fight for the users" by incorporating user-focused, deep connections with activists & reporters through hosted and attended events.

PARTNERSHIPS

We believe in protocols, not products / in partnerships, not proprietary fiefdoms / in building a community of collaborators, not a cacophony of criticism and unnecessary competition / in practical solutions to perilous problems.

EVERYDAY MOBILE INTERNET FREEDOM

Mobile users in censorship states can use Guardian apps to get around the content filters, firewalls and monitors. Everyday citizens use the apps to watch online video, read blogs, communicate safely with friends, and otherwise access whatever content they would like, encouraging open society and culture.

Business people travel all over the world, using foreign networks, bandwidth and systems. At any point, confidential information can be compromised. While some organizations implement solutions, these are often expensive, difficult to use, and not comprehensive

BUSINESS

ACTIVISTS & CITIZEN JOURNALISTS

Tech savvy citizen journalists and activists in the street use Guardian apps to share updates, photos and videos without interception or monitoring by the authorities.

HUMAN RIGHTS DEFENDERS

An undercover human rights researcher traveling through a remote region without mobile data service is able to use Guardian to document local conditions using secured video, audio and photo capture. Data is stored encrypted on the device, and if necessary, it can be safely and quickly erased.

Election monitoring teams distribute low cost Android phones to community organizations to report on issues. Guardian apps assure reports are sent without being tampered with and provides the ability to coordinate via secure instant messaging on low bandwidth networks.

ELECTION MONITORS

Reporters in the field can use Guardian apps to stay in touch with their safety networks, while safeguarding information on contacts, story notes and captured digital media, enabling a new, secure "reporter's notepad". In addition, high-resolution cameras of new Android hardware meet the quality standards for broadcast, print and online production.

FRONTLINE REPORTERS

SECURITY

Apps available publicly all over the world for download, installation and easy use.

ZIM

MOBILE PHONES

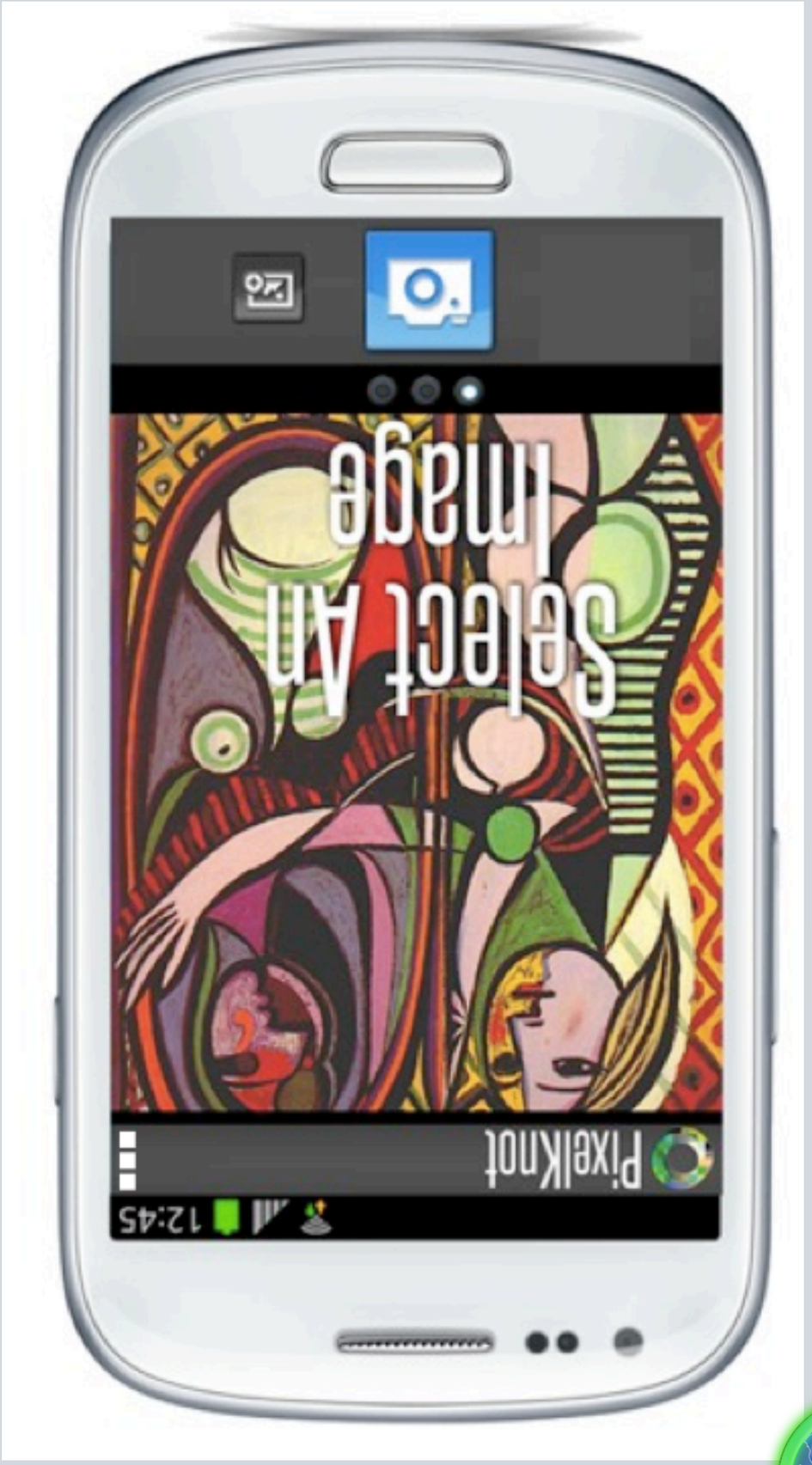
Have 2 computers:
Processor
&
Baseband

- One can be secured but the other serves as a ‘black box’, which is much harder to decipher and understand the security of.

MOBILE PHONES

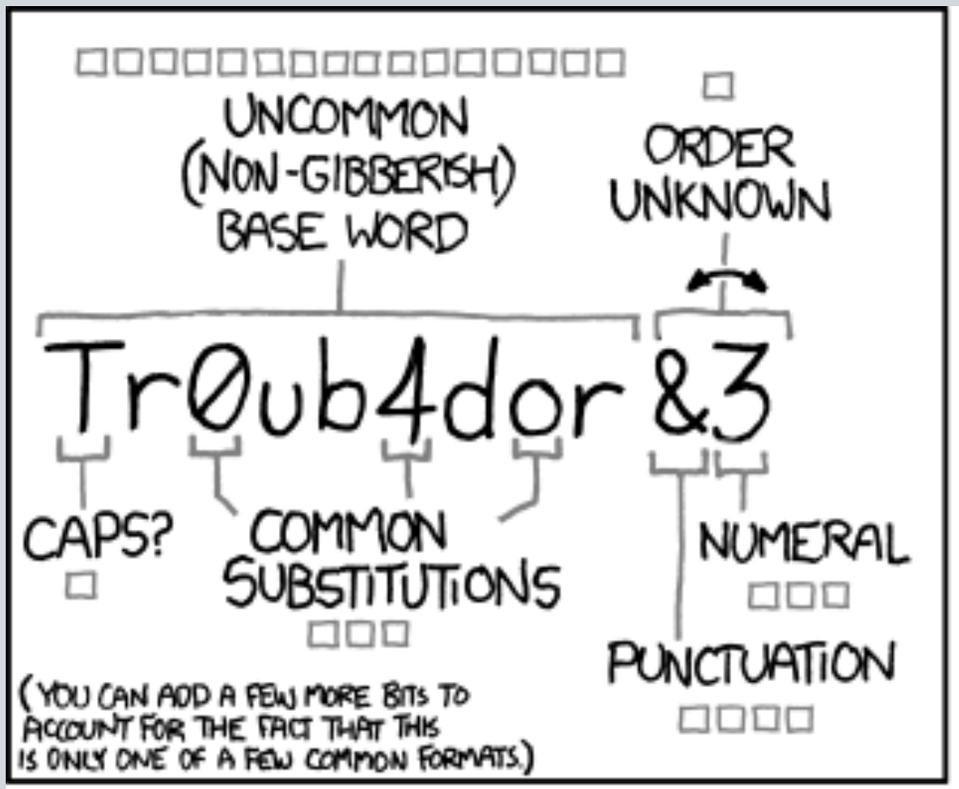
Rooting, ROMing, Unlocking & Jailbreaking

- Rooting/Jailbreaking - Getting ROOT access to control the underlying protocols of and additional privileges to your phone.
- ROMing - Installing a ROM or alternative operating system on your phone. Often requires ROOT access.
- Unlocking - Changing your phone to run on a different mobile phone carrier when it is not initially able to



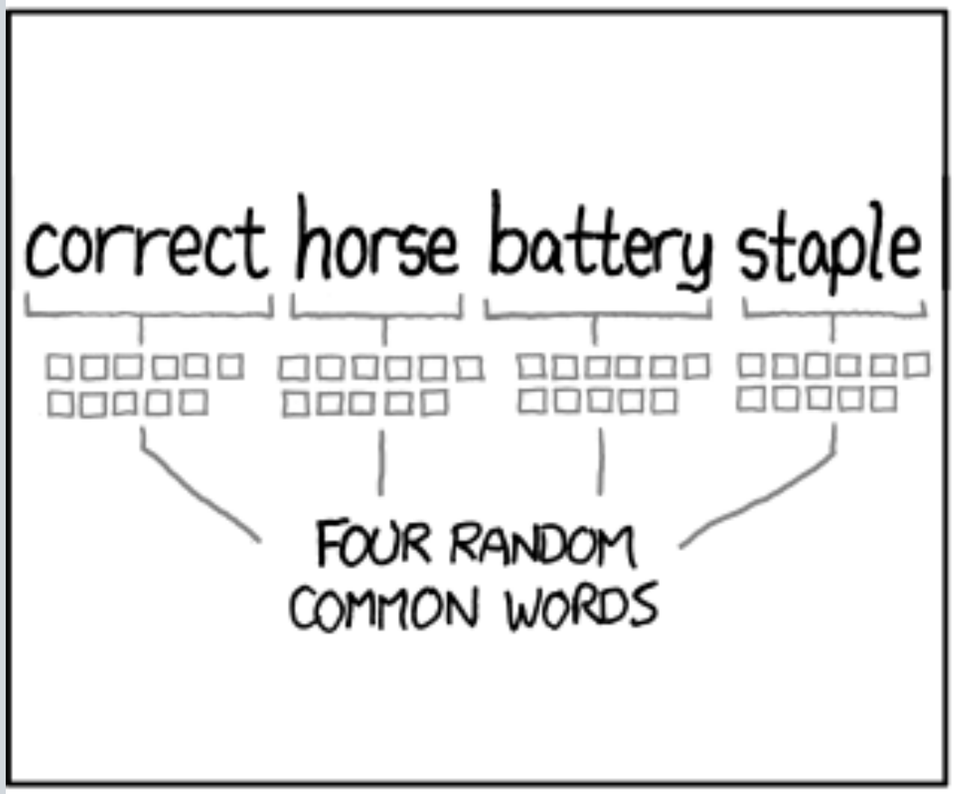
APP PERMISSIONS

PASSWORDS

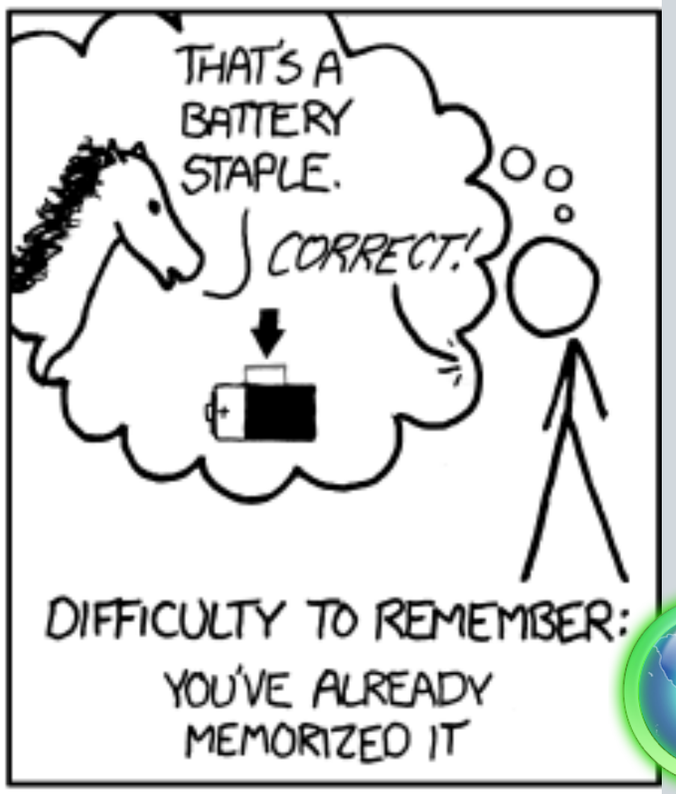

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)


~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY


WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD


correct horse battery staple
FOUR RANDOM COMMON WORDS

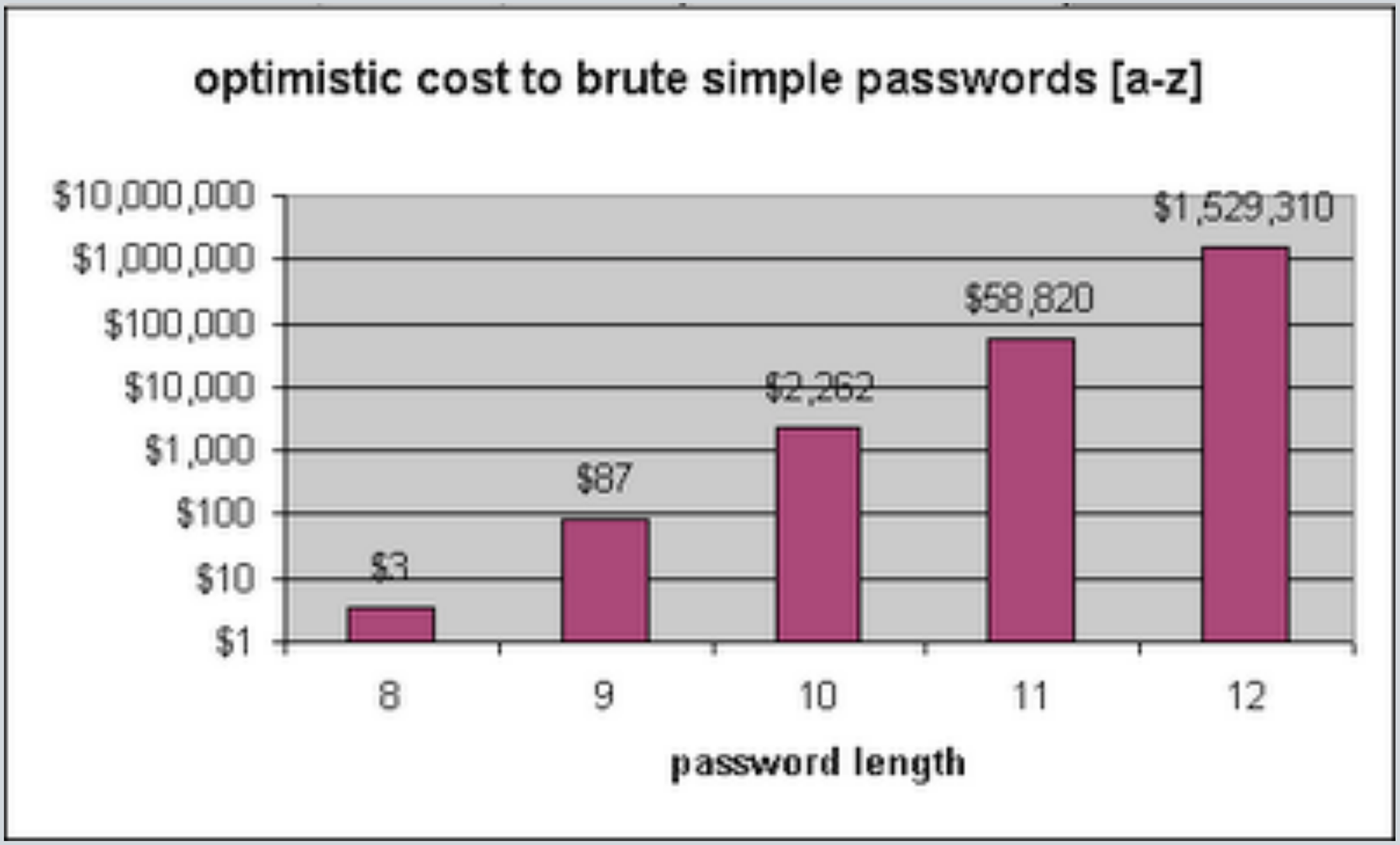

~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD


THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

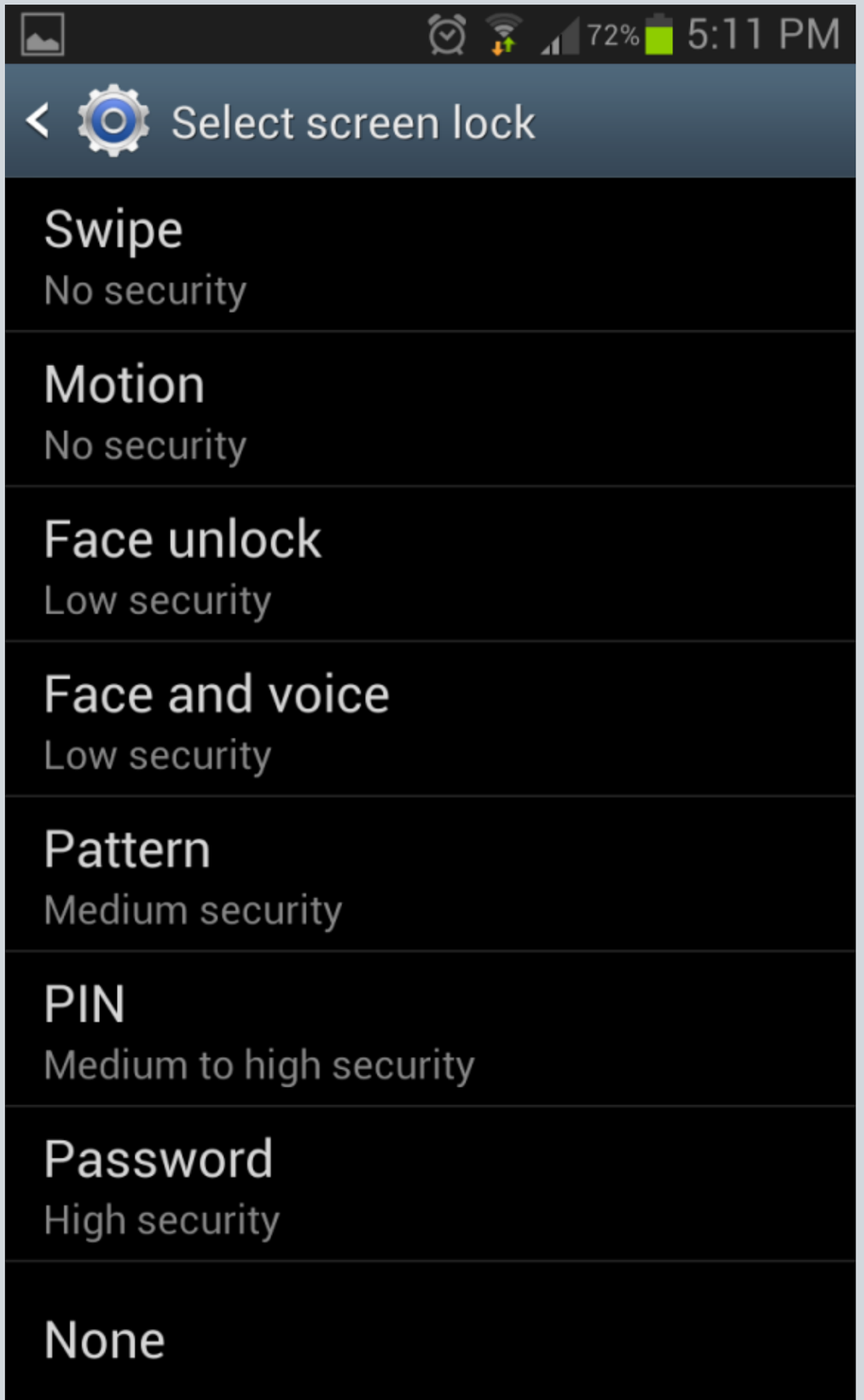
PASSWORDS

123456
password
12345678
qwerty
abc123
111111
monkey
12345
0
letmein
trustno1
dragon
1234567
baseball
superman
iloveyou
sunshine
1234
princess
starwars
whatever
shadow
cheese
123123
nintendo
football
computer
fuckyou
654321
blahblah

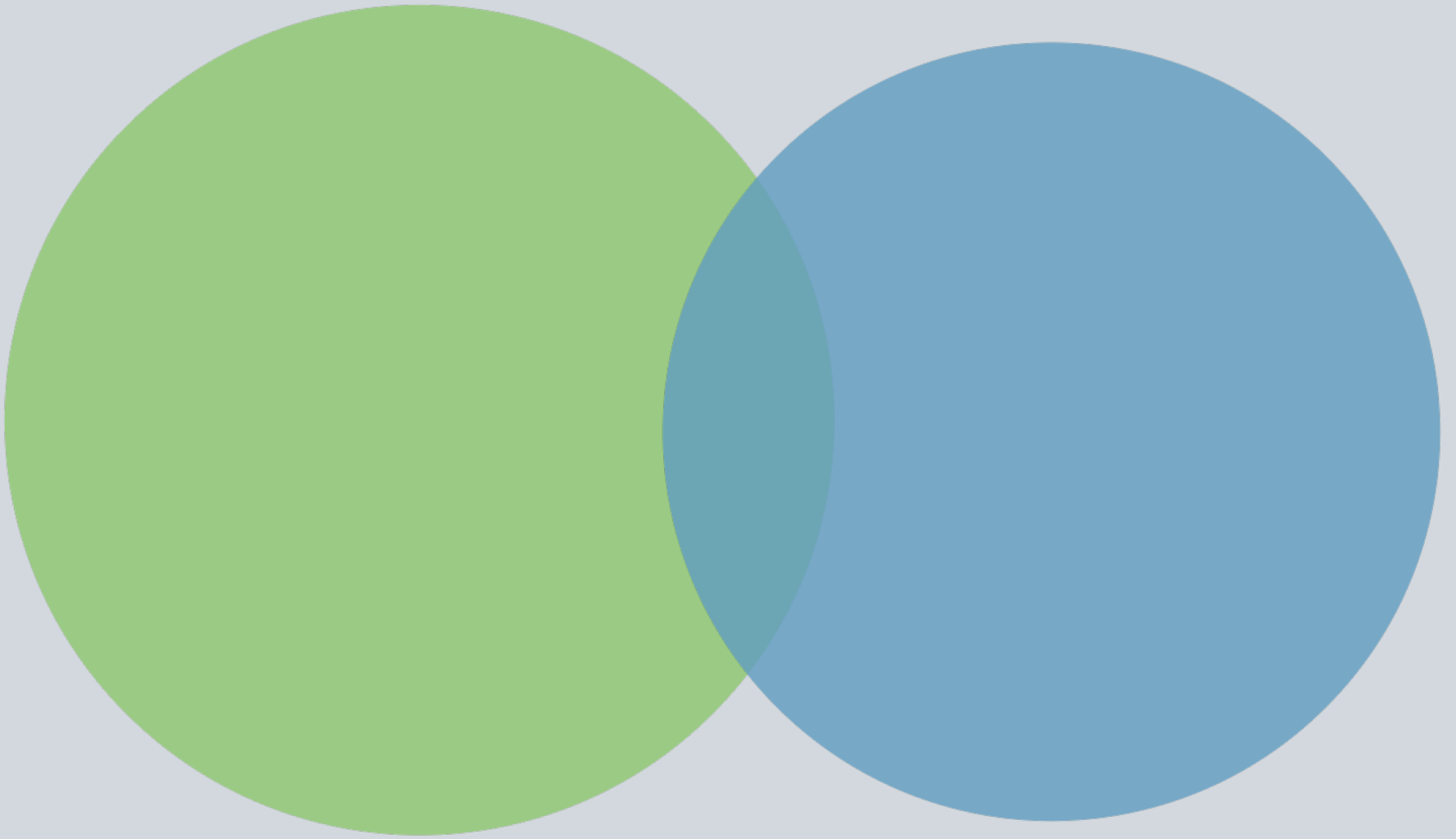
PASSWORDS


optimistic cost to brute simple passwords [a-z]
$10,000,000
$1,000,000
$100,000
$10,000
$1,000
$100
$10
$1
$3
$87
$2,262
$58,820
$1,529,310
8
9
10
11
12
password length

PHONE SCREEN LOCK

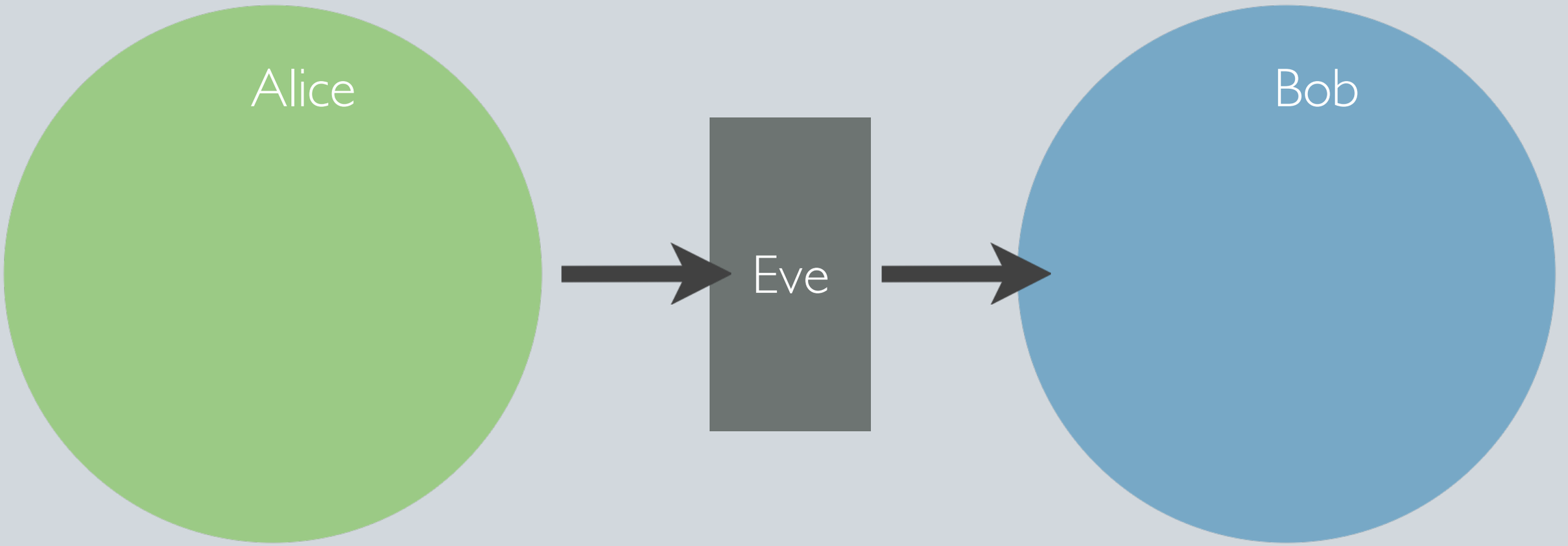


ENCRYPTION



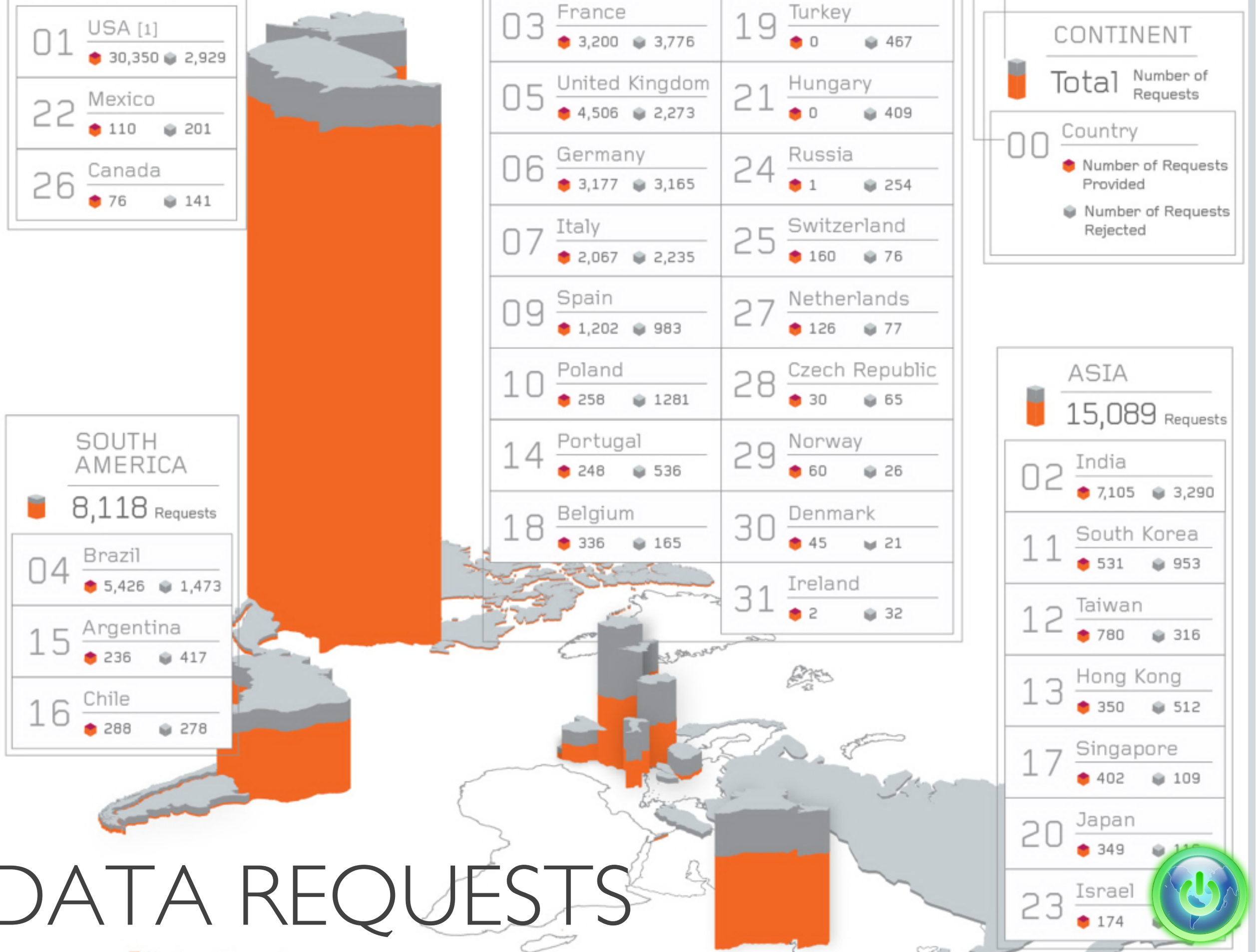
Public Key Cryptography :
Diffie-Hellman Key Exchange

END TO END ENCRYPTION



Public Key Cryptography :
Diffie-Hellman Key Exchange

DATA REQUESTS



01	USA [1]	30,350	2,929
22	Mexico	110	201
26	Canada	76	141
03	France	3,200	3,776
05	United Kingdom	4,506	2,273
06	Germany	3,177	3,165
07	Italy	2,067	2,235
09	Spain	1,202	983
10	Poland	258	1281
14	Portugal	248	536
18	Belgium	336	165
19	Turkey	0	467
21	Hungary	0	409
24	Russia	1	254
25	Switzerland	160	76
27	Netherlands	126	77
28	Czech Republic	30	65
29	Norway	60	26
30	Denmark	45	21
31	Ireland	2	32

SOUTH AMERICA

8,118 Requests

04	Brazil	5,426	1,473
15	Argentina	236	417
16	Chile	288	278

CONTINENT

Total Number of Requests

00 Country

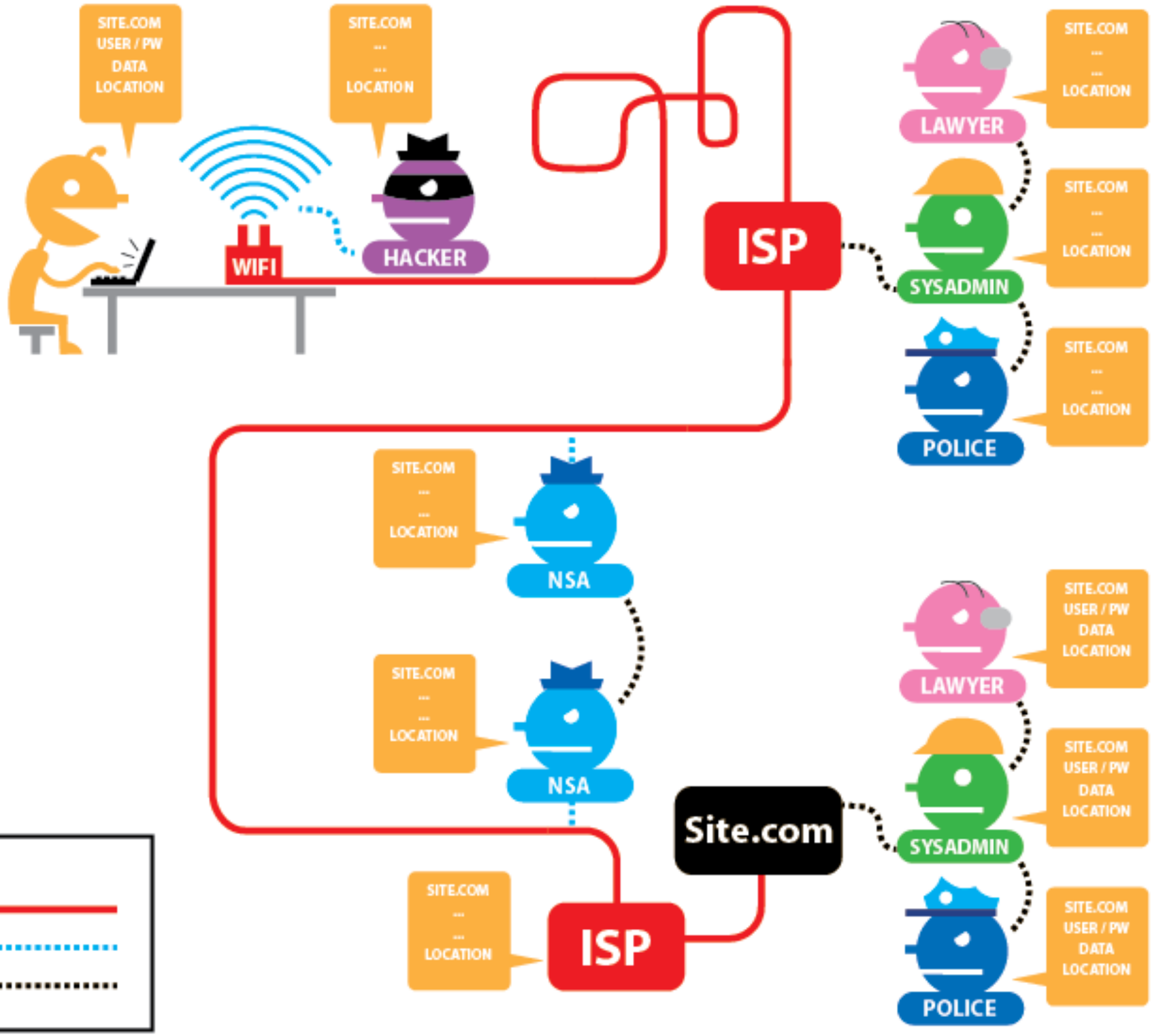
- Number of Requests Provided
- Number of Requests Rejected

ASIA

15,089 Requests

02	India	7,105	3,290
11	South Korea	531	953
12	Taiwan	780	316
13	Hong Kong	350	512
17	Singapore	402	109
20	Japan	349	
23	Israel	174	

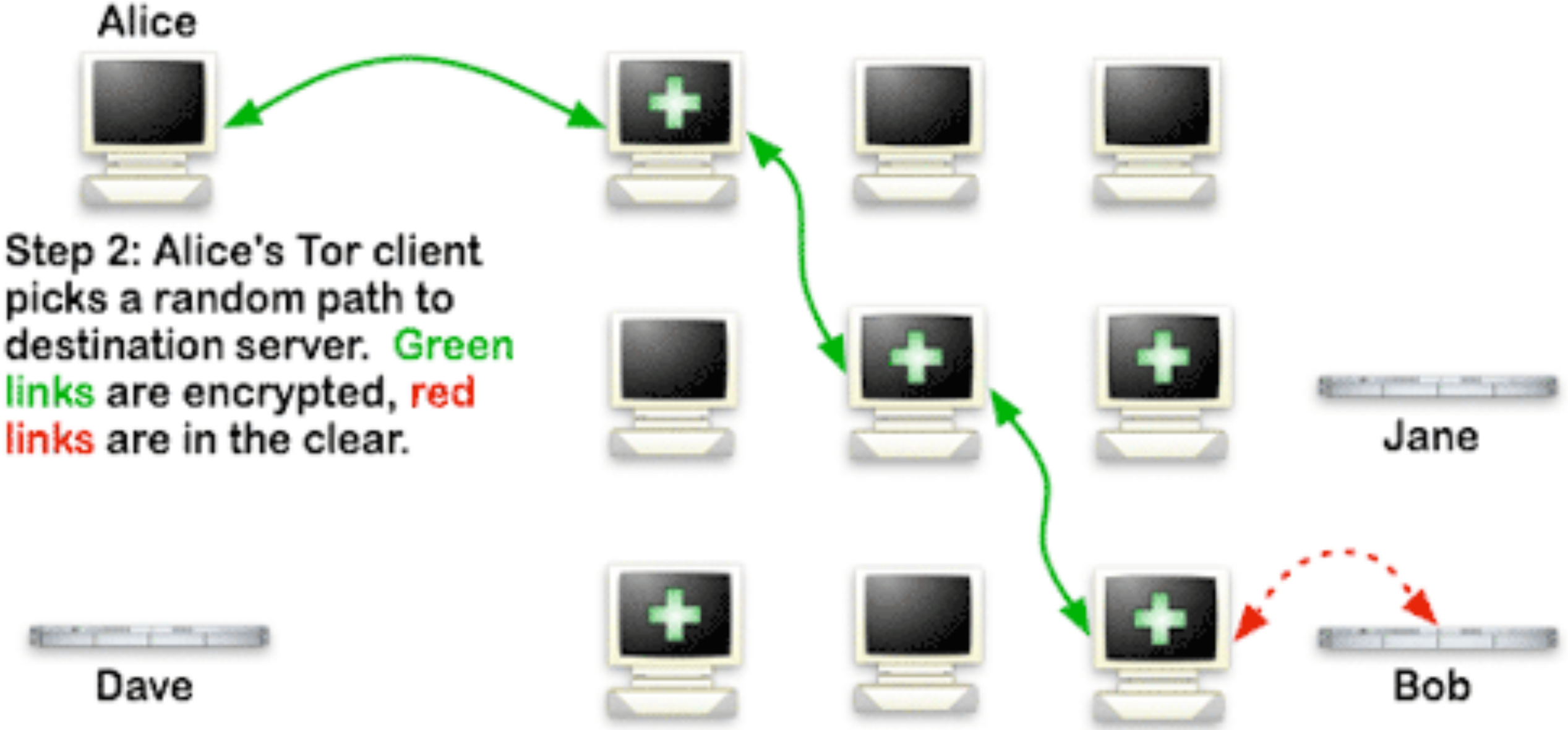
INTERNET BROWSING



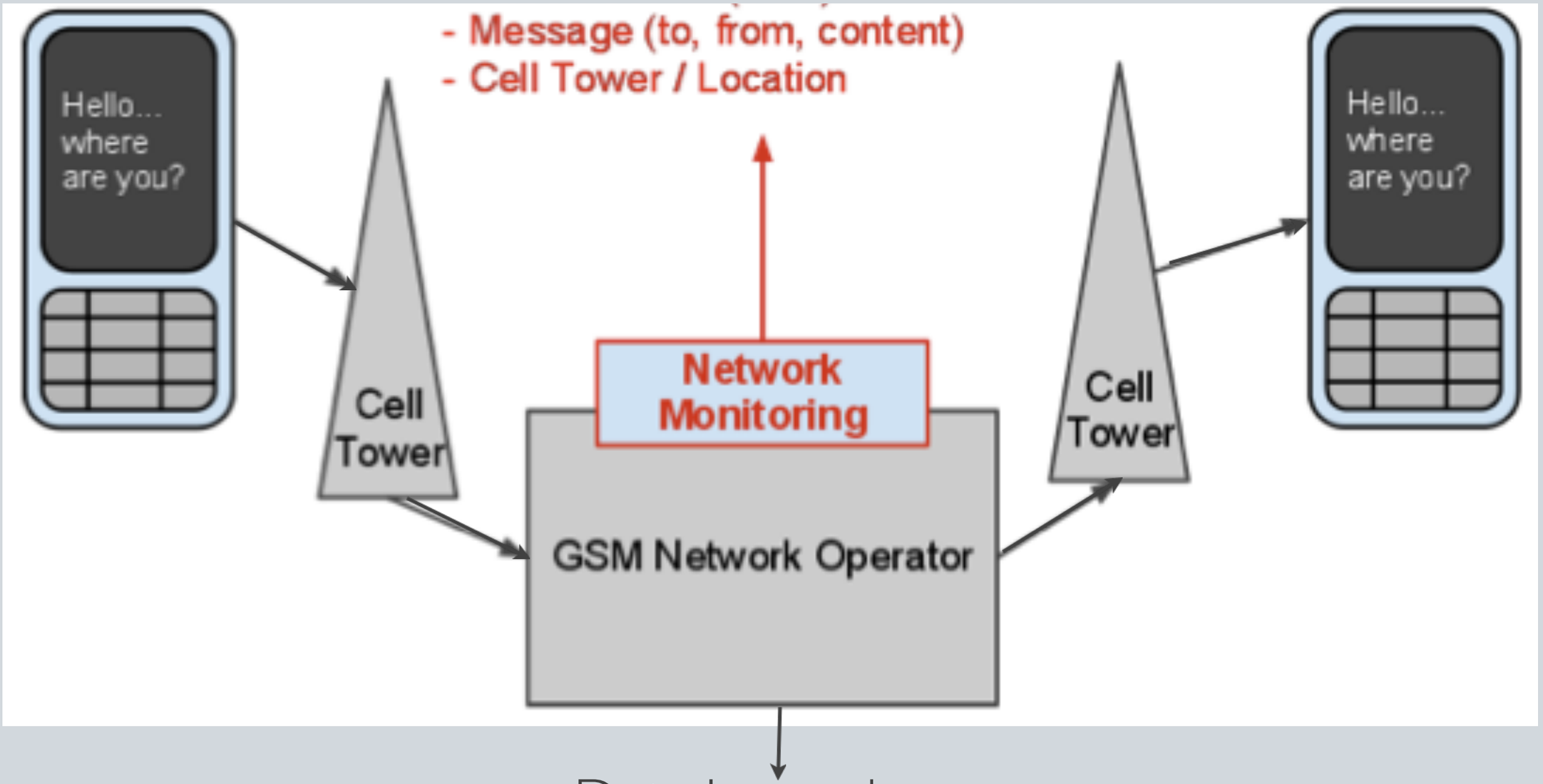
SECURE BROWSING

SECURE BROWSING

ANONYMOUS BROWSING



MOBILE NETWORKS



Data Logged :

- Device Equipment ID (IMEI)
- Subscriber ID (IMSI) / Phone #
- Message (to, from, content)
- Cell Tower / Location

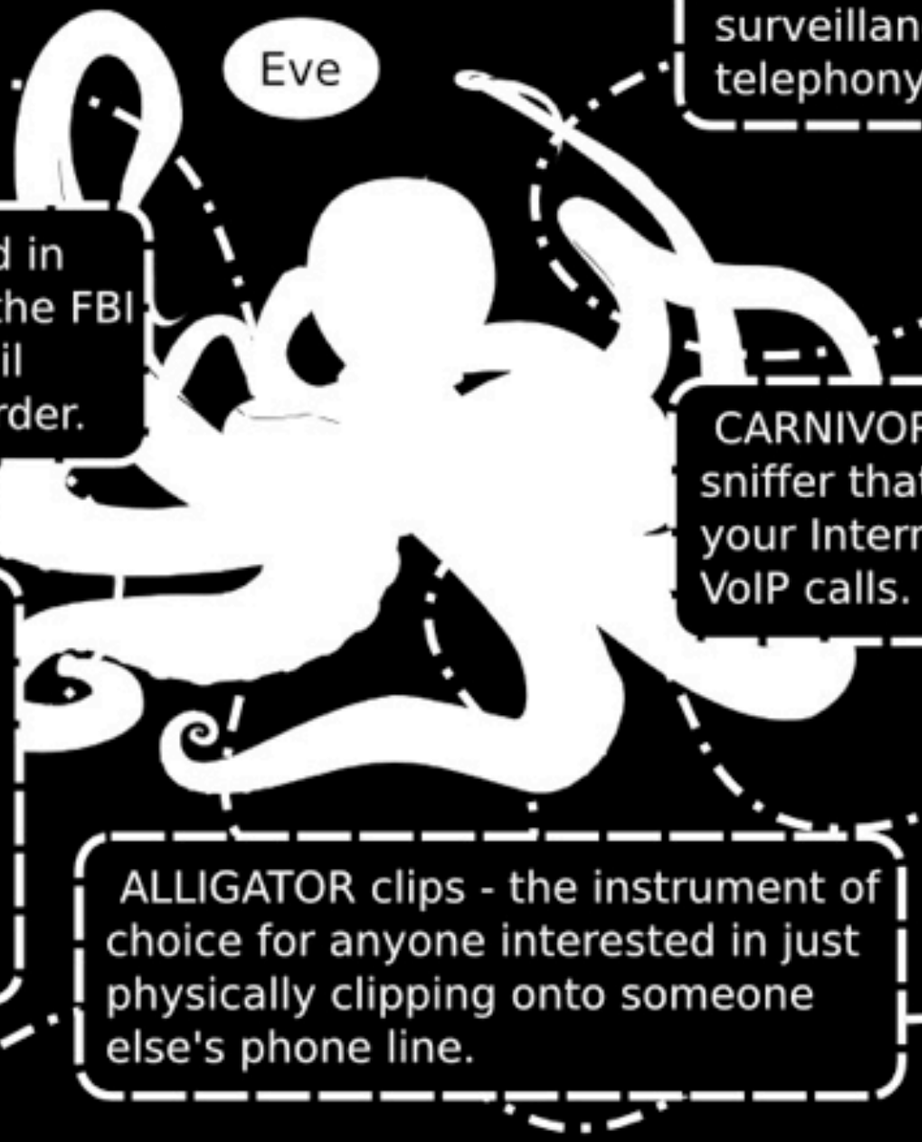
21st Century Phone Call Security

Bob

ECHELON - A signals intelligence collection and analysis network operating globally to intercept phone calls and data. Dates back to the 1960s.

CALEA - 1994 U.S. wiretapping law, mandates built-in surveillance for digital telephony.

Eve



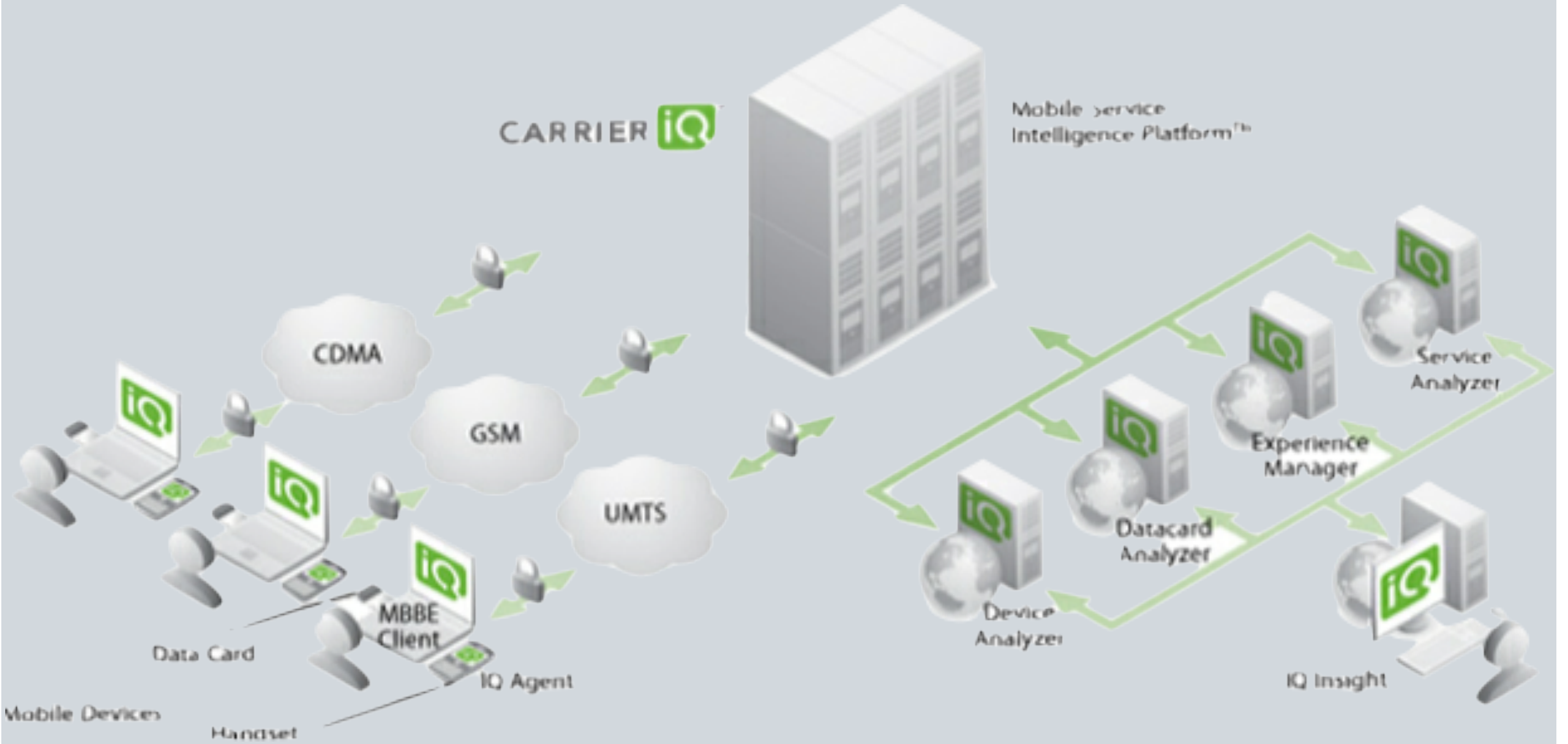
The PATRIOT Act - passed in 2001, clears the way for the FBI to search phone and email records without a court order.

CARNIVORE - FBI packet sniffer that can monitor all of your Internet traffic, including VoIP calls. Originated in 1997.

NSA - found in 2005 to be engaged in warrantless monitoring of phone calls by executive order of the President with AT&T's cooperation.

ALLIGATOR clips - the instrument of choice for anyone interested in just physically clipping onto someone else's phone line.

Alice


CARRIER iQ
Mobile Service
Intelligence Platform™
CDMA
GSM
UMTS
MBBE
Client
Data Card
IQ Agent
Mobile Devices
Handset
Service
Analyzer
Experience
Manager
Datacard
Analyzer
Device
Analyzer
IQ Insight

3 IN 10 PEOPLE ARE LIKELY TO CLICK ON AN UNSAFE LINK ON THEIR MOBILE DEVICE.

3 X >

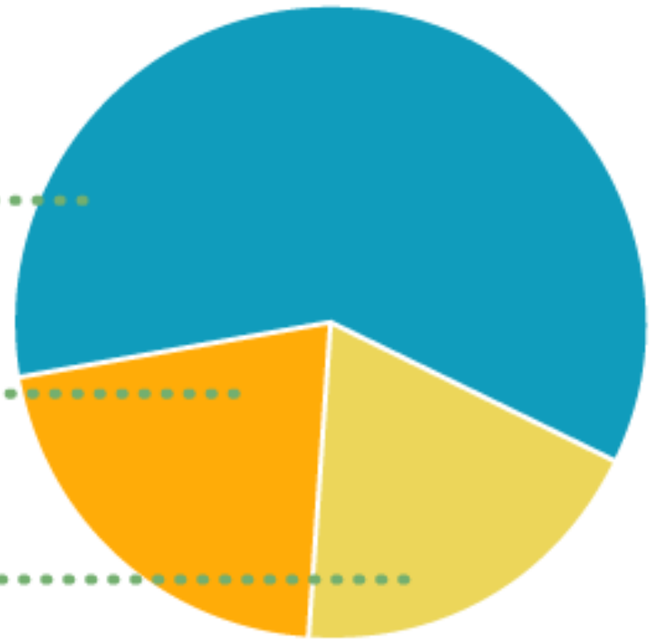
PEOPLE ARE 3 TIMES MORE LIKELY TO SUCCUMB TO A PHISHING ATTACK FROM THEIR PHONE THAN ON A DESKTOP COMPUTER.

CATEGORY BREAKDOWN OF UNSAFE LINKS OPENED BY MOBILE USERS

60% MALICIOUS

19% COMPROMISED

21% PHISHING



TOP TYPES OF APPS THAT HAVE BEEN BUNDLED WITH MALWARE

GAMING

UTILITY

PORN APPS

OVER THE LAST MONTH (JULY 2011), LOOKOUT HAS DETECTED MORE ANDROID MALWARE THAN IN ALL OF 2010.

TOP THREE ANDROID THREATS

GGTRACKER
DROIDDREAM
DROIDDREAMLIGHT

WHAT CAN HAPPEN IF A USER DOWNLOADS AN APP WITH THIS MALWARE?

PERSONAL DATA STOLEN

MONEY STOLEN (UNWANTED PHONE BILL CHARGES)

THE APPLICATION CAN TAKE CONTROL OF THE PHONE*

lookout MOBILE SECURITY

* Leading to unwanted charges, theft of

HOW THE ANDROID *GEINIMI* TROJAN WORKS

GEINIMI TROJAN FACTS

- Targeting Android users in China
- Posted on third party app stores
- Found in more than 25 repackaged apps

1. Developer creates a game called Monkey Jump.

LEGITIMATE DEVELOPER

2. Developer uploads game to Android Market.

ANDROID MARKET

3. Malicious Developer takes legitimate game and repackages it with malware.

4. Malicious Developer uploads game to 3rd party app store.

3RD PARTY APPS

3RD PARTY APP STORE

5. User downloads game with malware.

MALICIOUS DEVELOPER

END USER

6. Malicious developer can control the phone remotely and access users' private information.

- SEND LOCATION
- SEND CONTACT INFO
- SEND AND READ SMS MESSAGES
- PLACE PHONE CALLS
- SILENTLY DOWNLOAD FILES
- LAUNCH WEB BROWSER

AND MORE...

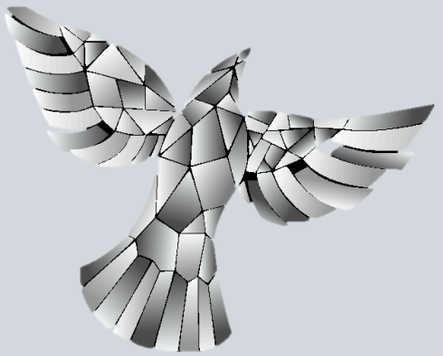
lookout MOBILE SECURITY

REMOTE EAVESDROPPING

REMOTE EAVESDROPPING

The Guardian Project aims to create easy to use mobile apps, open-source firmwares, and customized, commercial mobile phones that can be used and deployed around the world, by any person looking to protect their communications from unjust intrusion.

Whether your are an average citizen looking to affirm your rights or an activist, journalist or humanitarian organization looking to safeguard your work in this age of global communication, Guardian is the solution for your mobile security needs.



THE GUARDIAN PROJECT
https://guardianproject.info

USER TOOLS

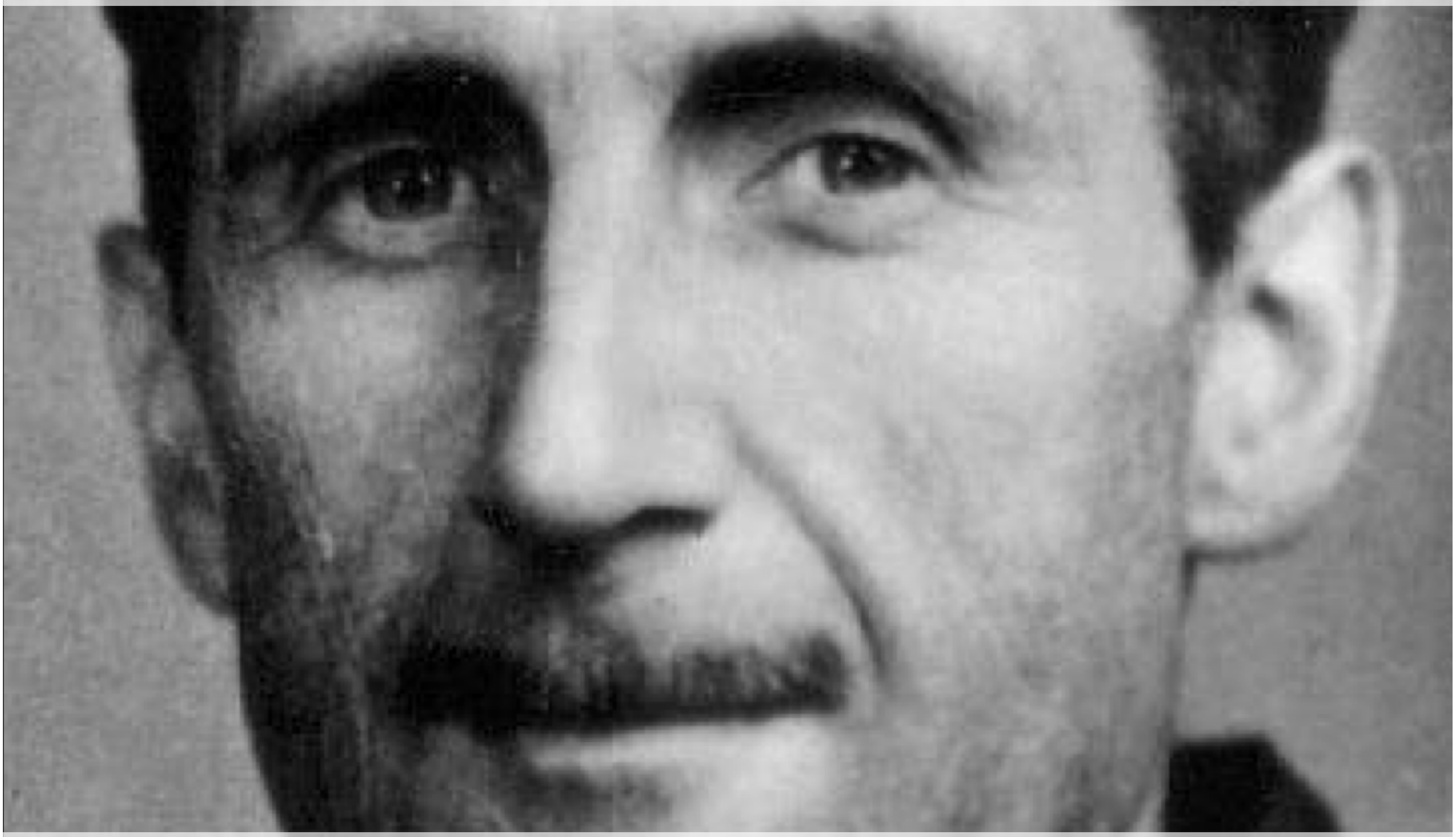
Apps available publicly all over the world for download, installation and easy use.

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

WHY ORWELL?



WHEN YOU CAN

So you want to bypass censorship on Android?

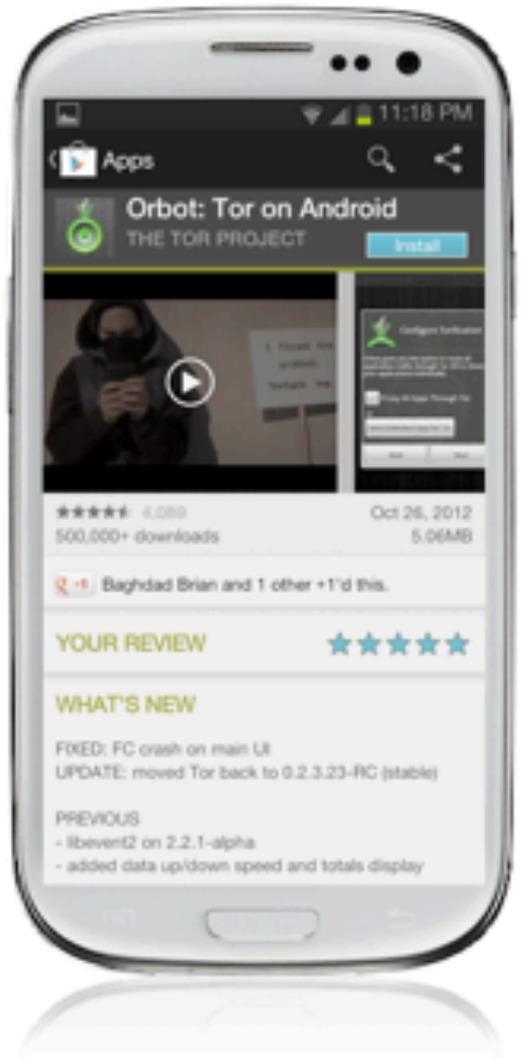
Yes! How do I get find a tool to surf freely and anonymously?

So you want to bypass censorship on Android?

1. Open the Google Play Store. Easy. Next?
It's blocked. Help!

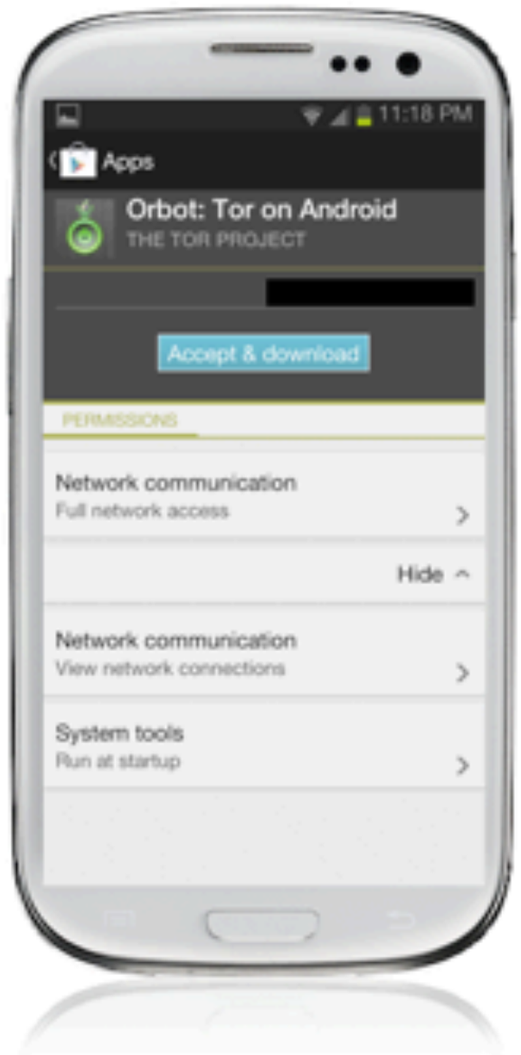
So you want to bypass censorship on Android?

2. Search for *Orbot*. Got it.



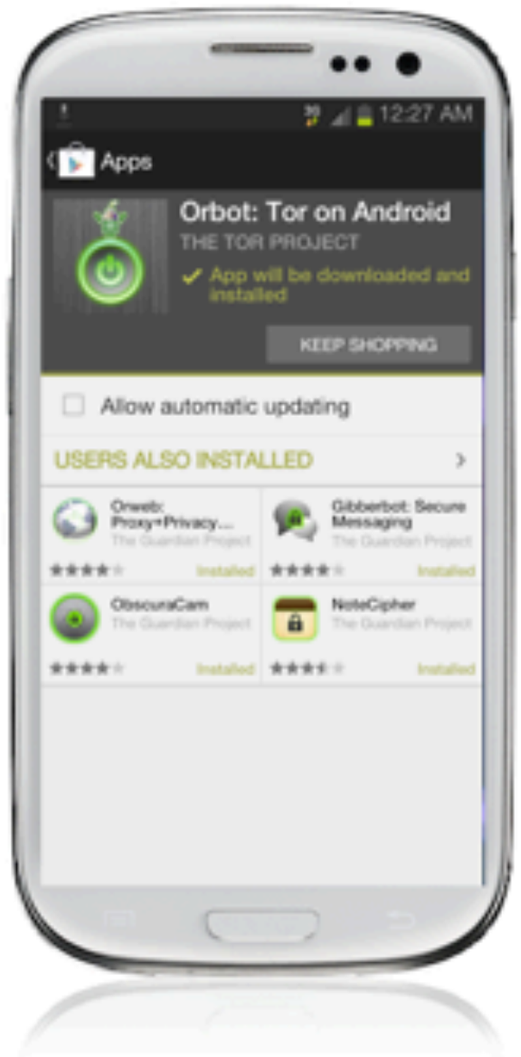
So you want to bypass censorship on Android?

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?

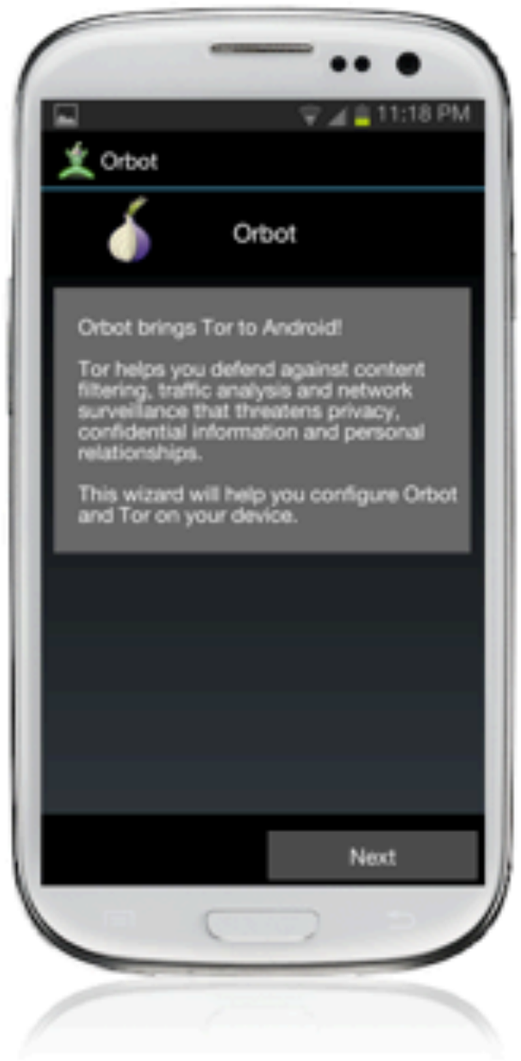
5. Open *Orbot*. Done.

So you want to bypass censorship on Android?

6. Choose your language and get started. Let's go with English.

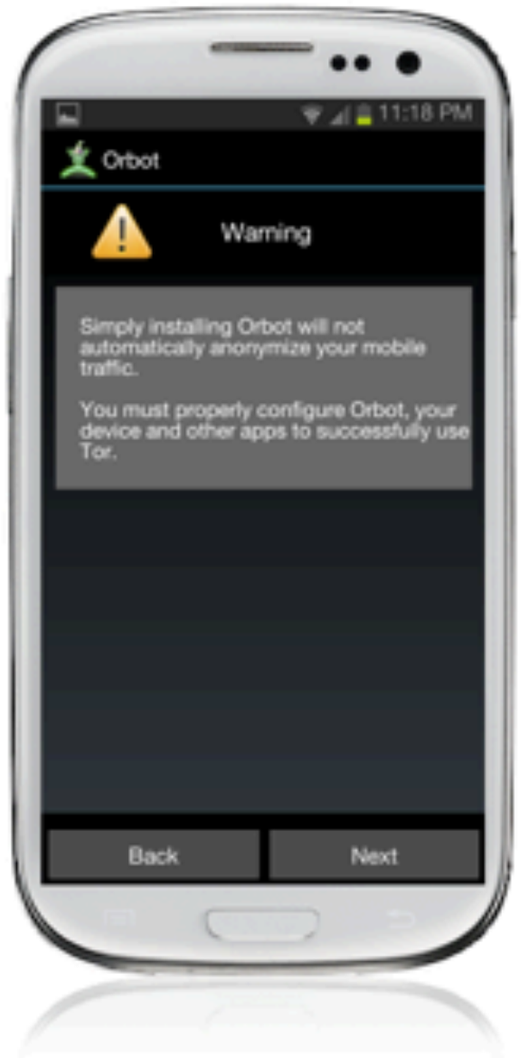
So you want to bypass censorship on Android?

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



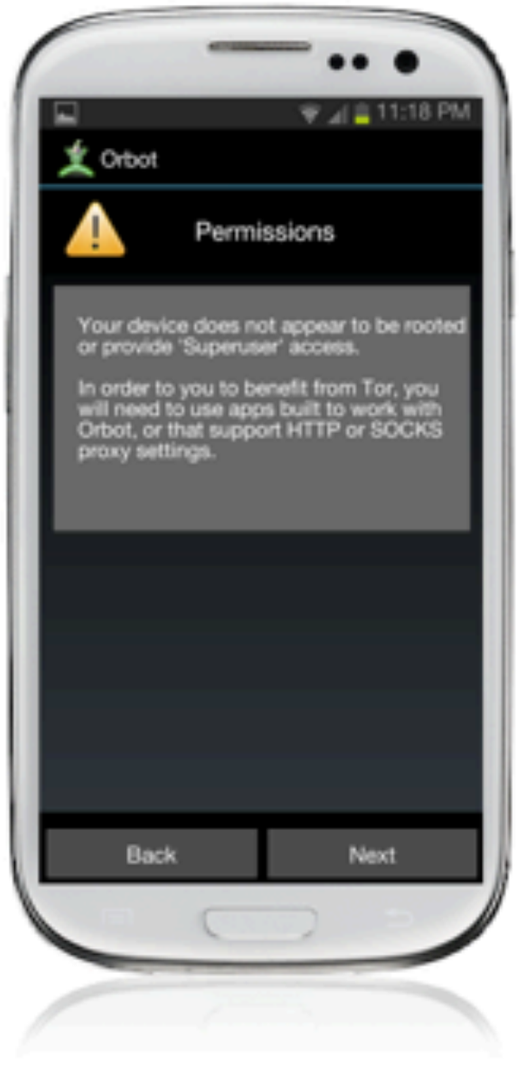
So you want to bypass censorship on Android?

Is it really secure? We break it down.



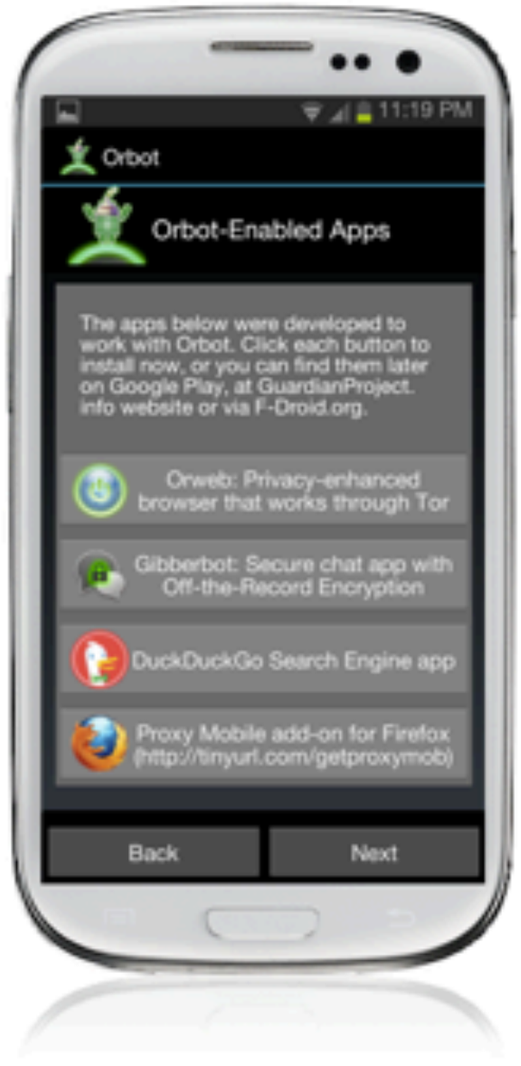
So you want to bypass censorship on Android?

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



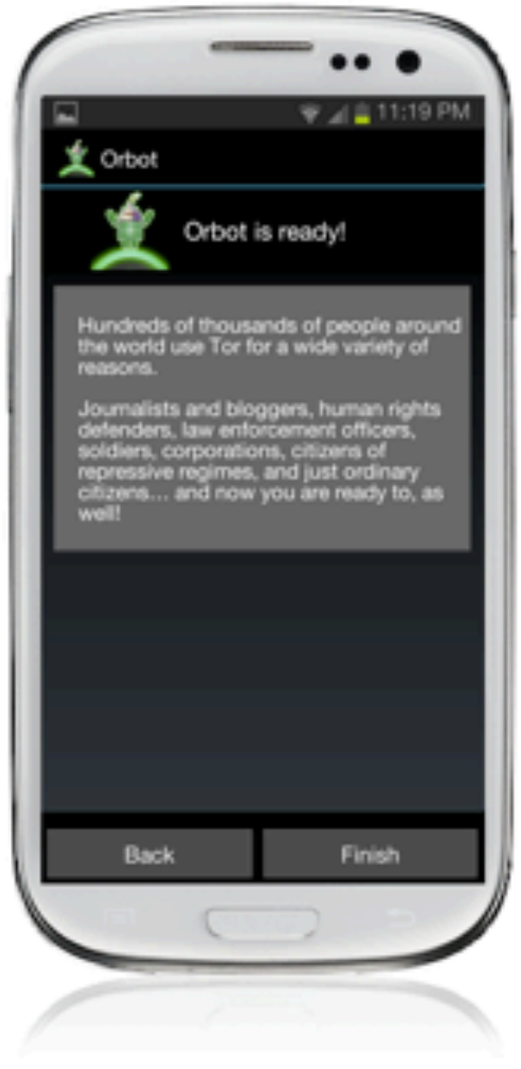
So you want to bypass censorship on Android?

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?

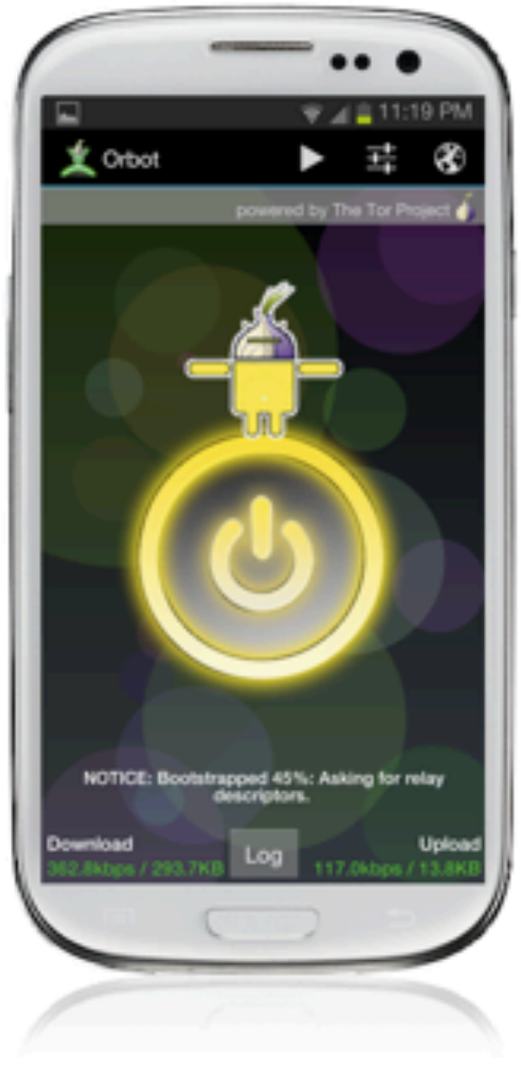
8. Now we long press the button to getting started. Pressing!

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?

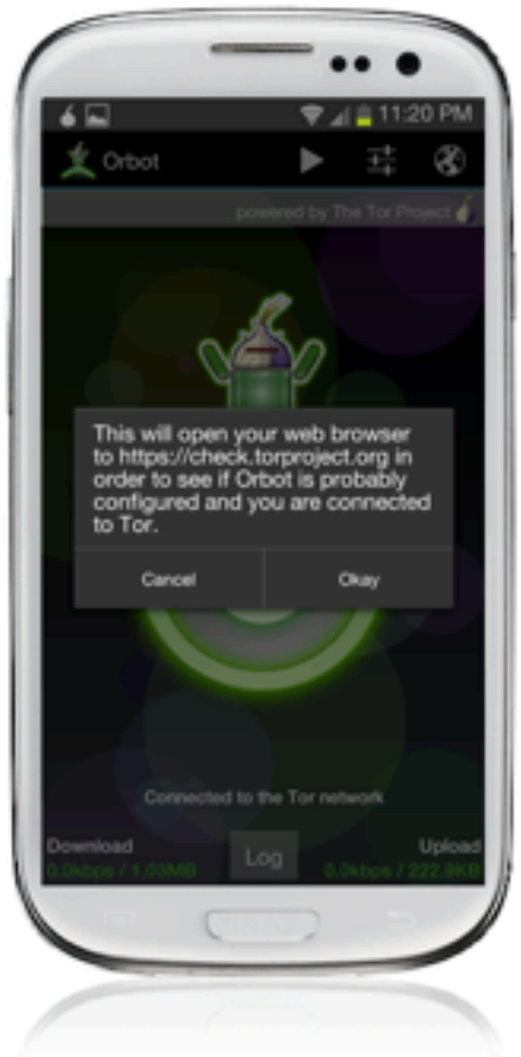
Orbot turns green when it's connected to Tor.

So you want to bypass censorship on Android?

9. Let's confirm we can now bypass the censors. Ok, how?

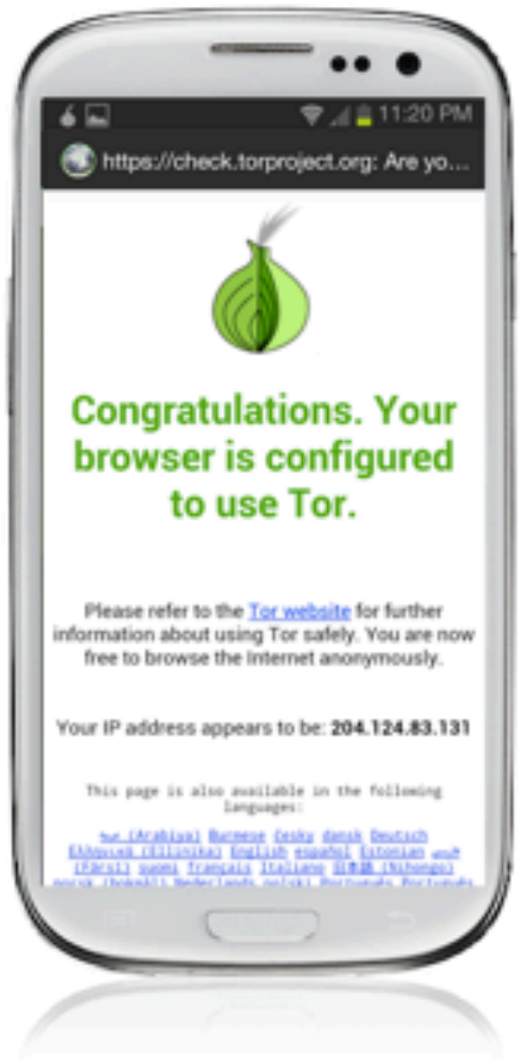
So you want to bypass censorship on Android?

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.*

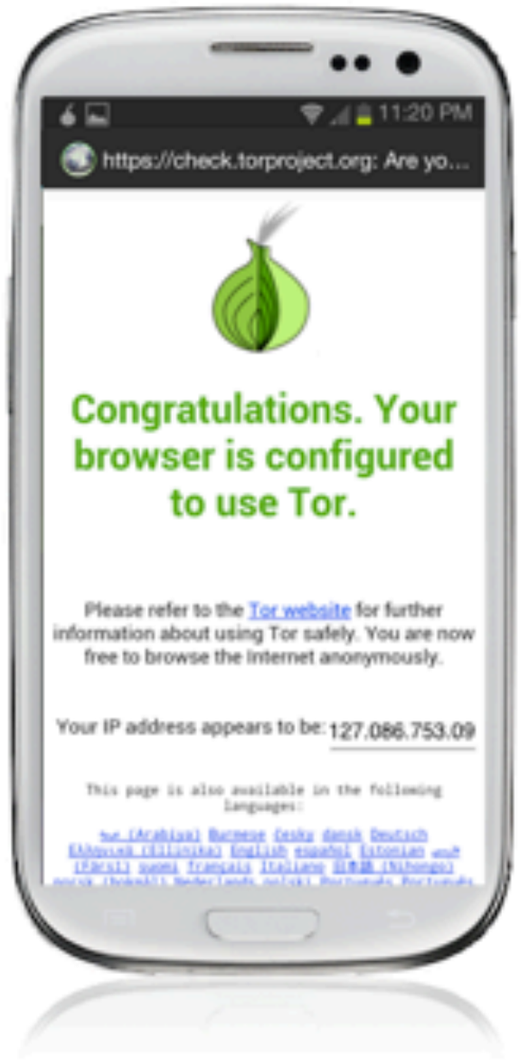


So you want to bypass censorship on Android?

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

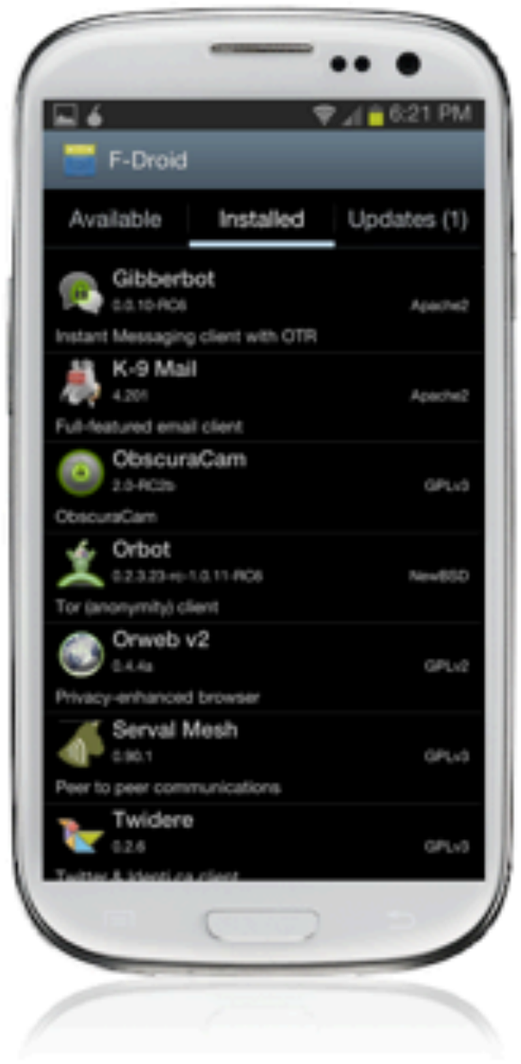
Cool. What do I enter?

So you want to bypass censorship on Android?

Enter: https://guardianproject.info/repo/ (don't forget the s!)
Done. Where are the apps?

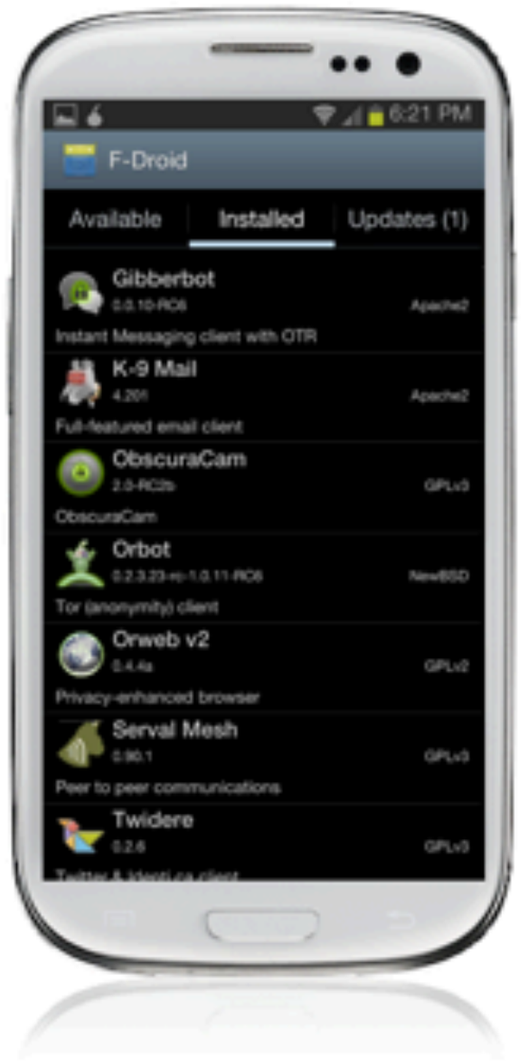
So you want to bypass censorship on Android?

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.



ENABLE HTTP PROXY

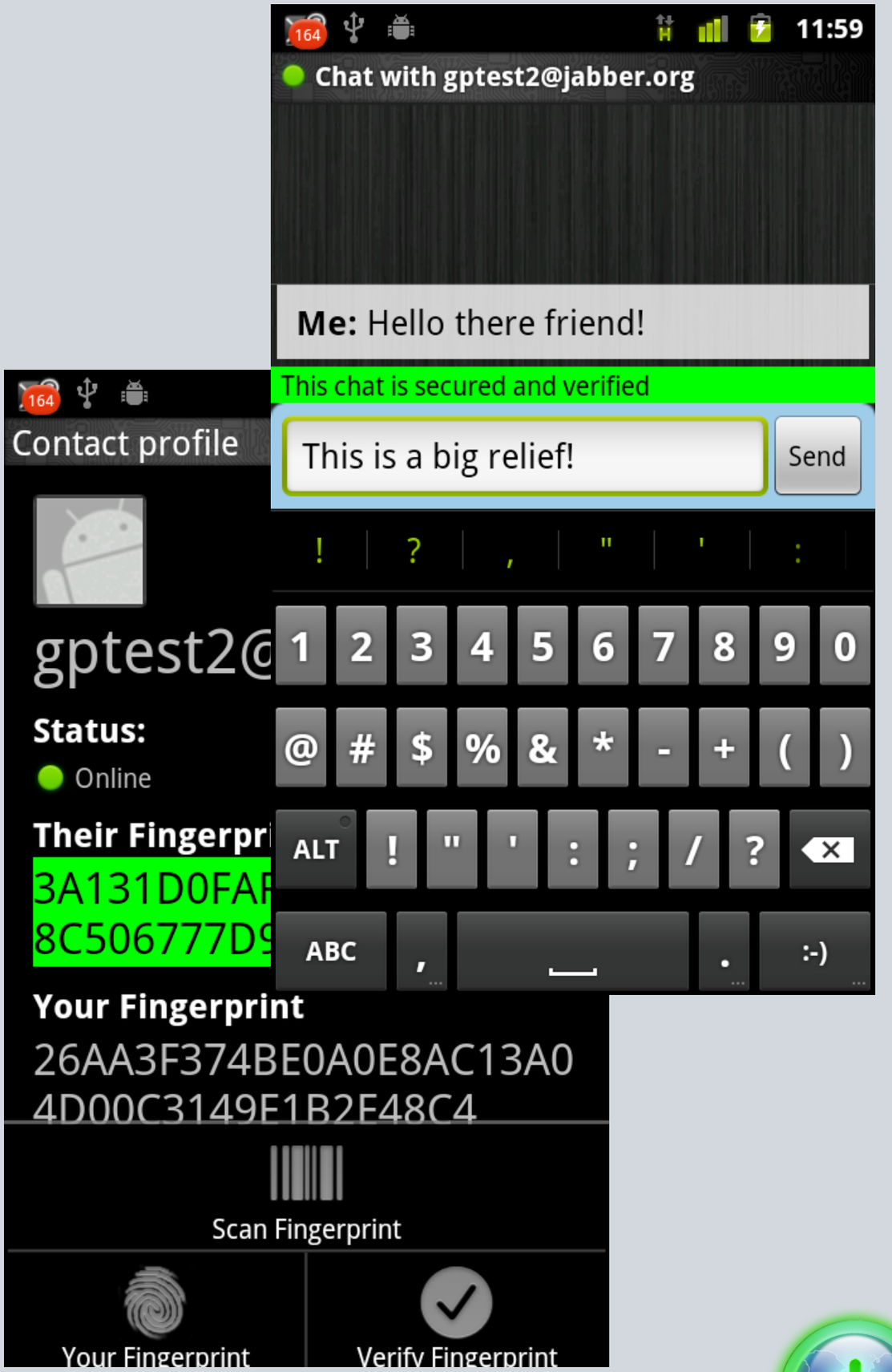
PROXY HOST: LOCALHOST

PROXY PORT: 8118

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?

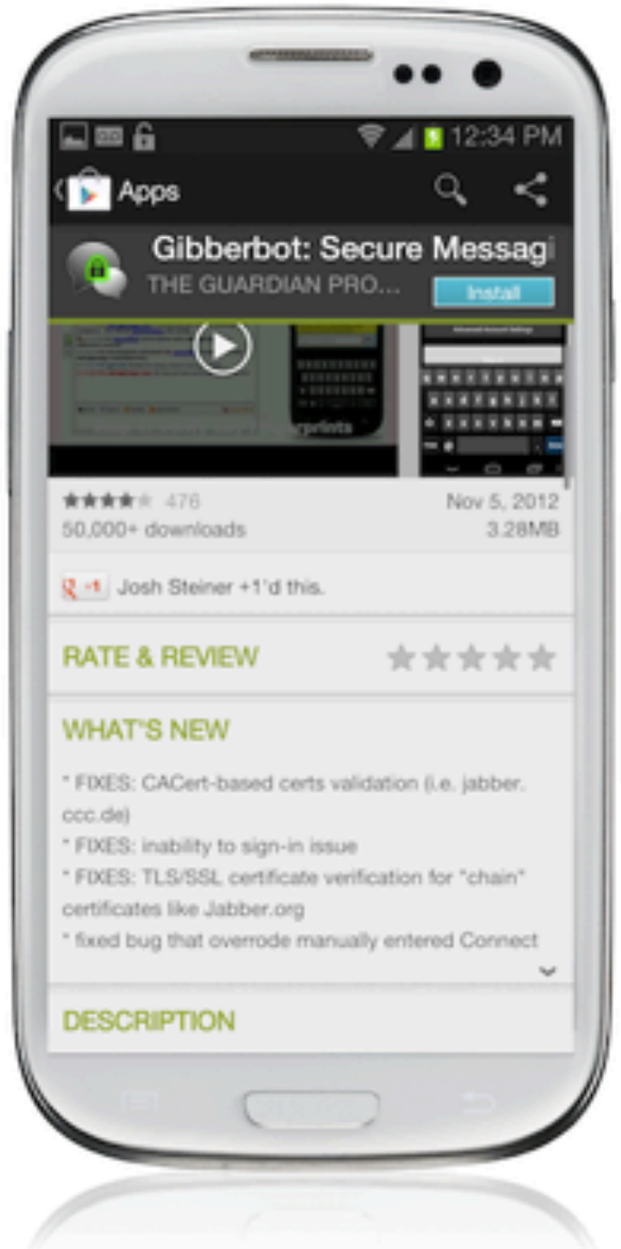
Yes. How do I do that?

So you want to chat securely on Android?

1. Open the Google Play Store. Easy. Next?
It's blocked. Help!

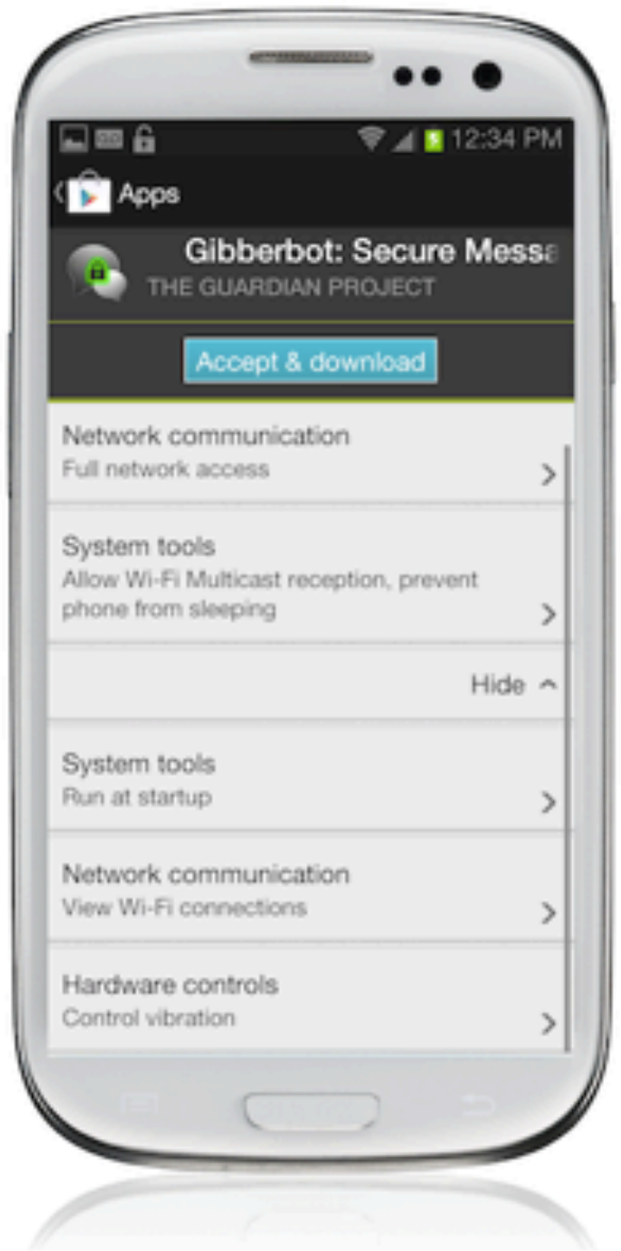
So you want to chat securely on Android?

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?

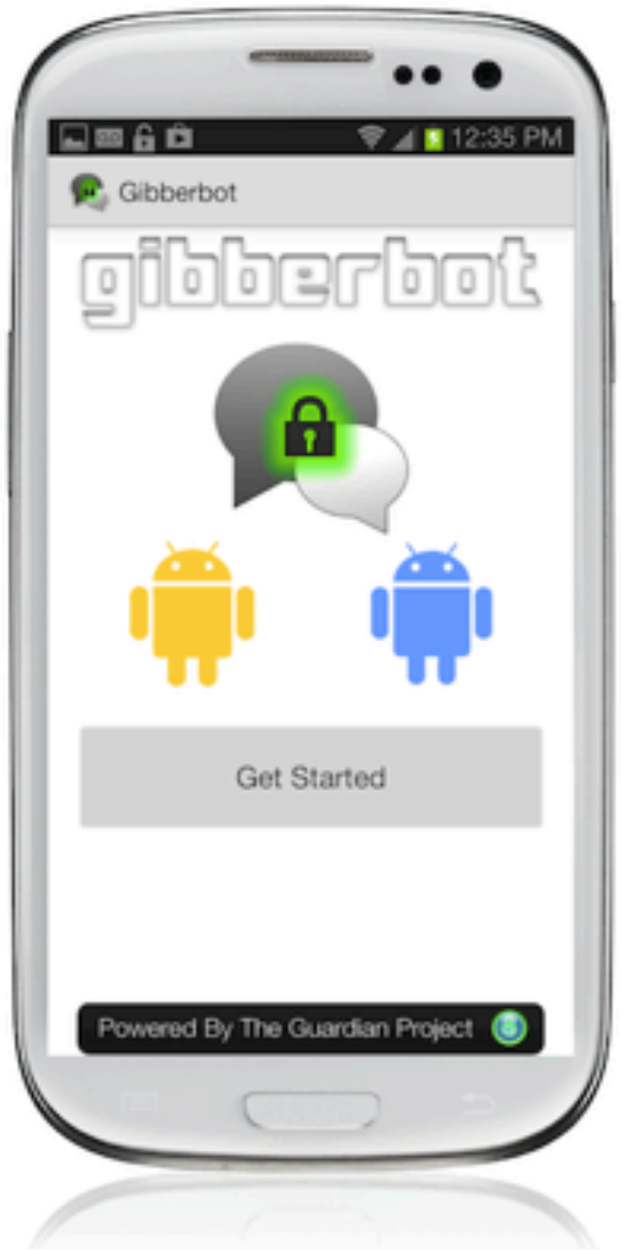
4. Open *Gibberbot*. Done.

So you want to chat securely on Android?

5. Choose your language and get started. Let's go with English.

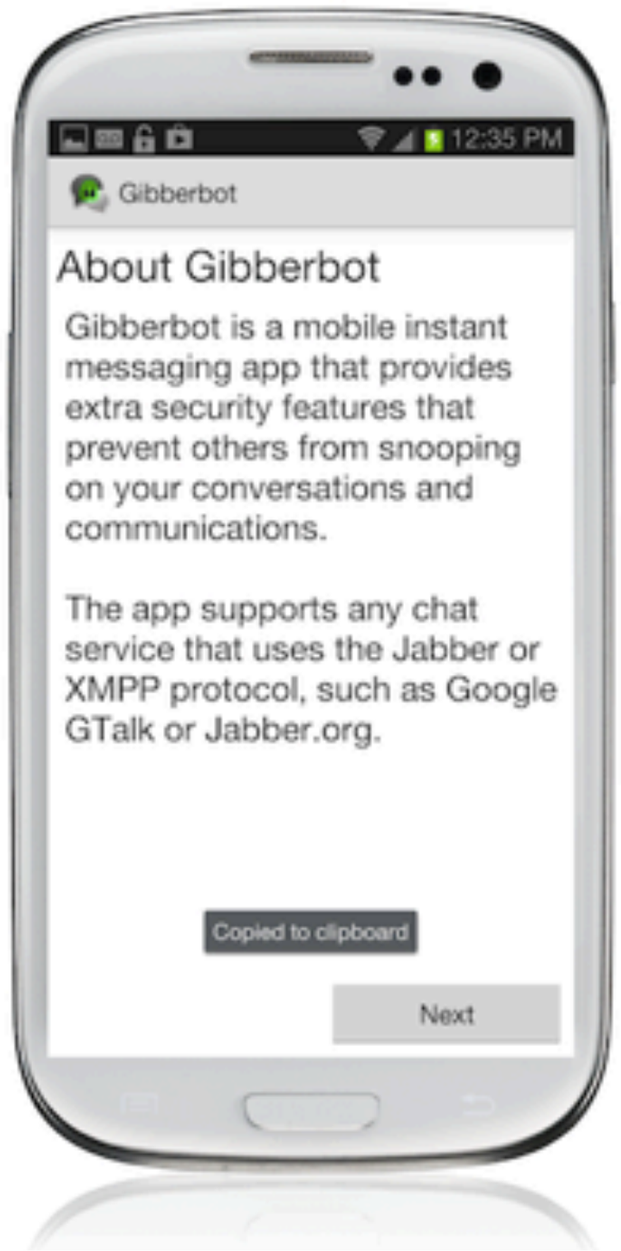
So you want to chat securely on Android?

Now we're getting started.



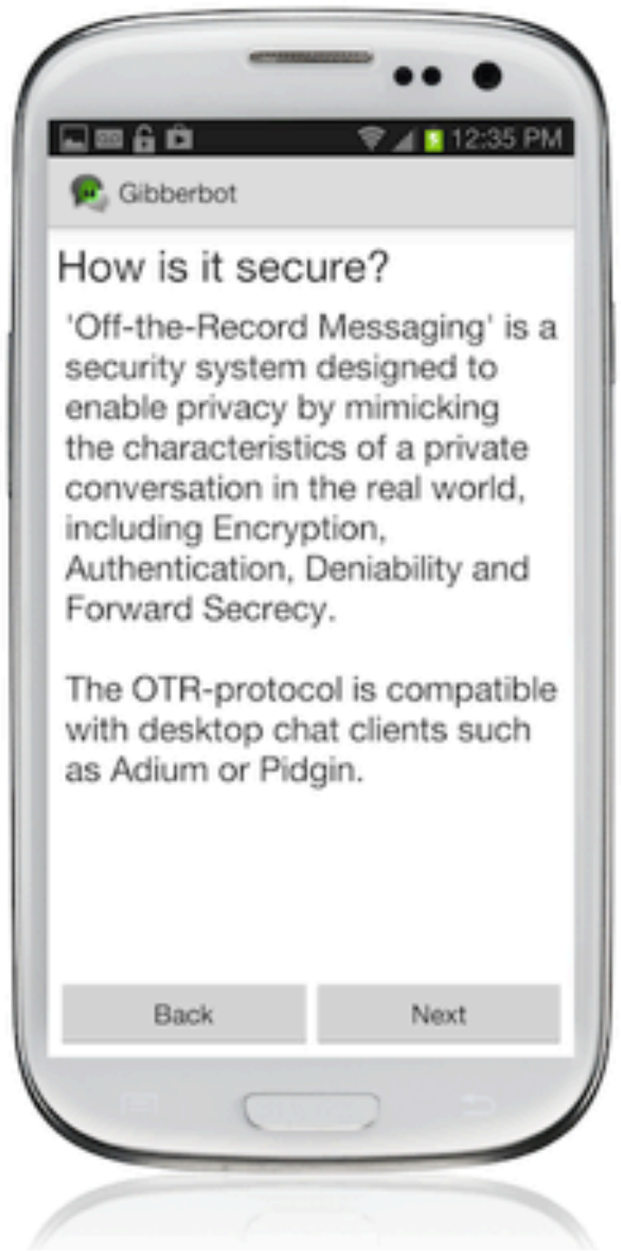
So you want to chat securely on Android?

It will tell you about our project.



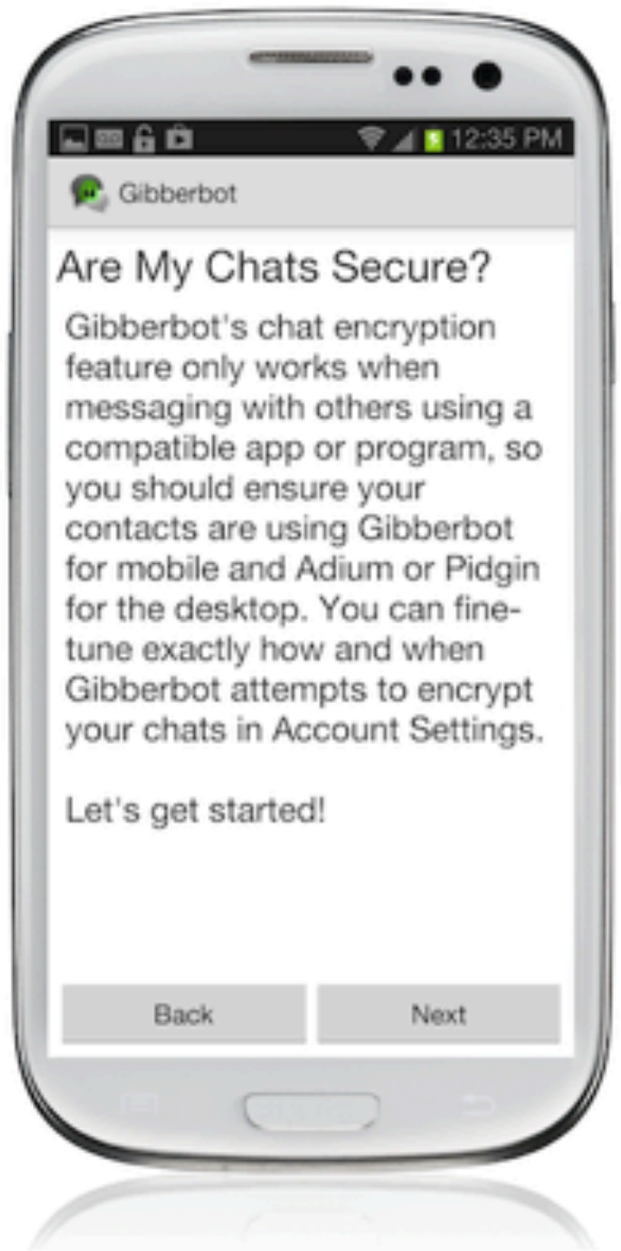
So you want to chat securely on Android?

Is it really secure? We break it down.



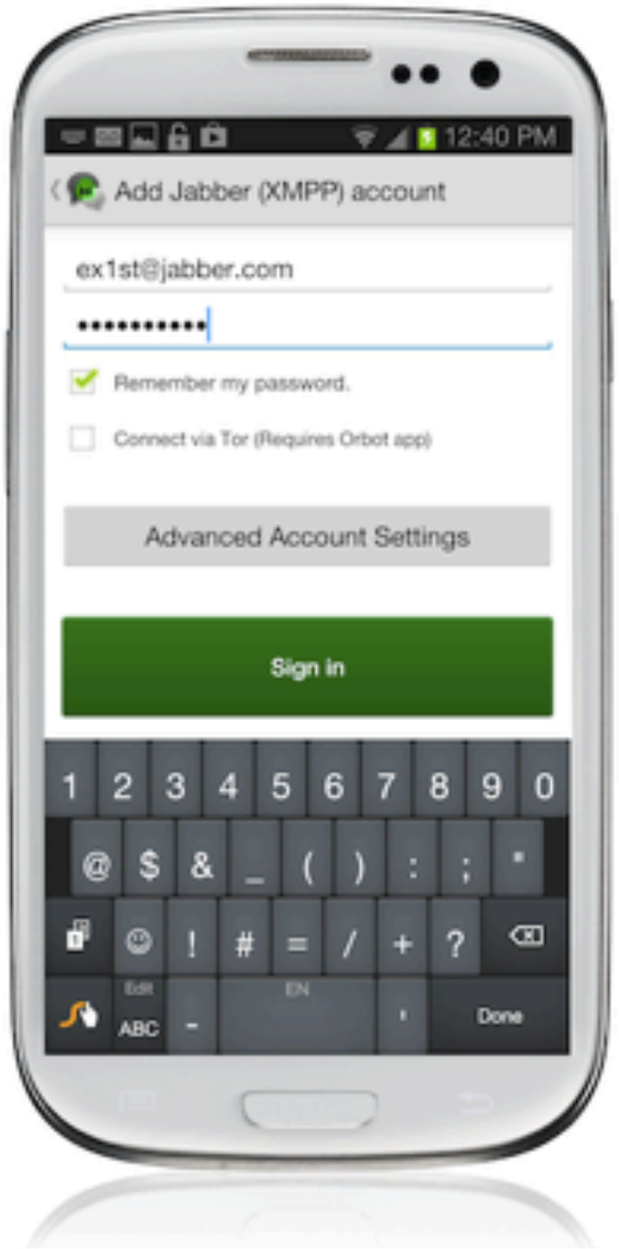
So you want to chat securely on Android?

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!

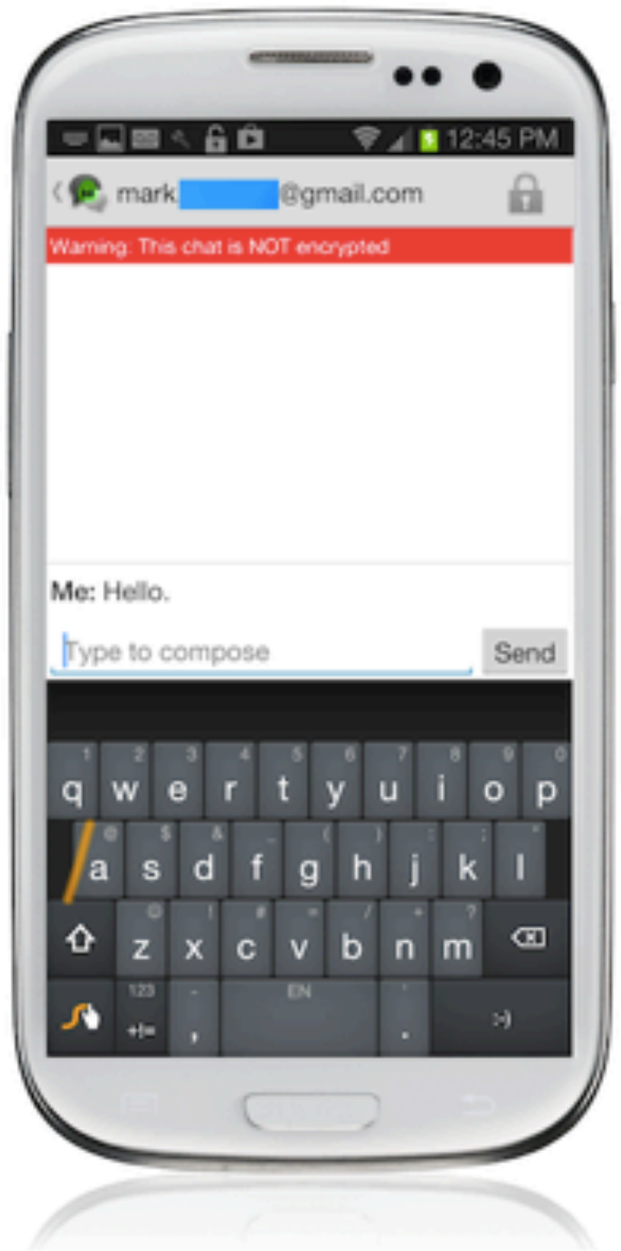


So you want to chat securely on Android?

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

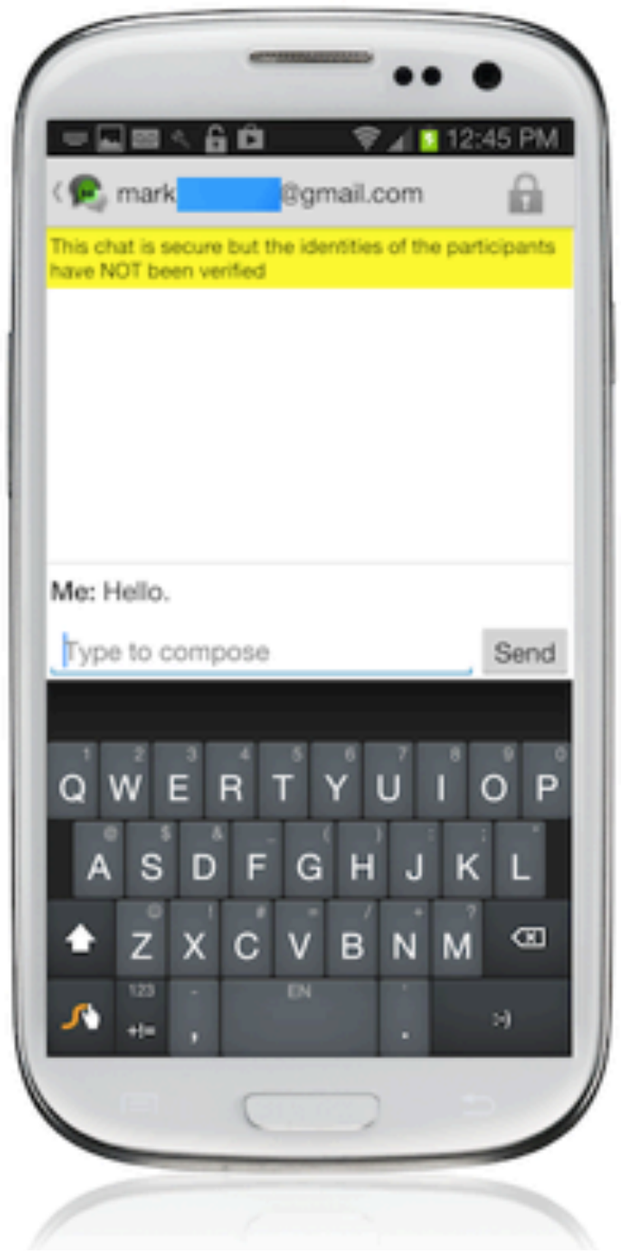
So you want to chat securely on Android?

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



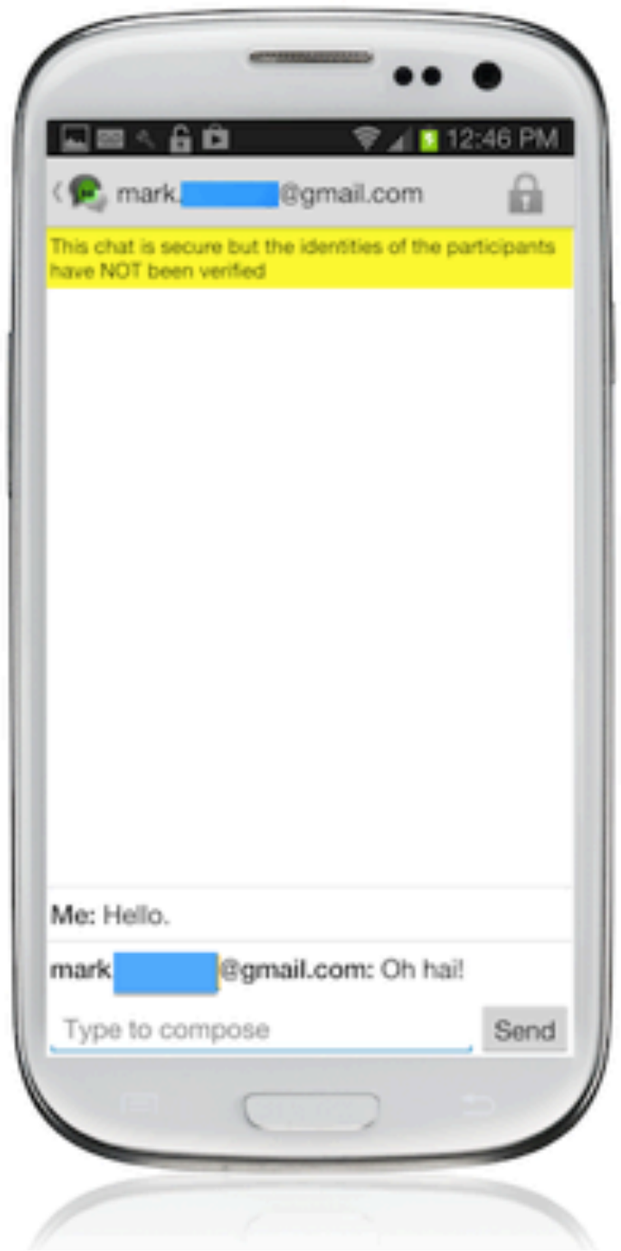
So you want to chat securely on Android?

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!"

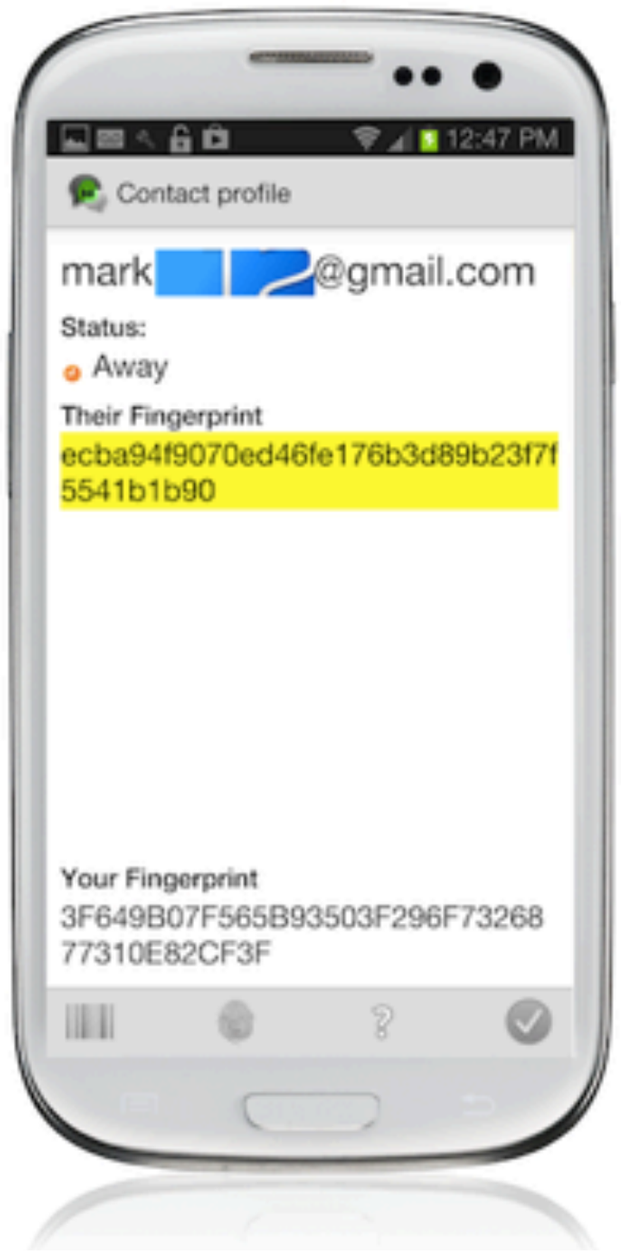


So you want to chat securely on Android?

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

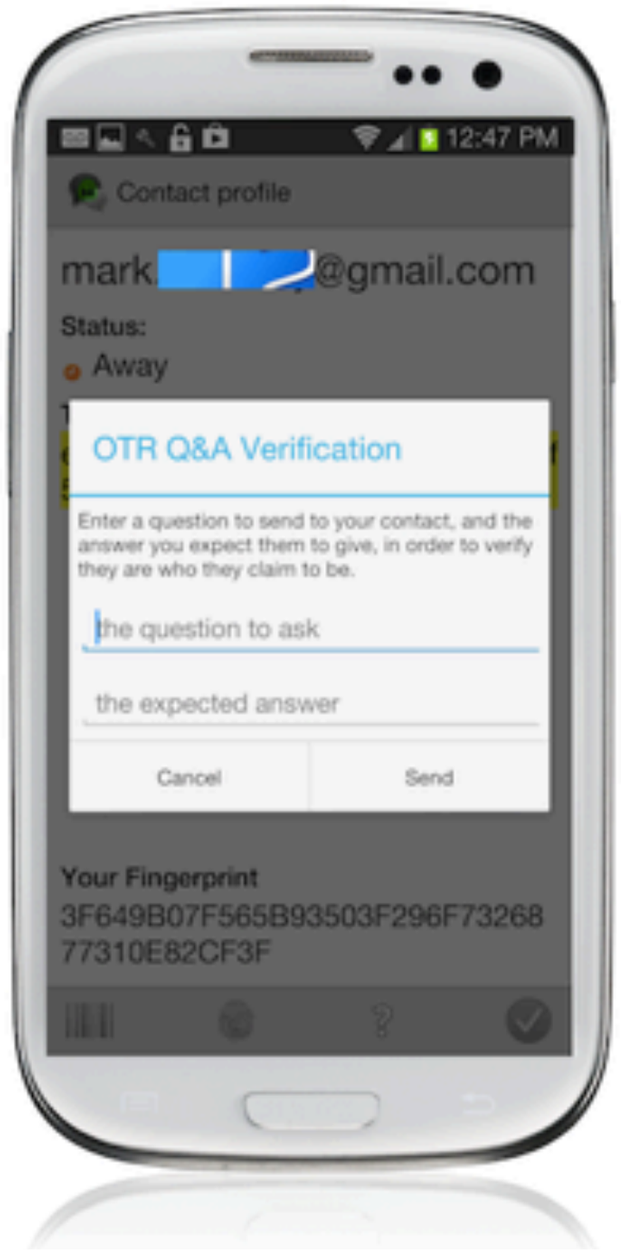
So you want to chat securely on Android?

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



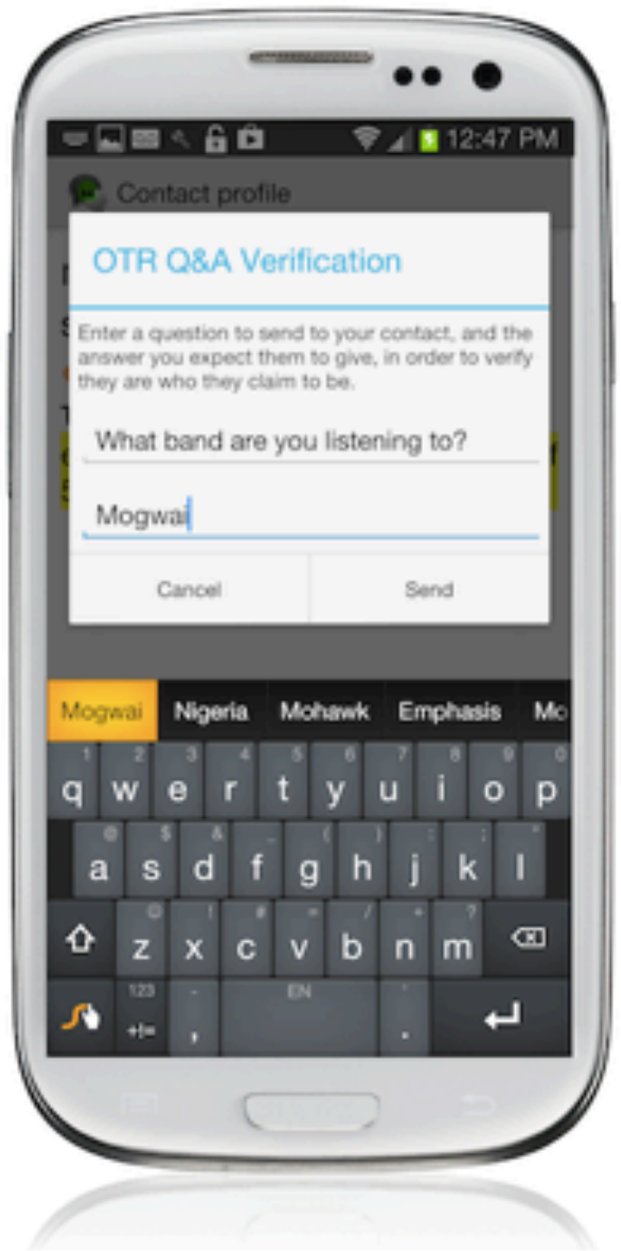
So you want to chat securely on Android?

I'm thinking of a question...



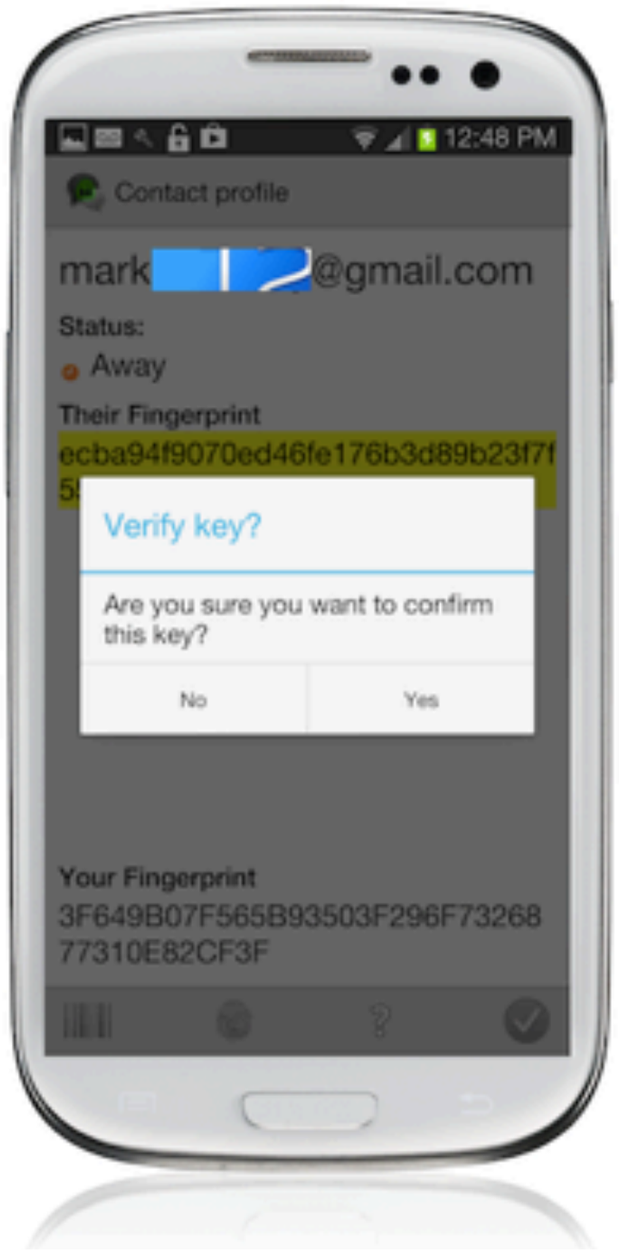
So you want to chat securely on Android?

Got it! I checked on a trusted channel: Spotify. Send the secret.



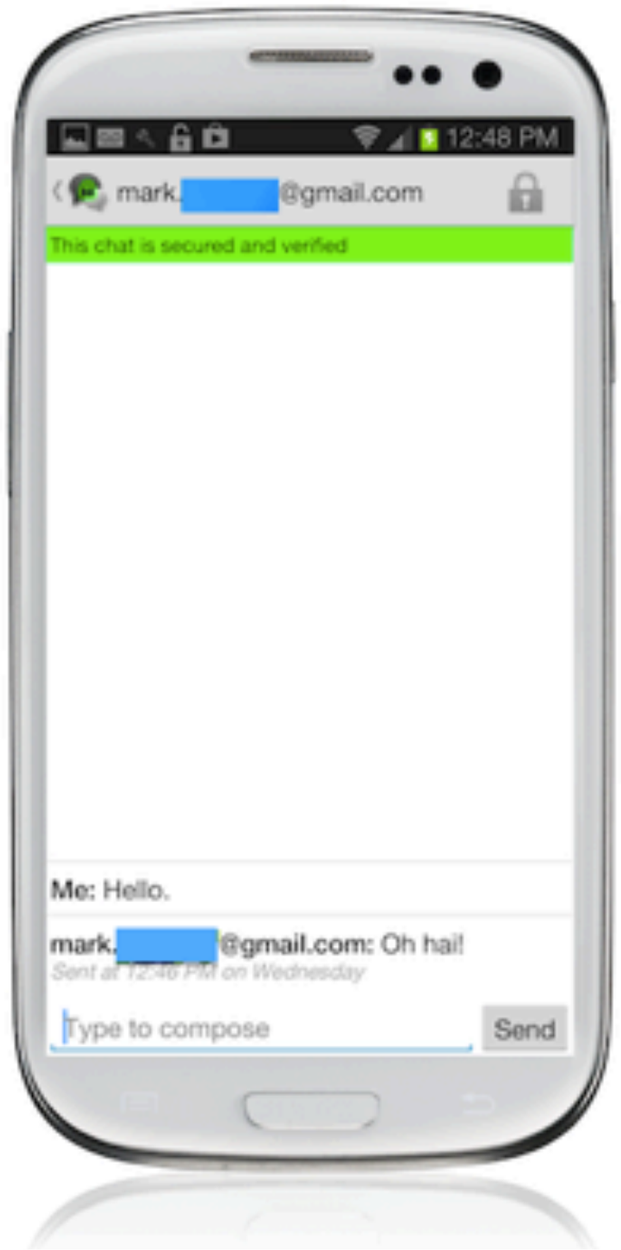
So you want to chat securely on Android?

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



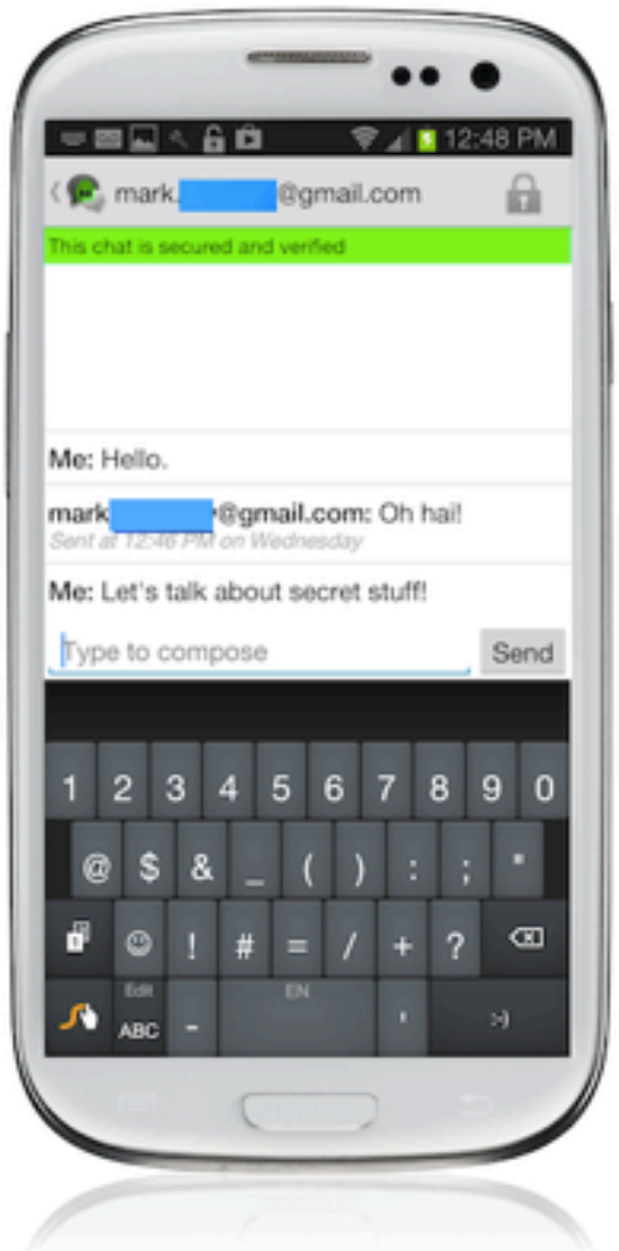
So you want to chat securely on Android?

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?

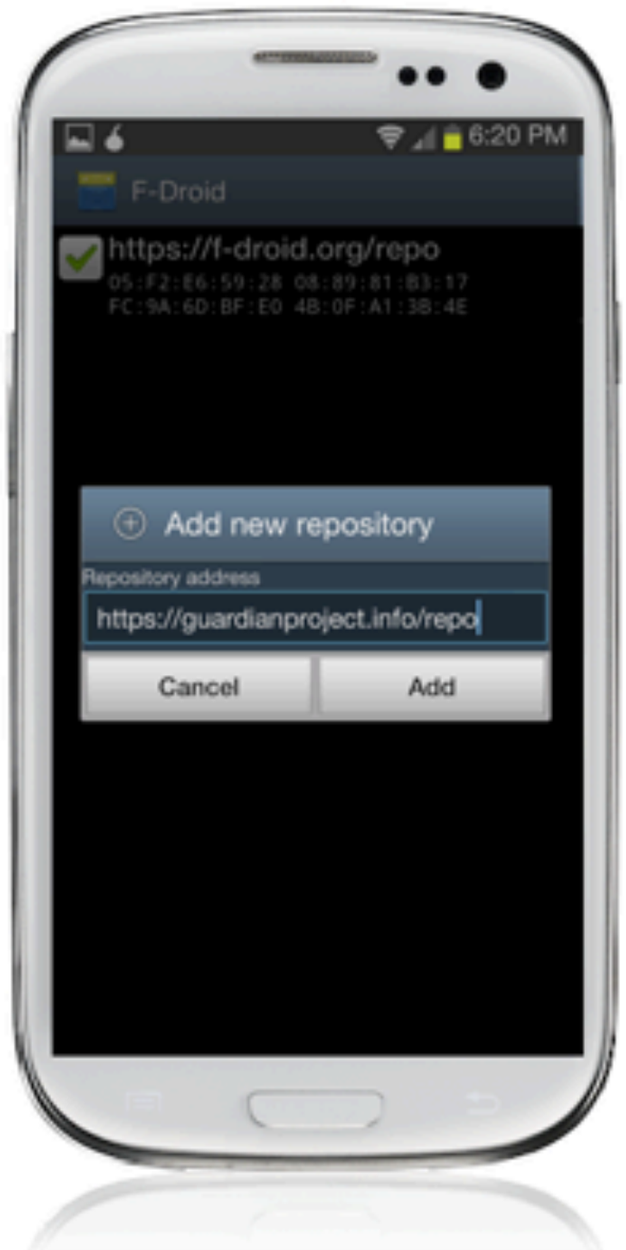
So you want to chat securely on Android?

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.

CHATSECURE

An iOS encrypted messaging application that uses Cypherpunks' Off-the-Record protocol to secure a communication channel over XMPP (Google Talk, Jabber, etc) or Oscar (AIM).

- A partnership with Chris Ballinger & team
- 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

GRYPHN
Secure Mobile Messaging

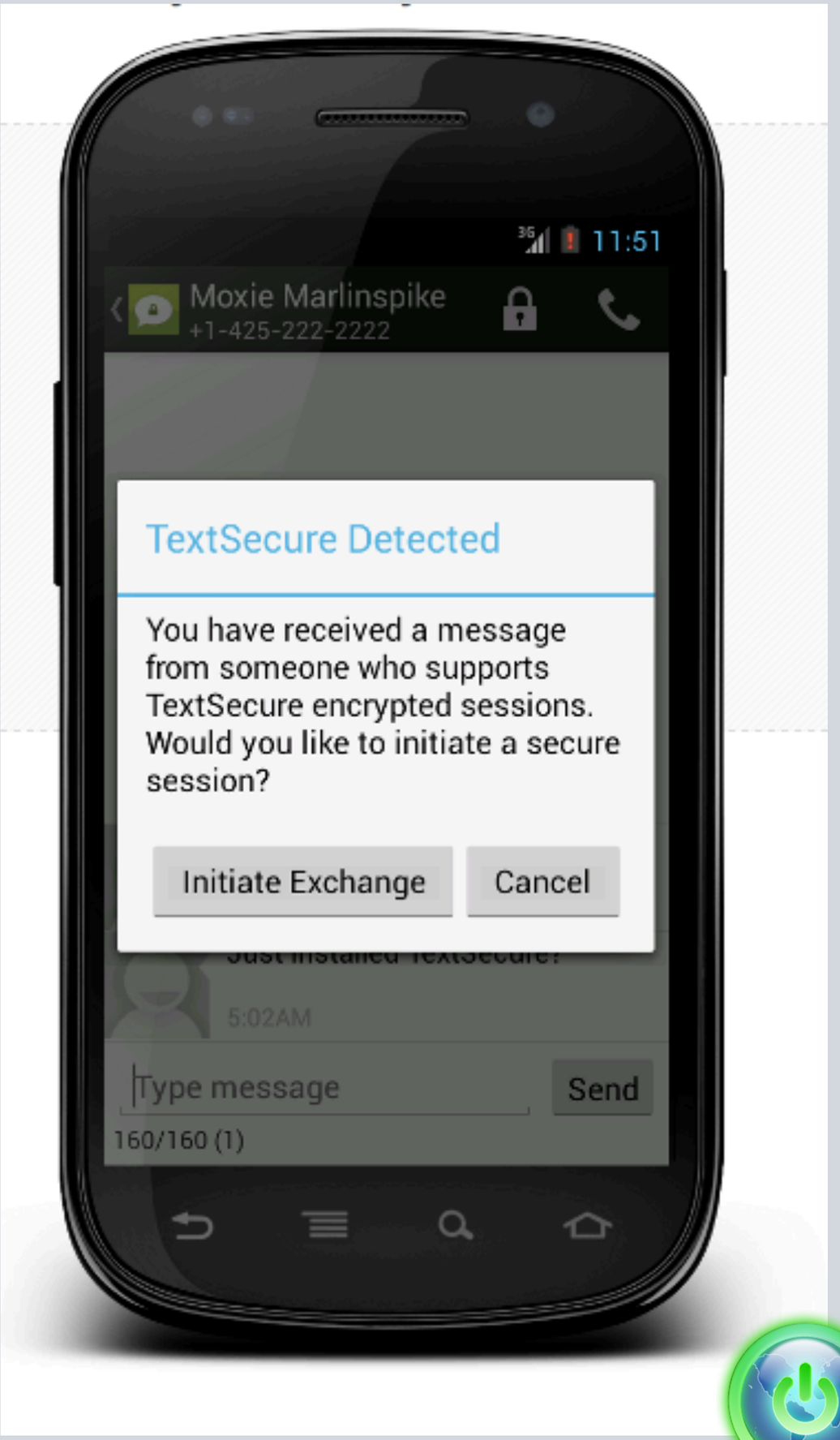
An Android encrypted messaging application that uses encryption to secure a communication channel over SMS & MMS.

- Gryphn Secure Messaging is powered by Guardian Project cipher projects (IOCipher and SQLCipher).
- Secure & Encrypted text messages
- Self-destructing images
- Disabled screenshots
- http://gryphn.co/

TEXTSECURE

An Android encrypted messaging application that uses encryption to secure a communication channel over SMS & MMS.

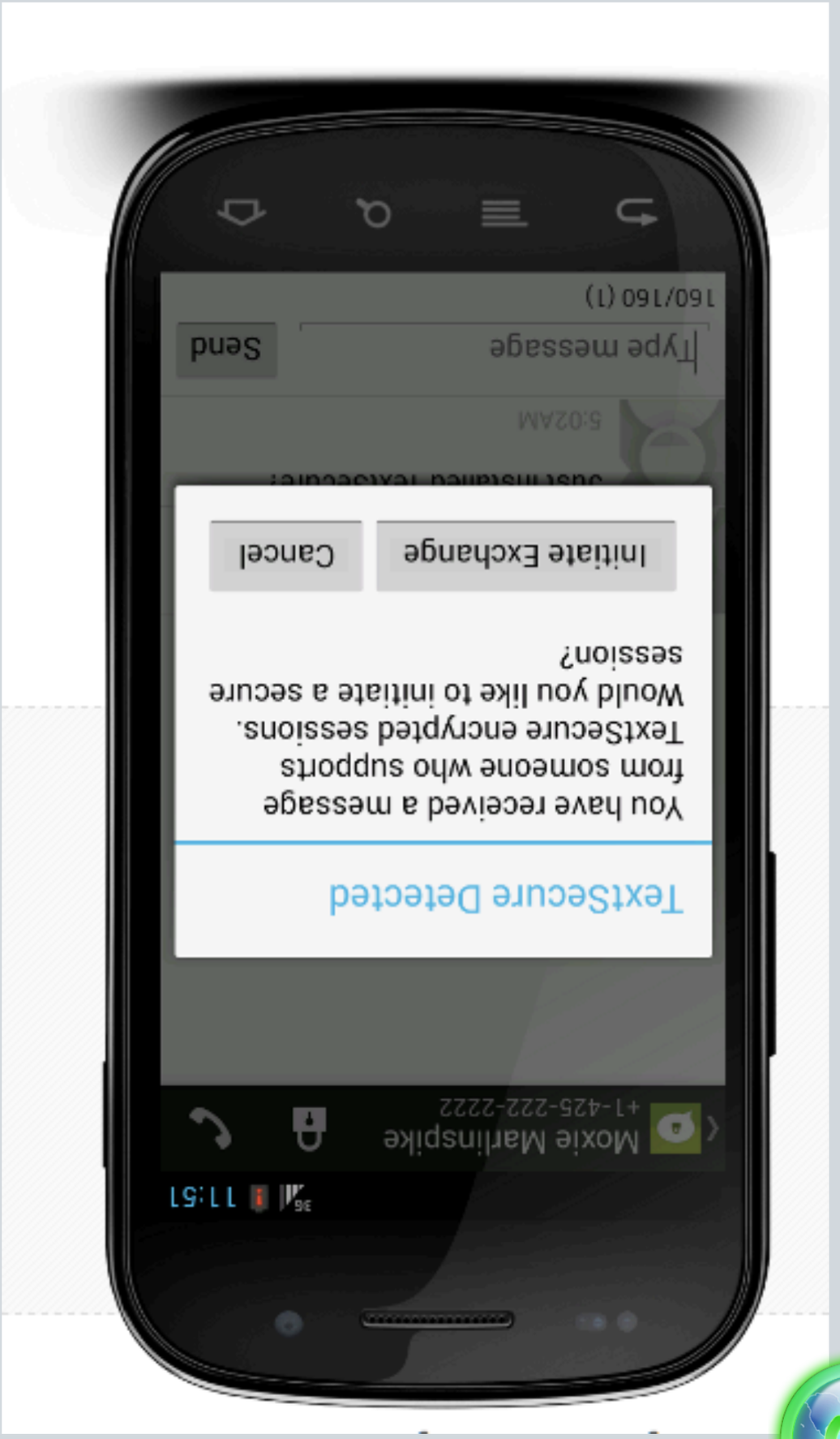
- Secure & Encrypted text messages
- Open Source
- http://www.whispersystems.org



SECRET SMS

There are a lot of security toys.

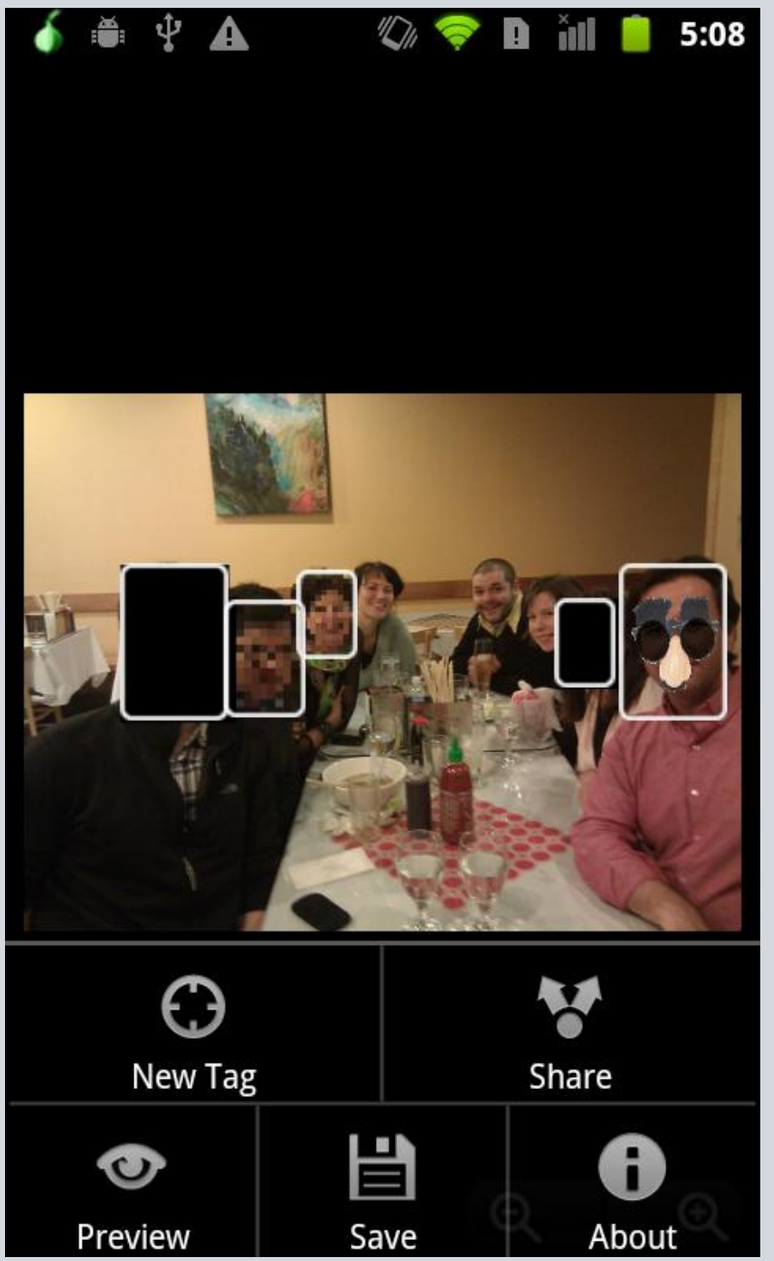
How do we identify a toy?



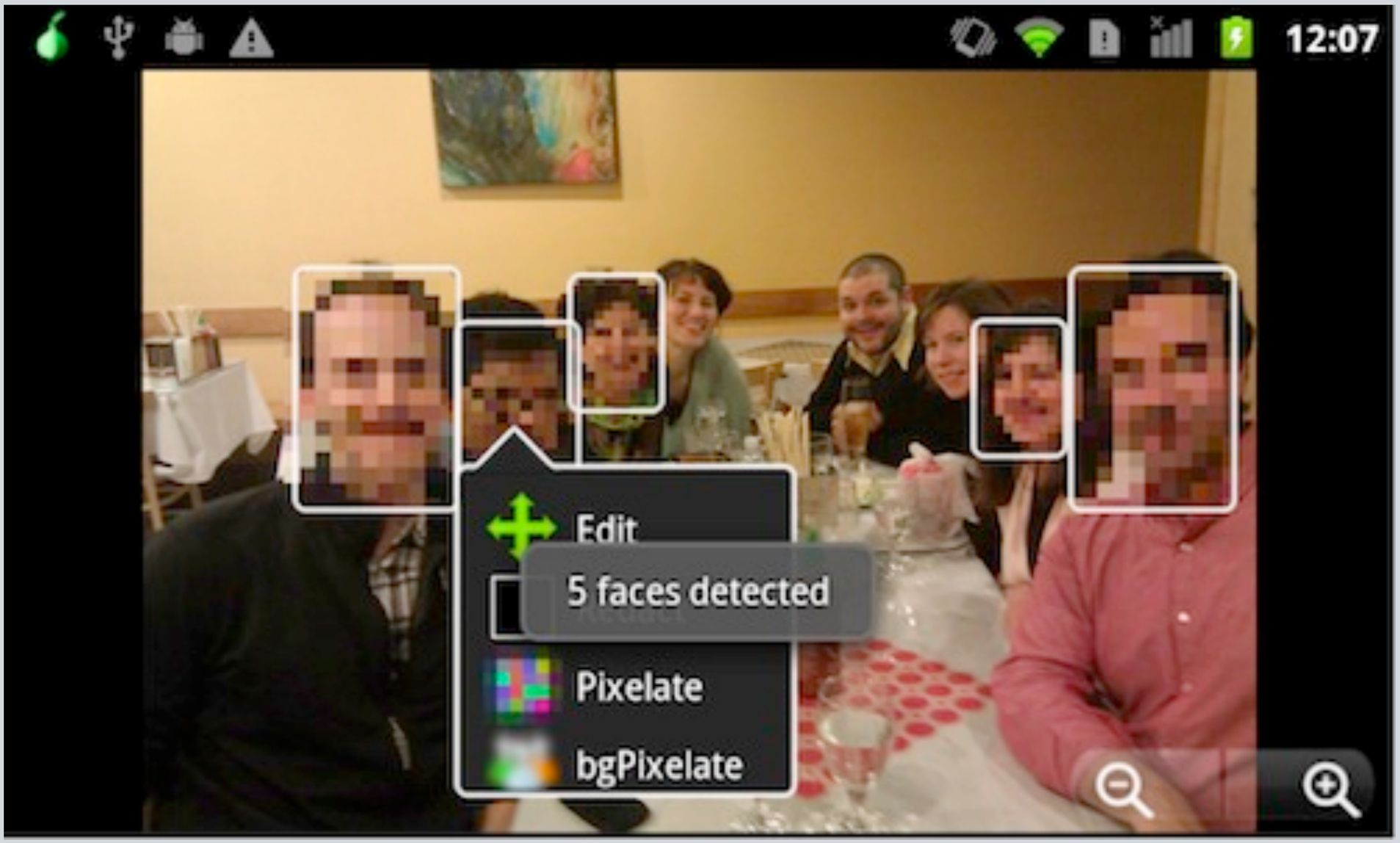
SECURE SMARTCAM

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.

- Obscura & Informa modes
- Advanced meta-data captureEncrypted local storage
- Secure remote sync of media over slow networksFace detection and blurring
- Built-in public key encryption



OBSCURACAM



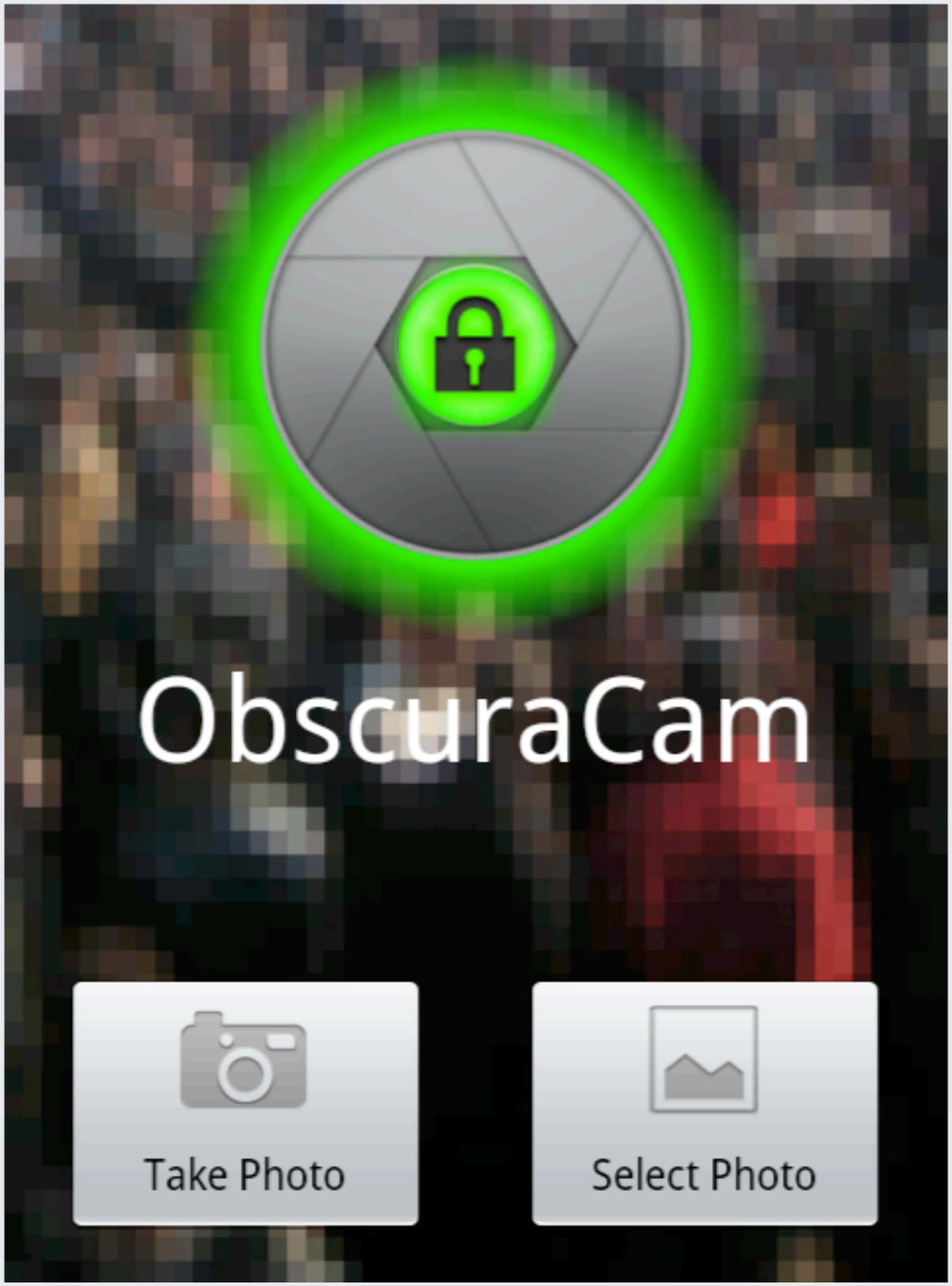
A secure camera application being developed with WITNESS, to help improve visual privacy, secure human rights media content, and innovate in software camera tools for activists.

OBSCURACAM

How-To Guide

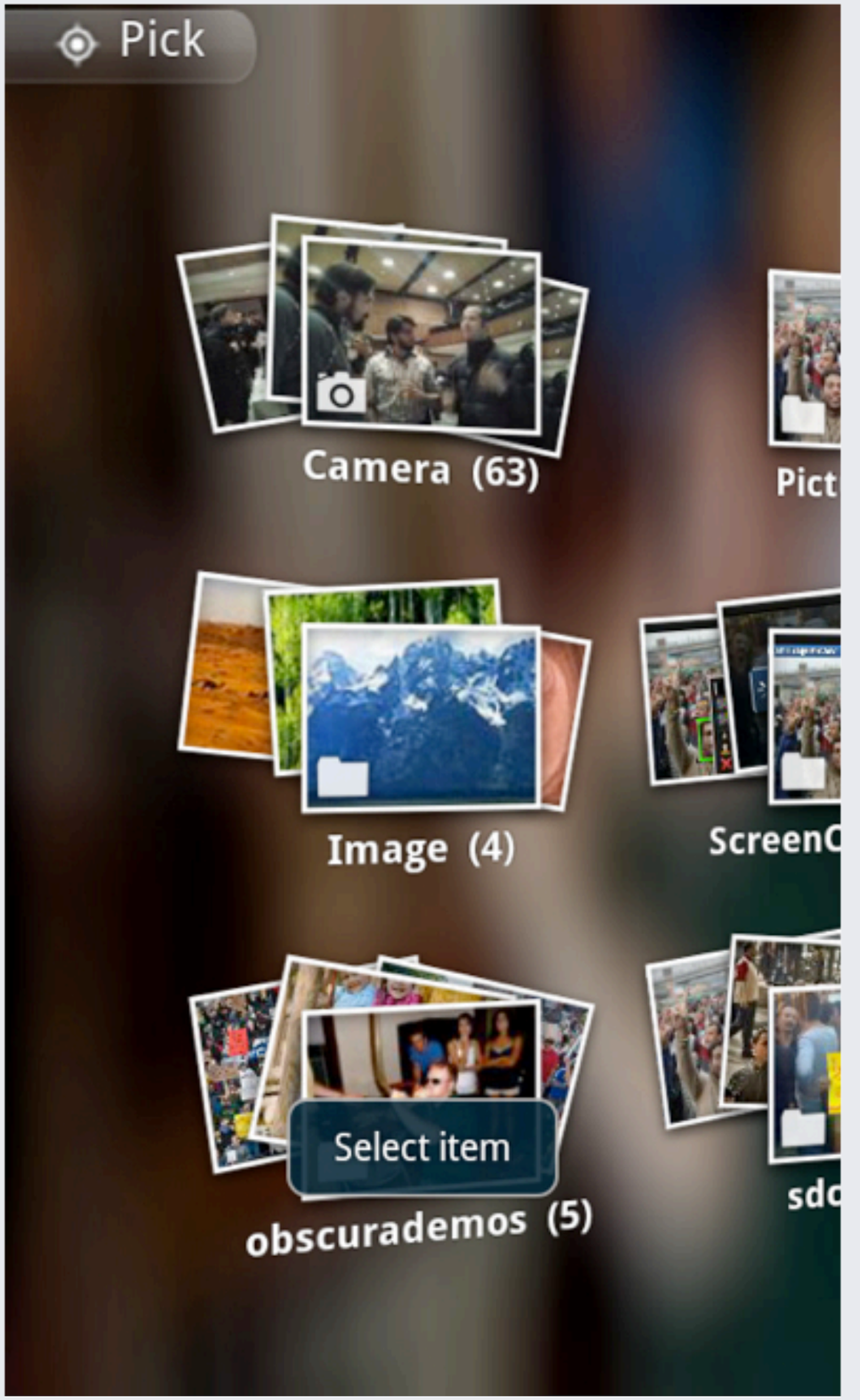
HOME SCREEN

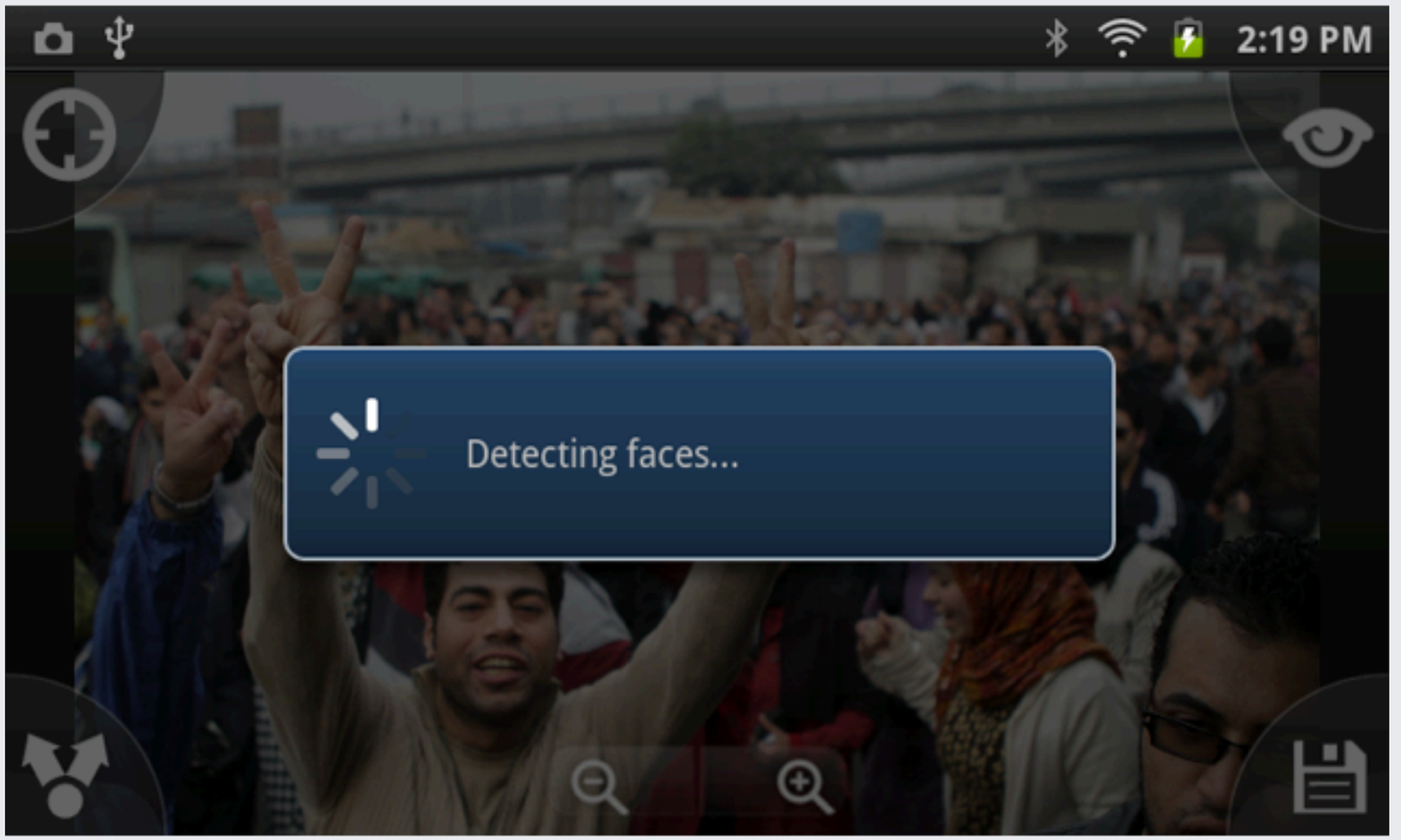
Take a picture or select one from the gallery



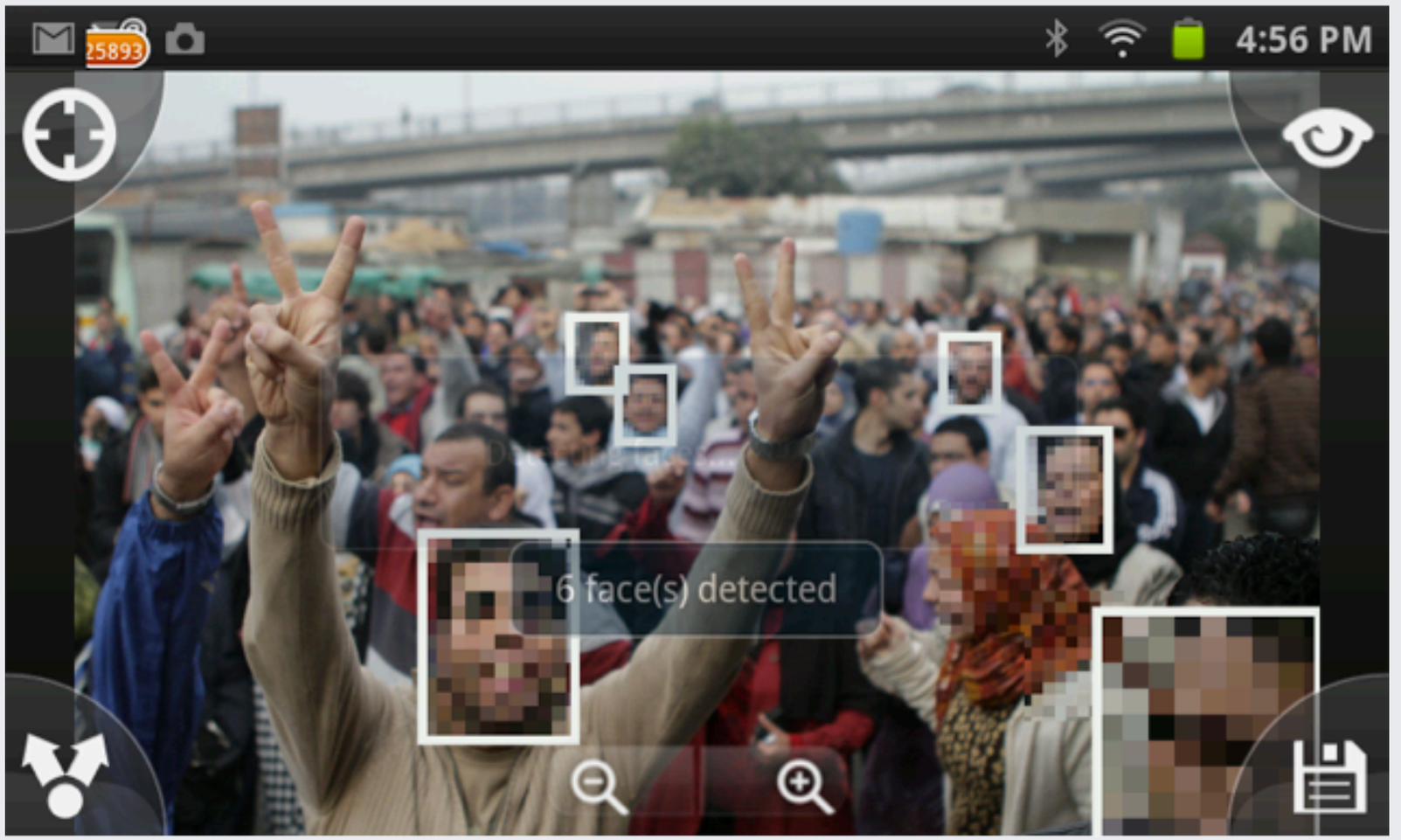
TAKE A PICTURE

you can also select from the gallery

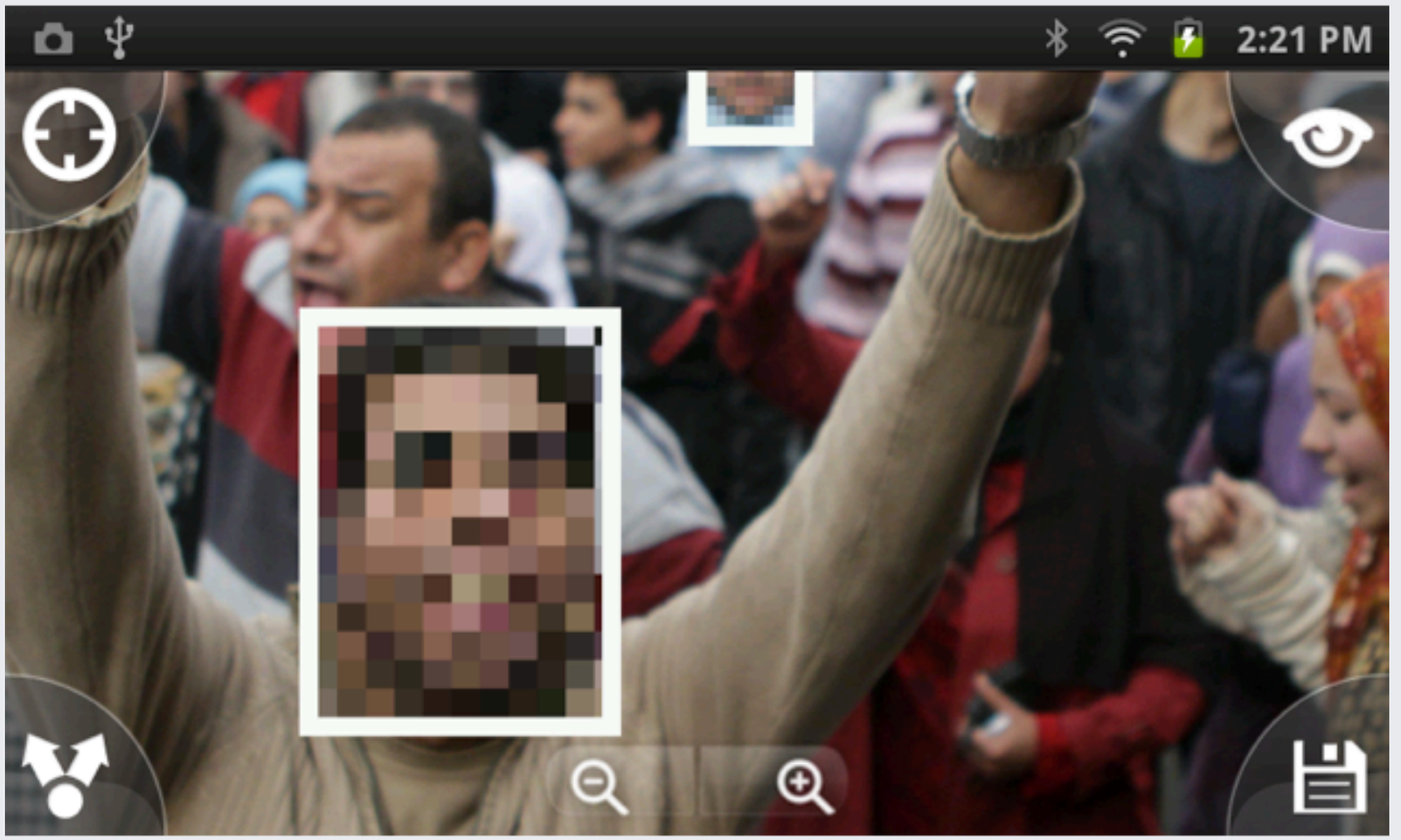




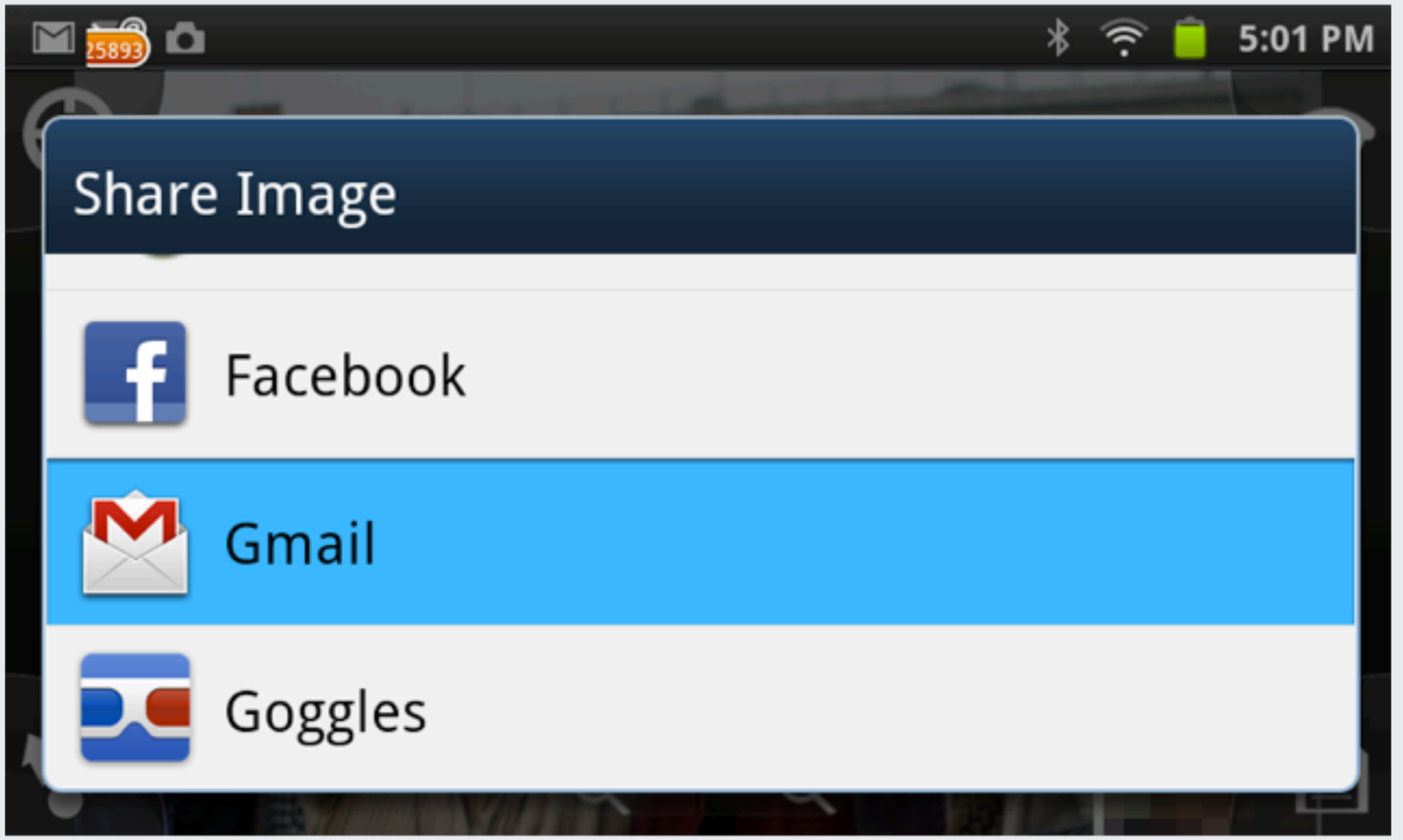
AUTOMATIC FACE DETECTION



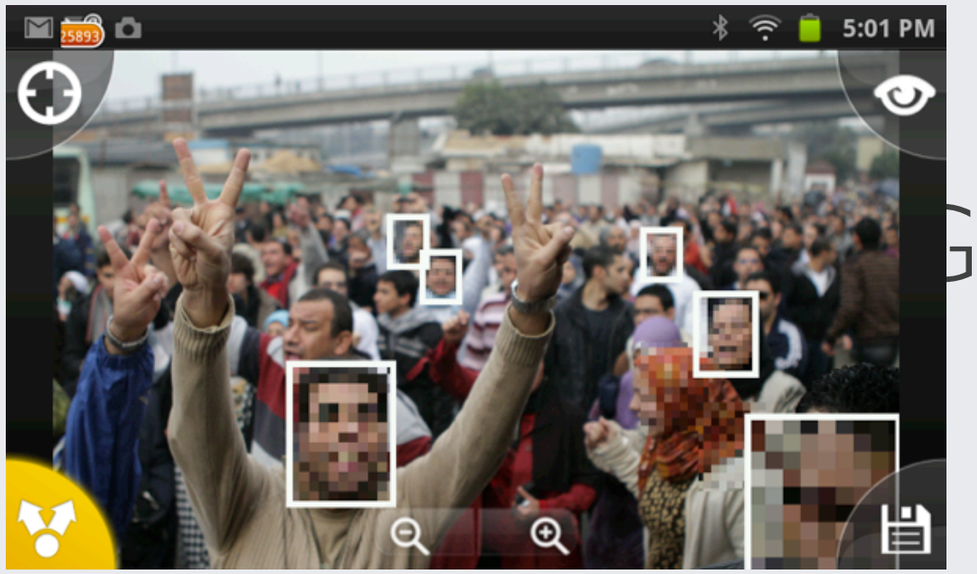
FACES DETECTED

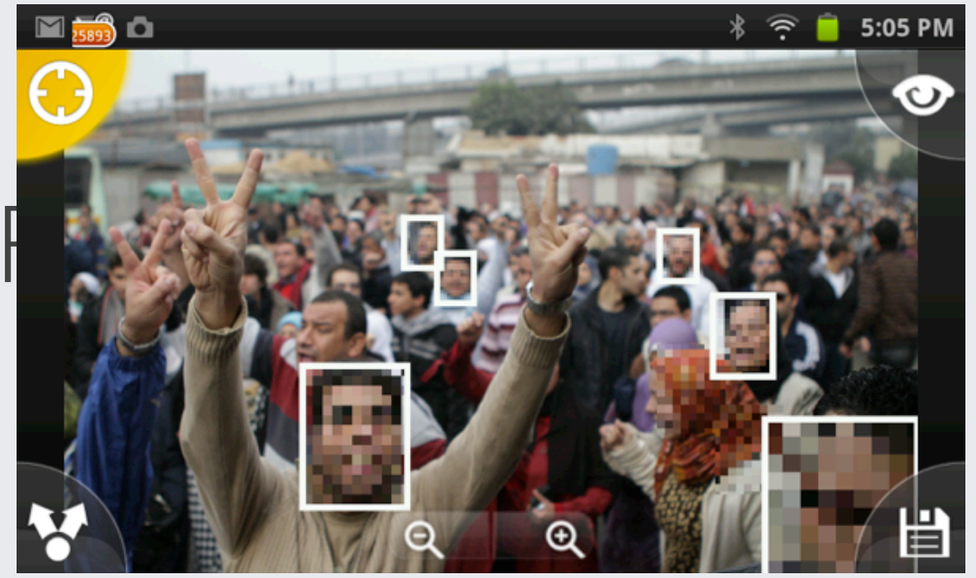


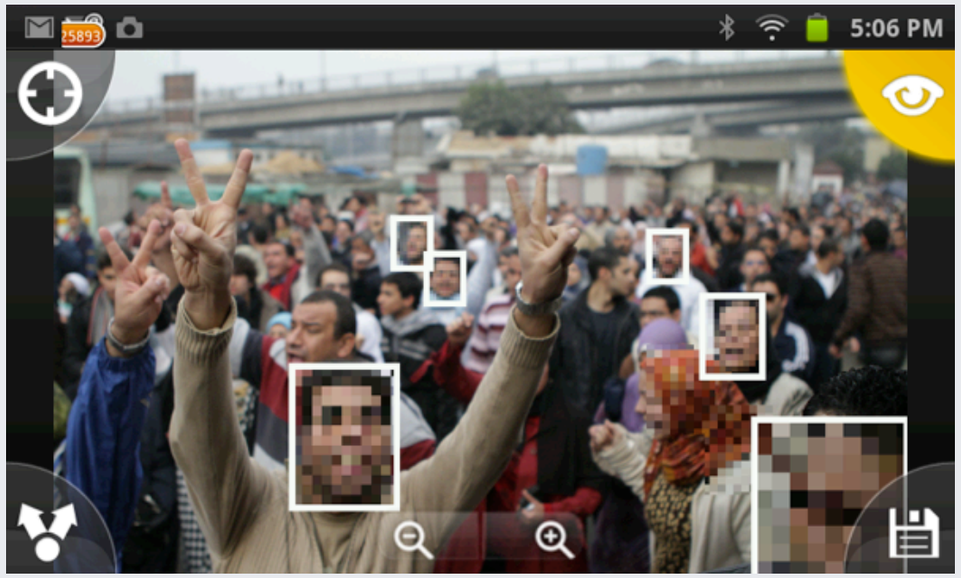
ZOOM IN TO DETAILS

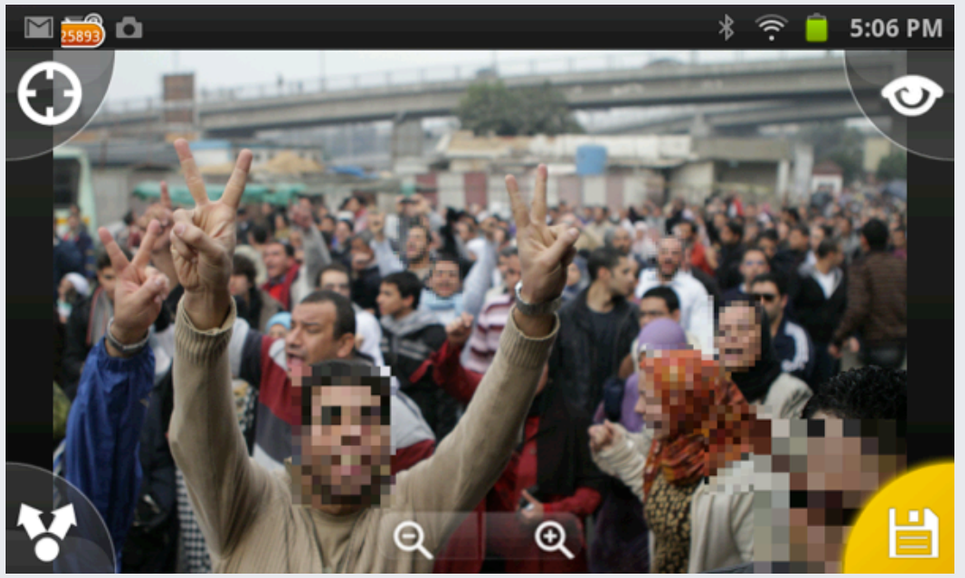


EMAIL OR SHARE









SHARE, TAG, PREVIEW, SAVE

SHARE

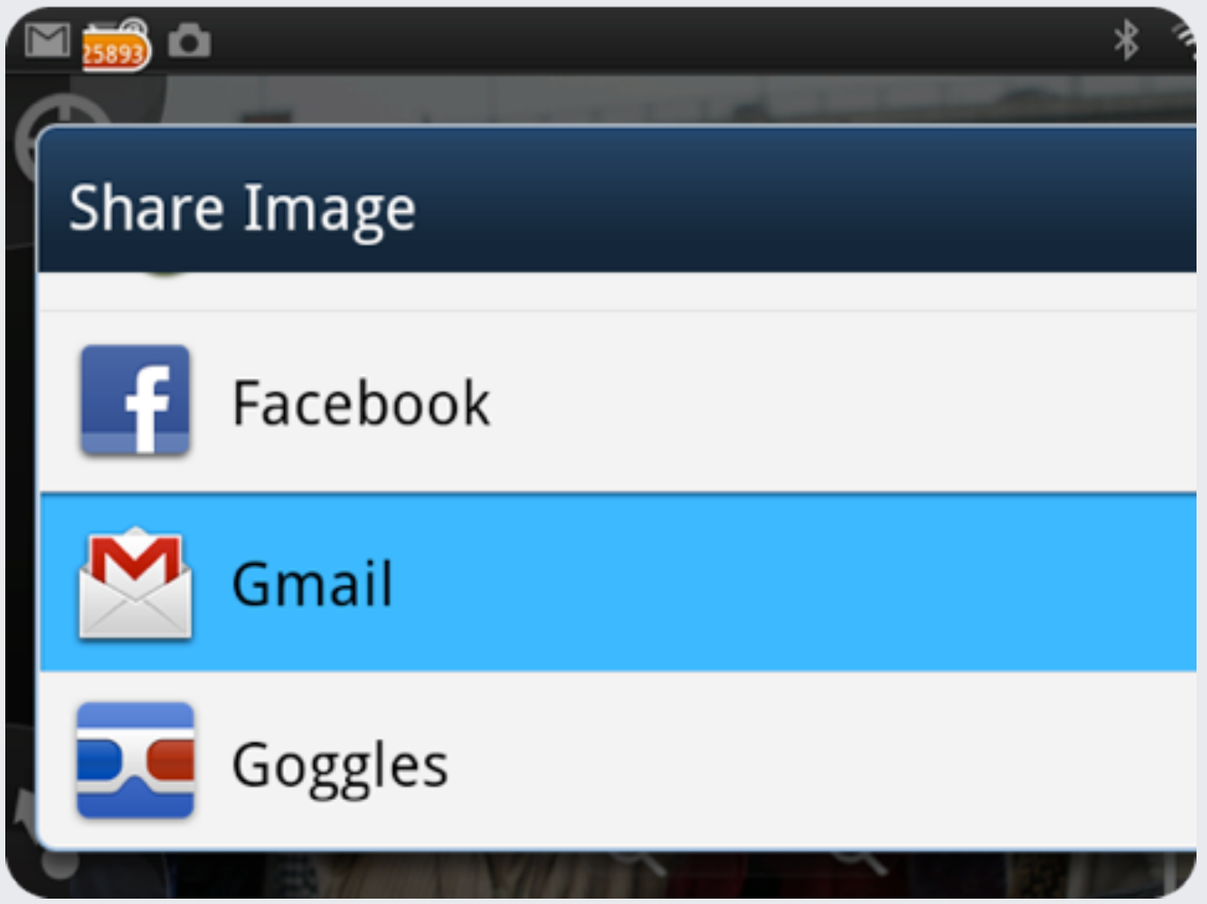
- Tap on the Share icon in the lower left corner

- Select a method for sharing

SHARE

- Select method for sharing

- Most apps that accept images will appear as options



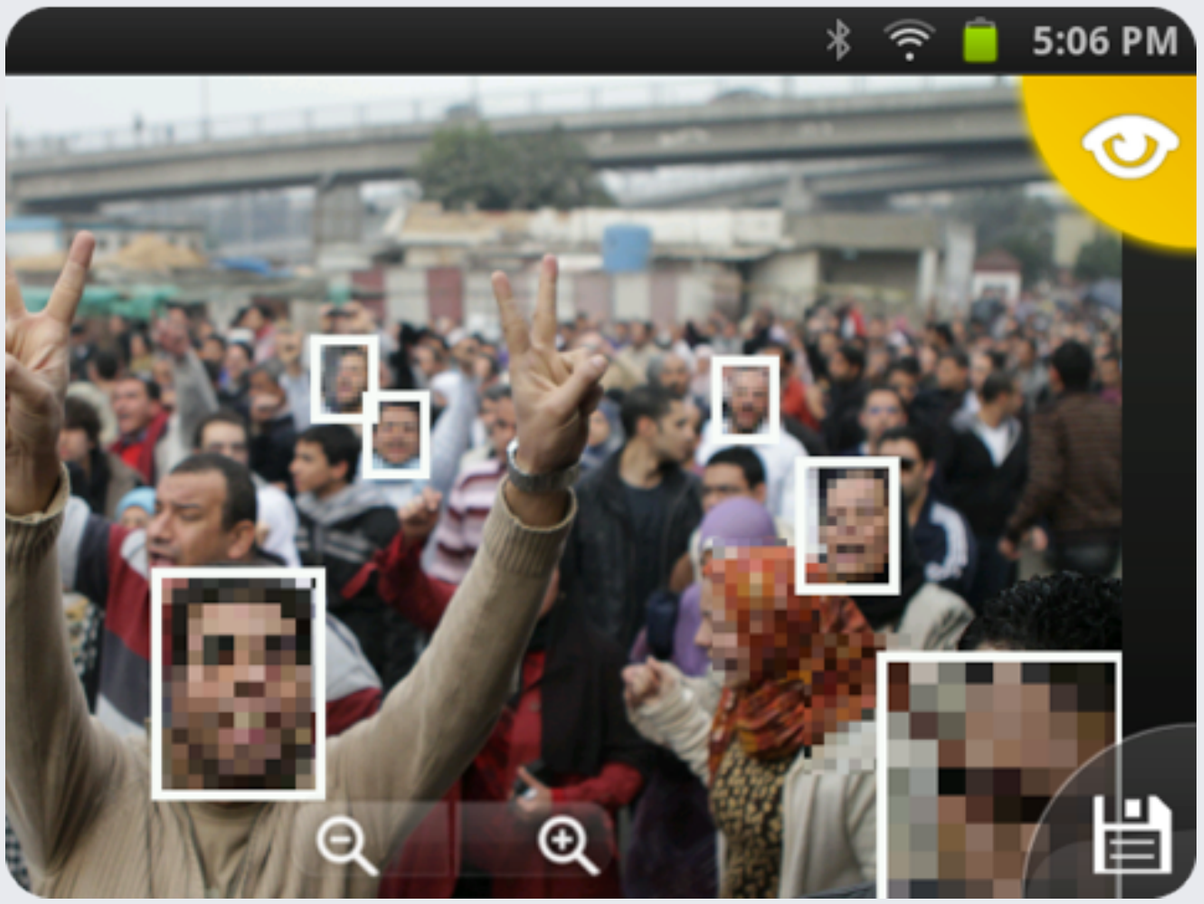
CREATE NEW REGION

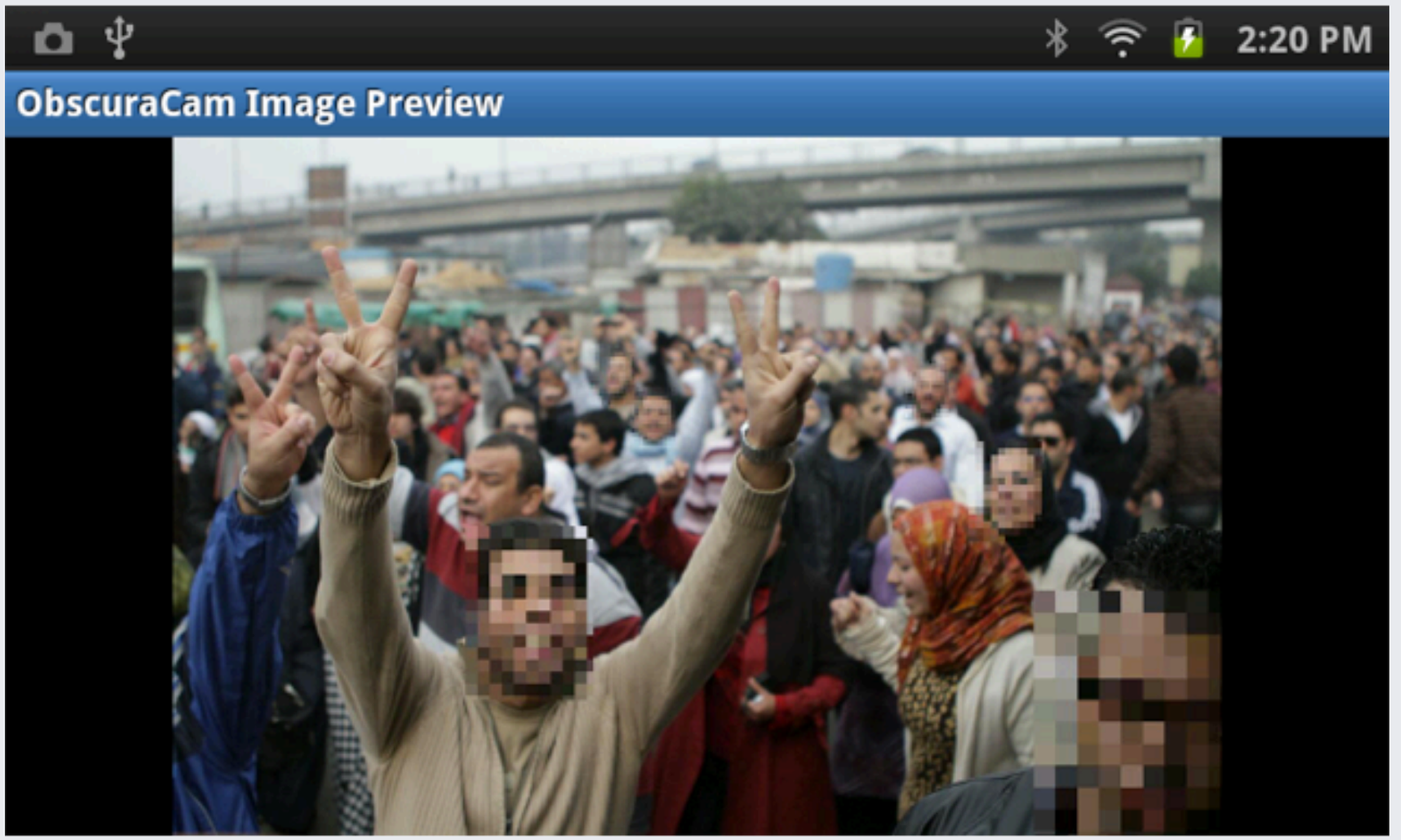
- Tap on the icon in the upper left corner

- Alternately you can tap on the screen to create a new region

PREVIEW

- Tap the icon in the upper right corner

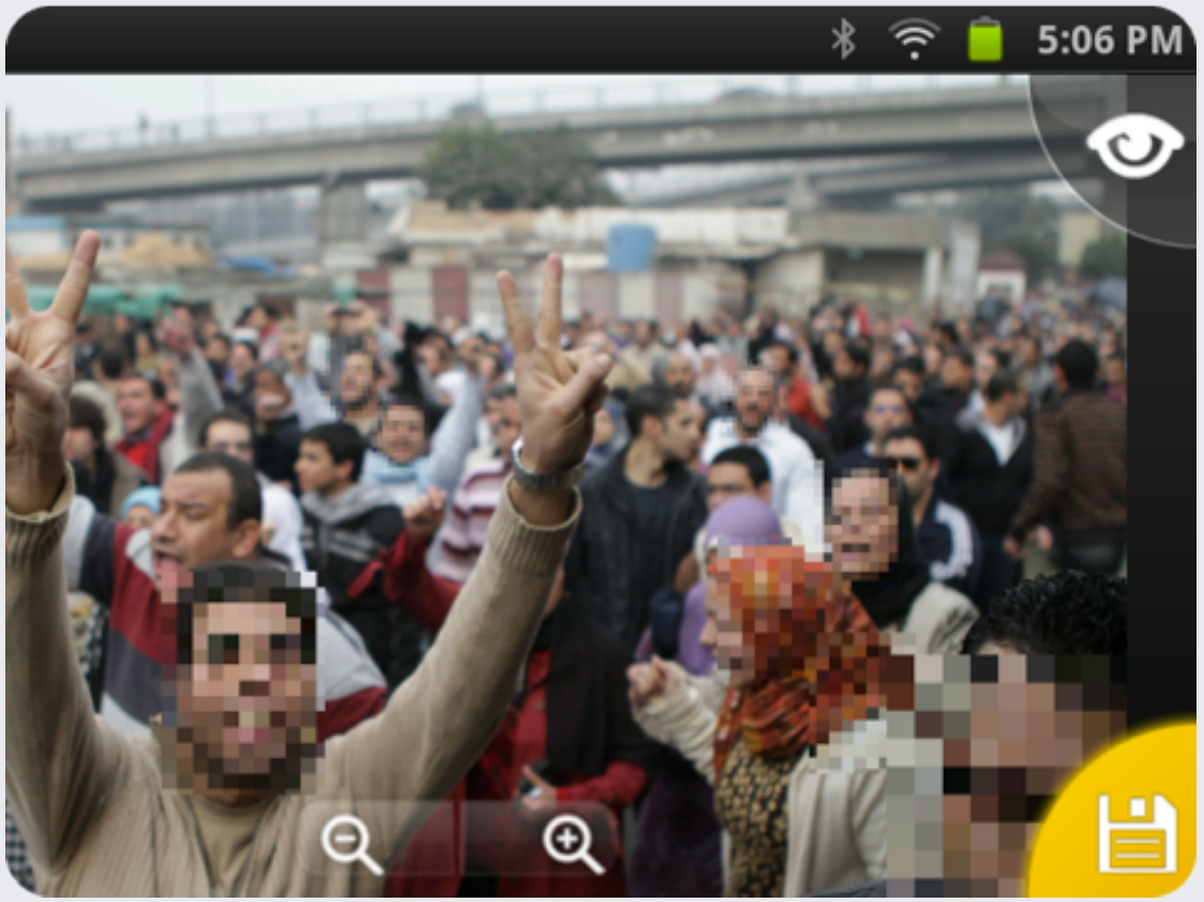




PREVIEW

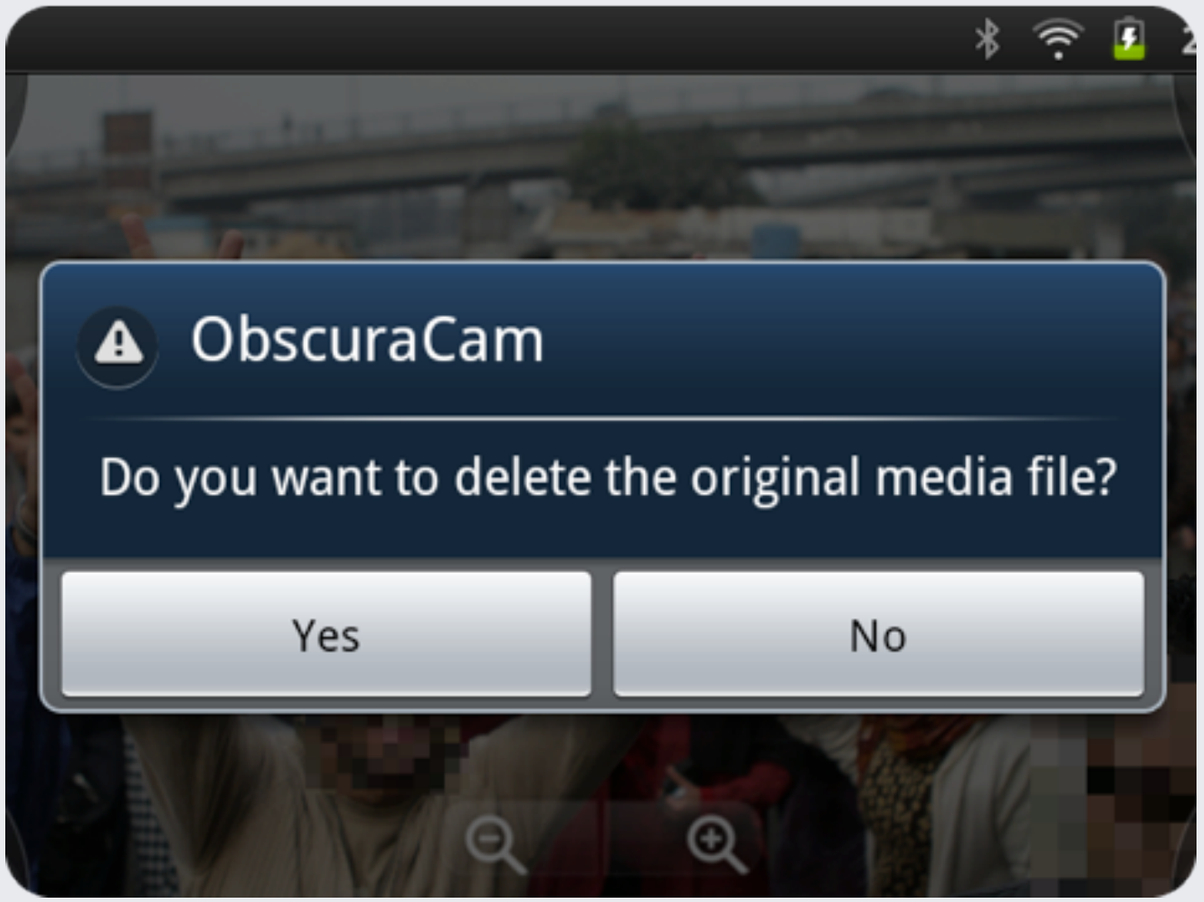
SAVE

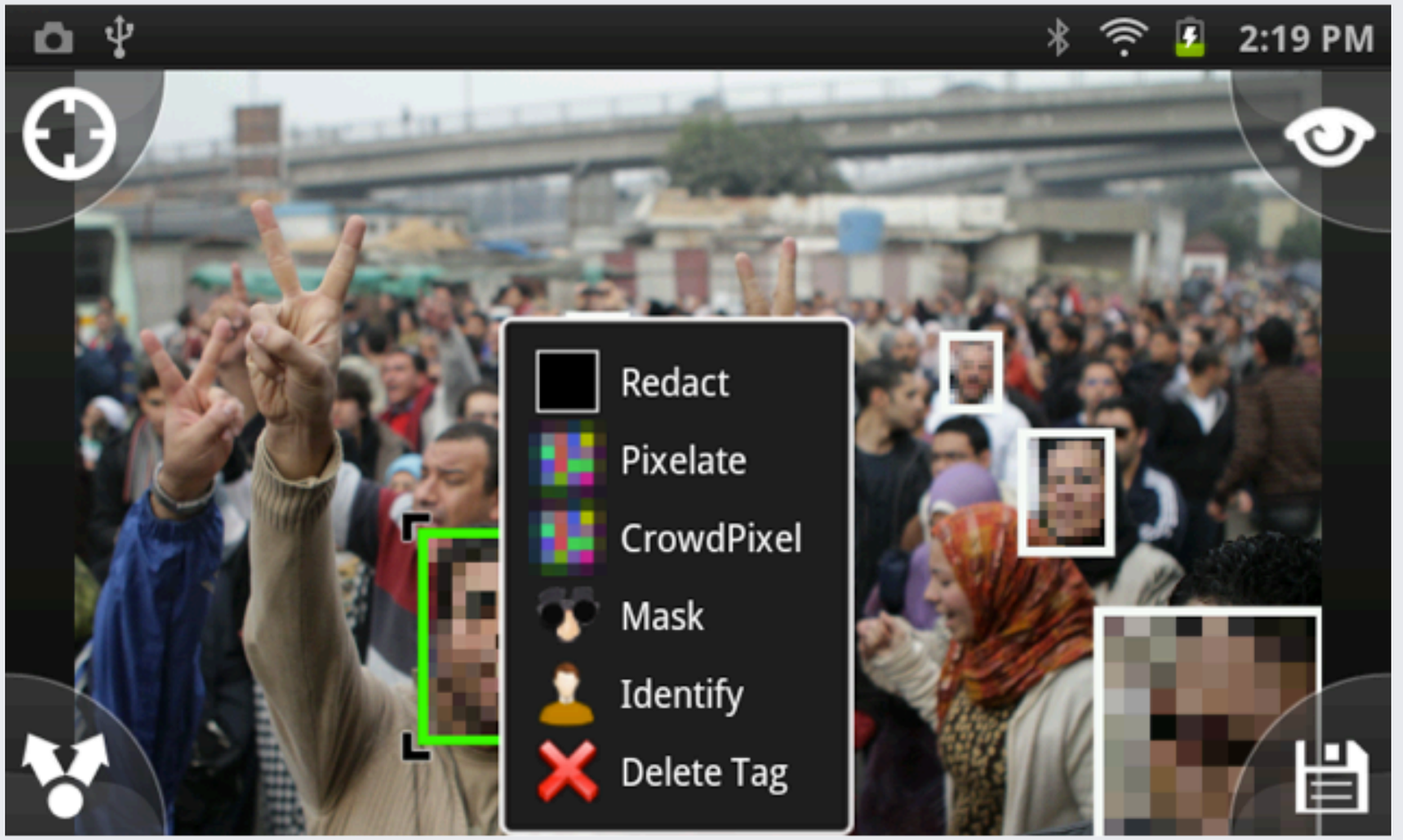
- Tap on the icon in lower right corner



SAVE

- Select option to save or delete original

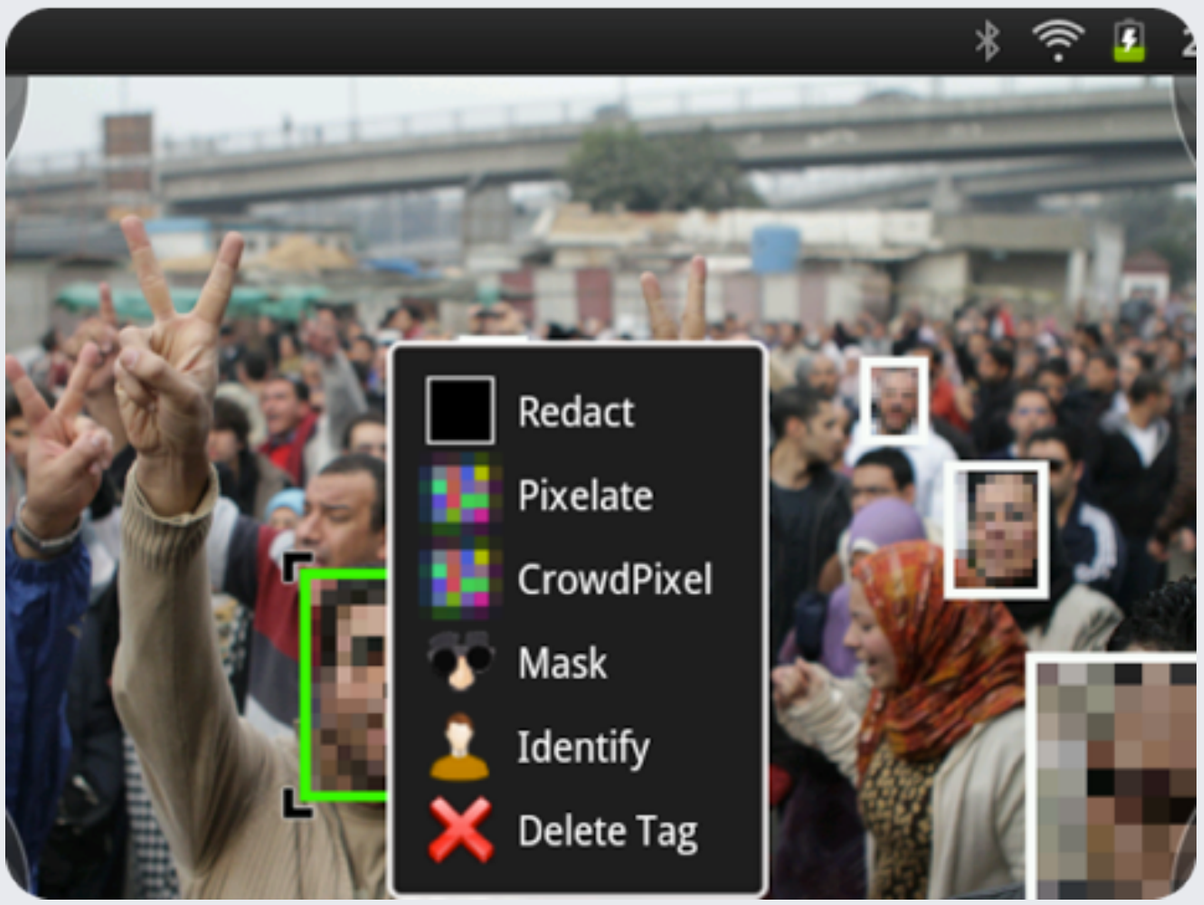



2:19 PM
Redact
Pixelate
CrowdPixel
Mask
Identify
Delete Tag

EDIT MENU

EDIT MENU

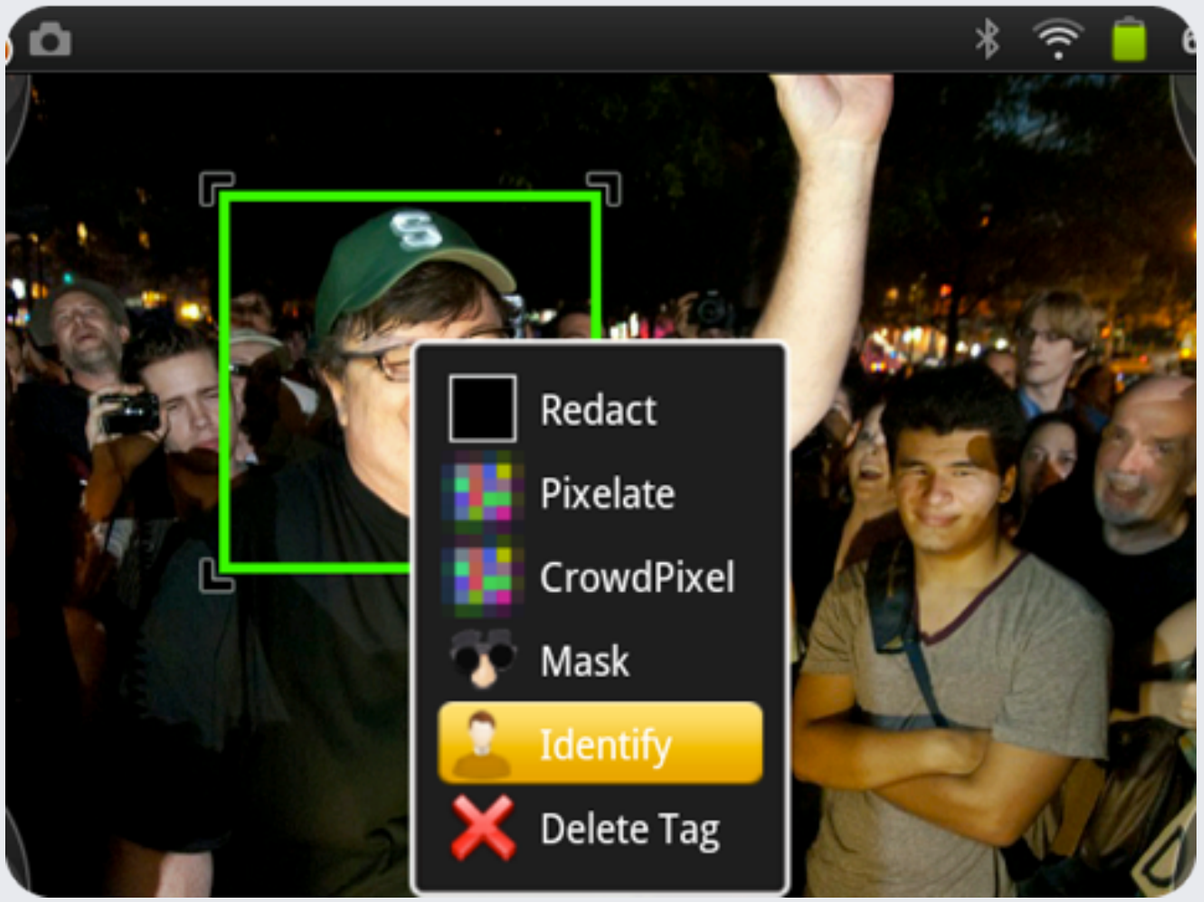
- Redact: Remove completely
- Pixelate: Blur
- CrowdPixel: Blur all but the region
- Identify: Add name and other info
- Delete Tag

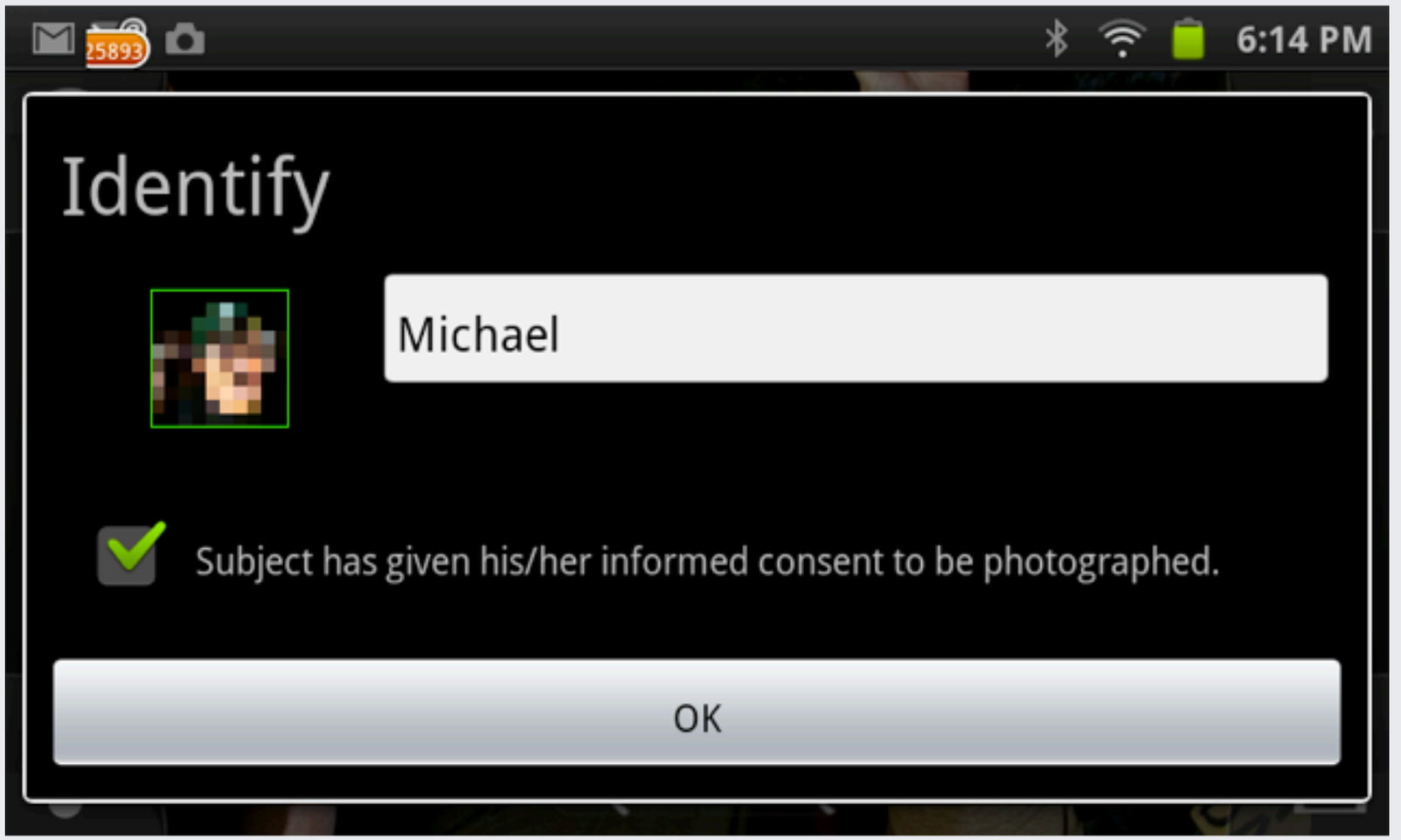


IDENTIFY

- Tap region you wish to identify

- Select the Identify option in the popup menu

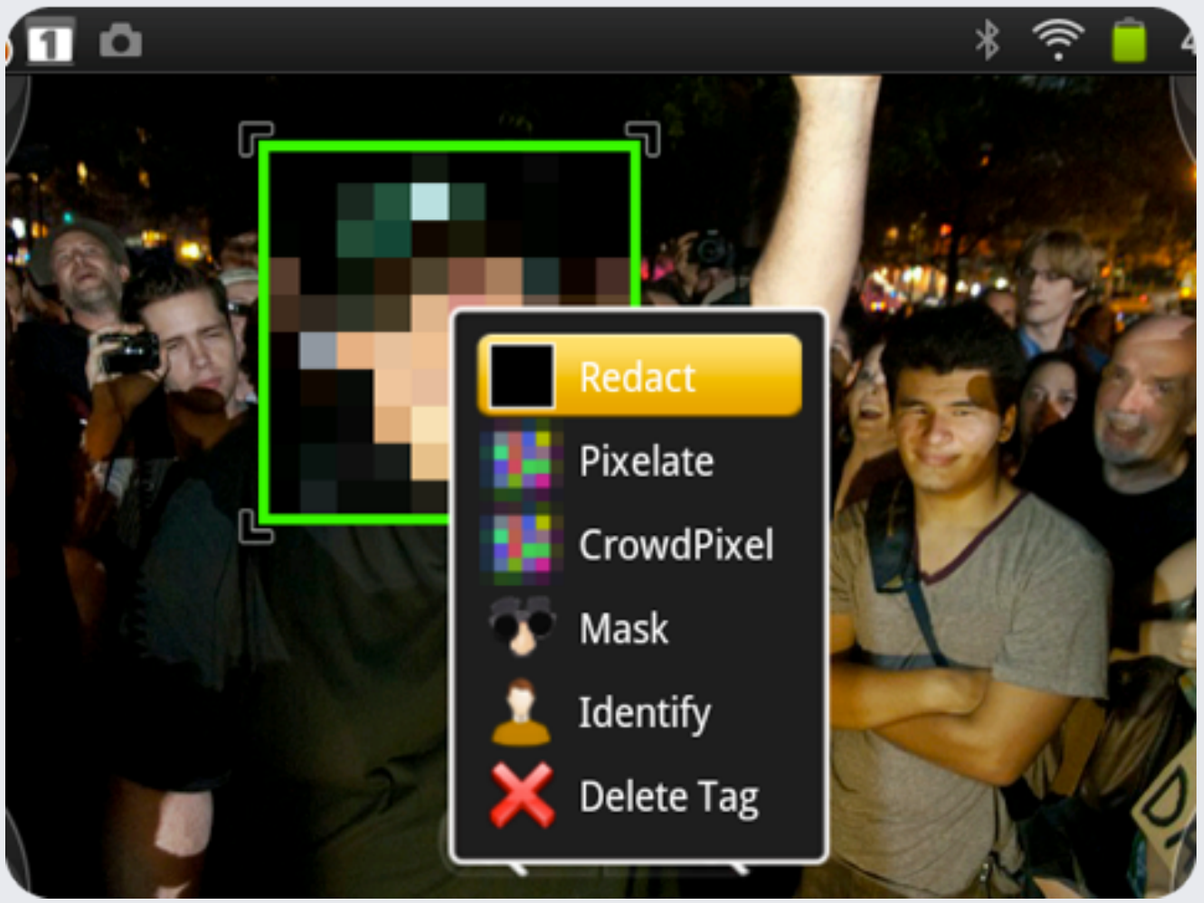



25893
6:14 PM
Identify
Michael
Subject has given his/her informed consent to be photographed.
OK

IDENTIFY

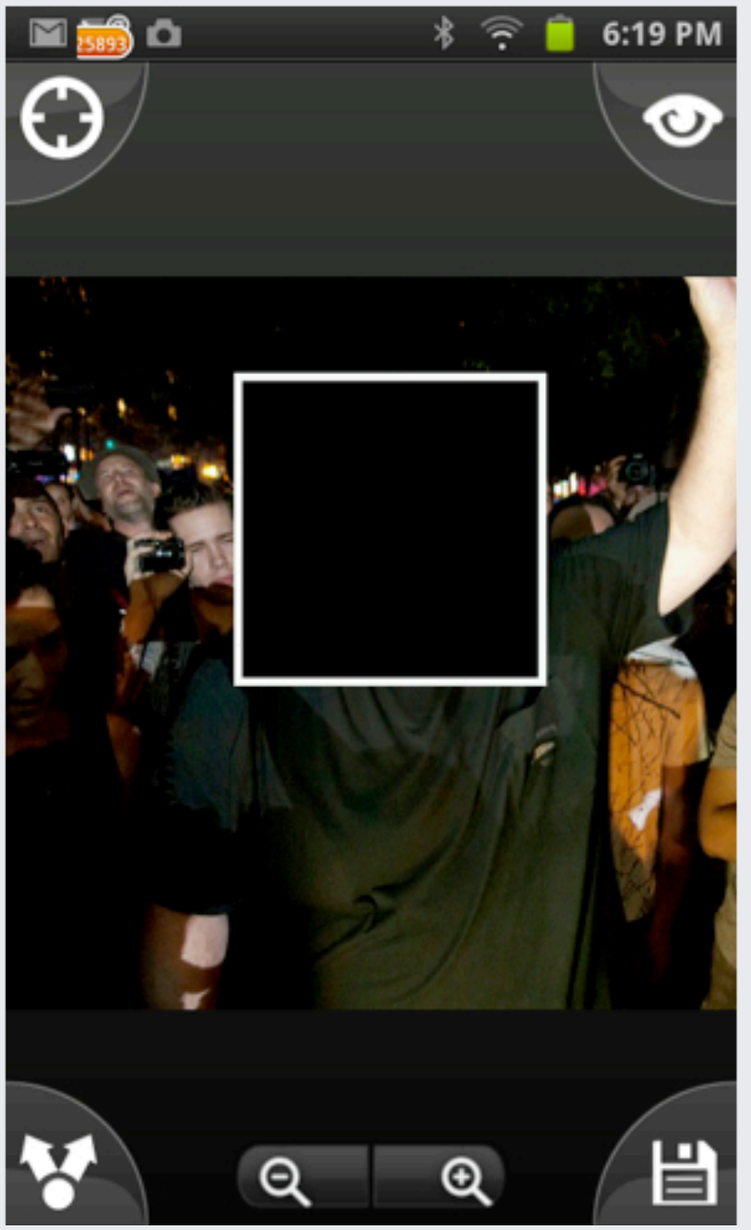
REDACT

- From the edit menu select Redact



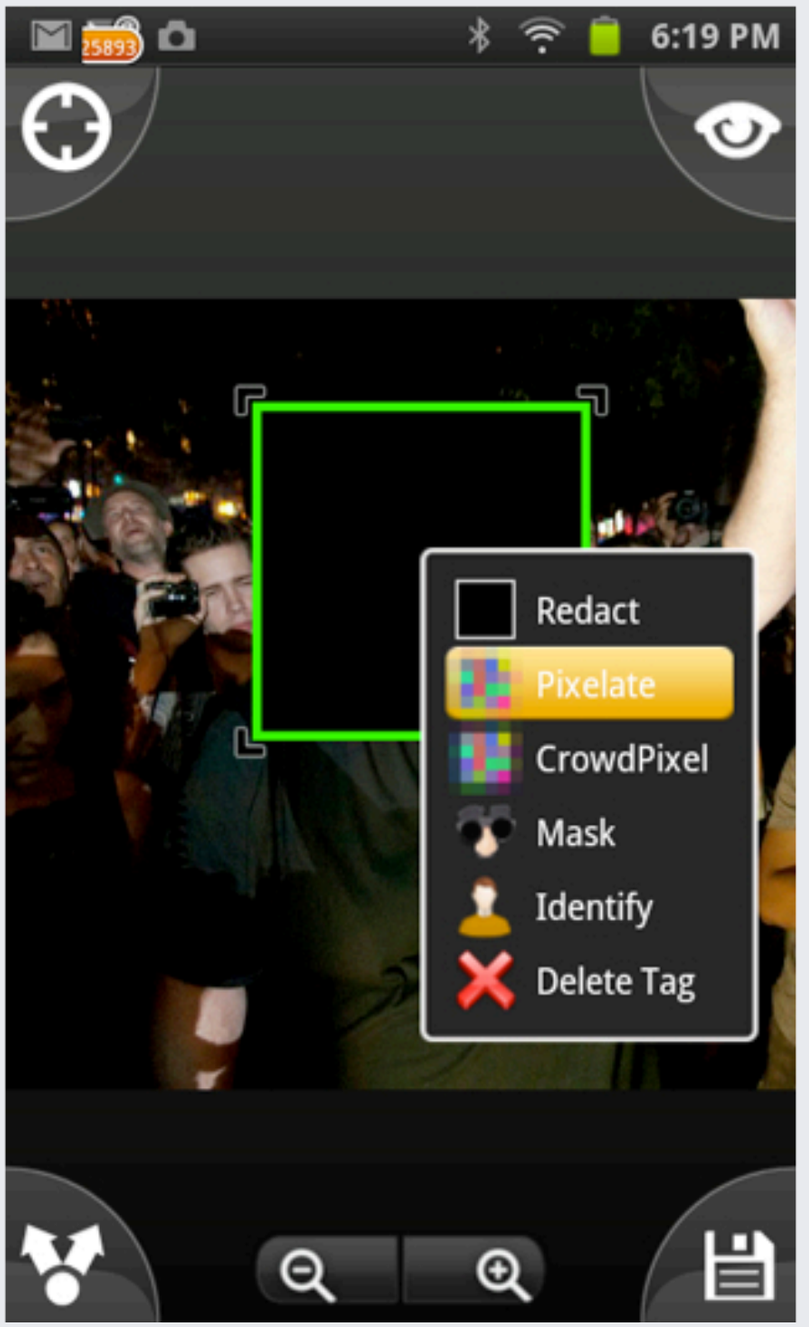
REDACT

- The selected region will be completely removed



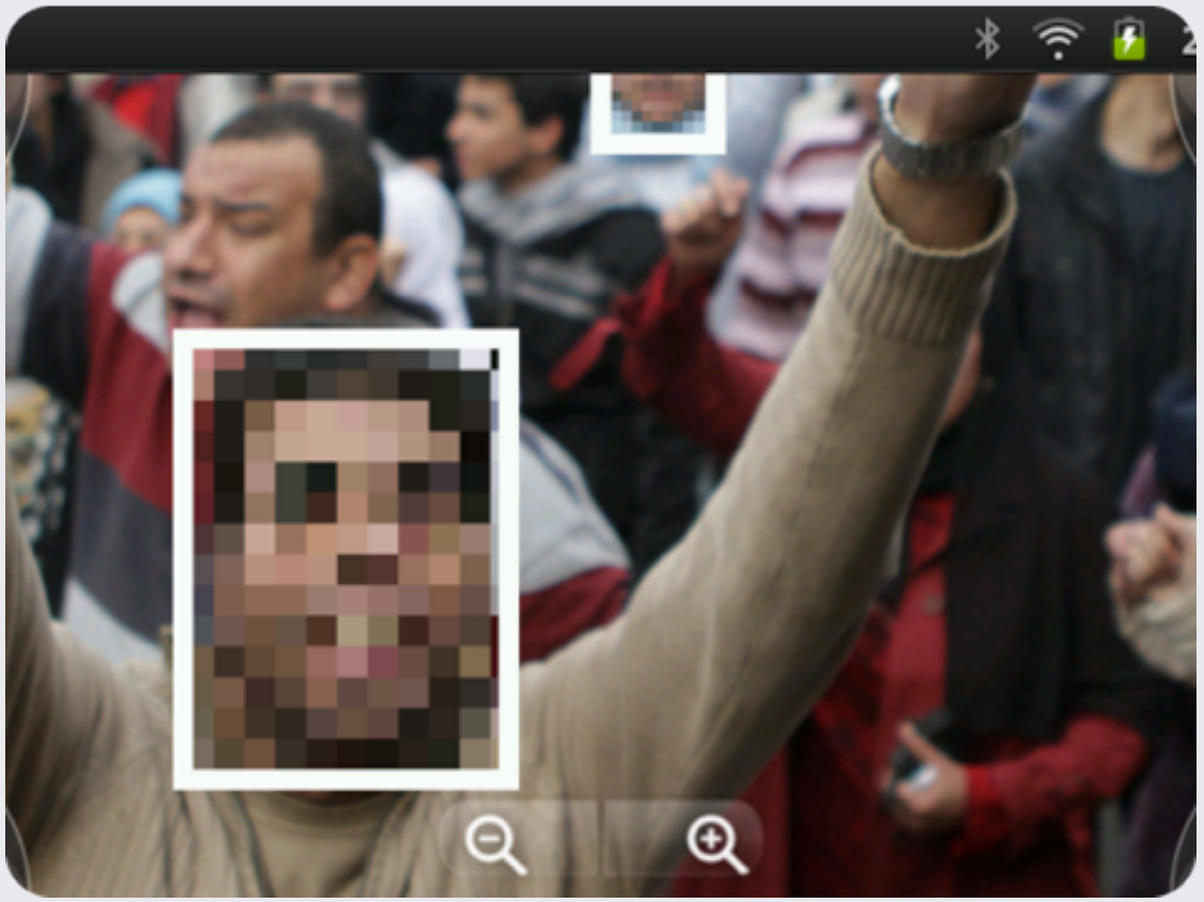
PIXELATE

- From the edit menu select Pixelate



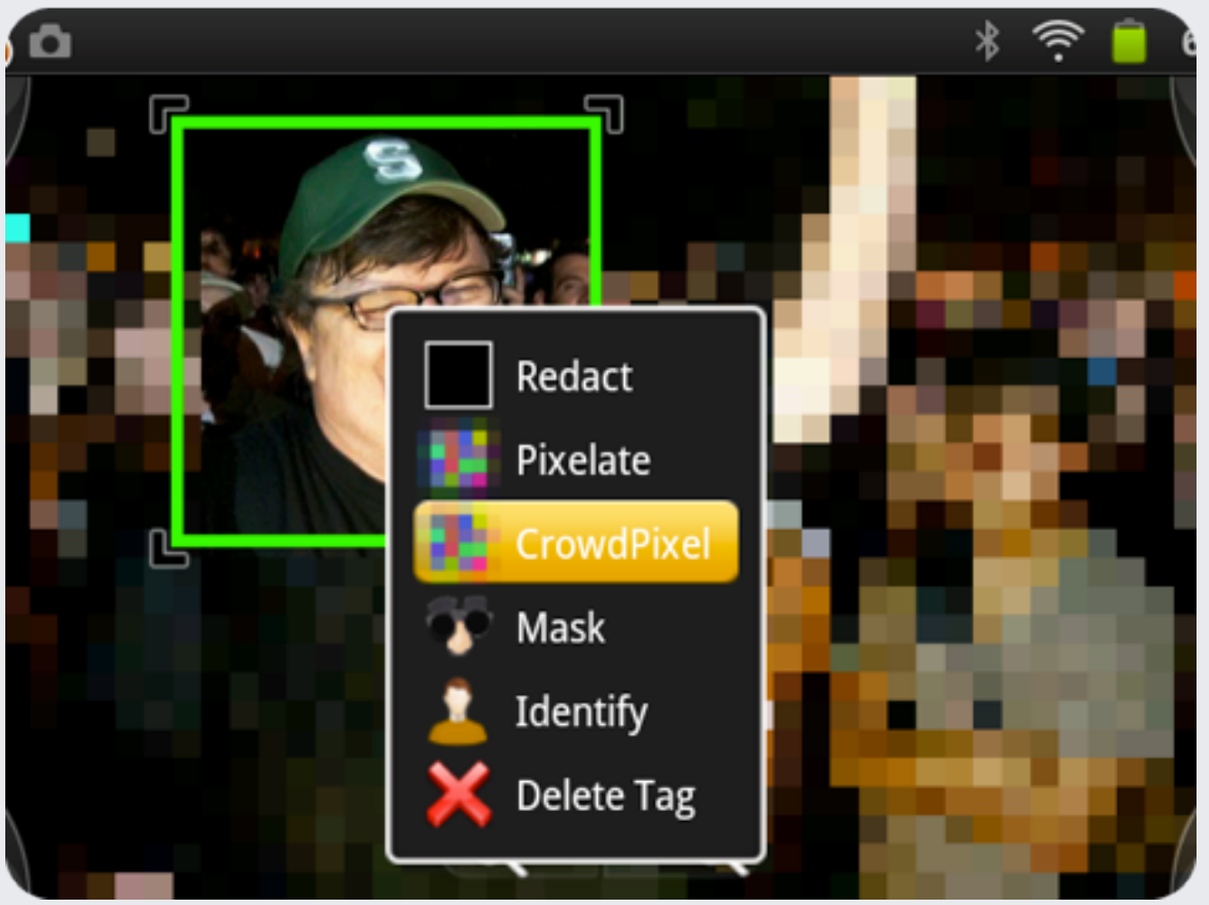
PIXELATE

- The selected region will be pixelated



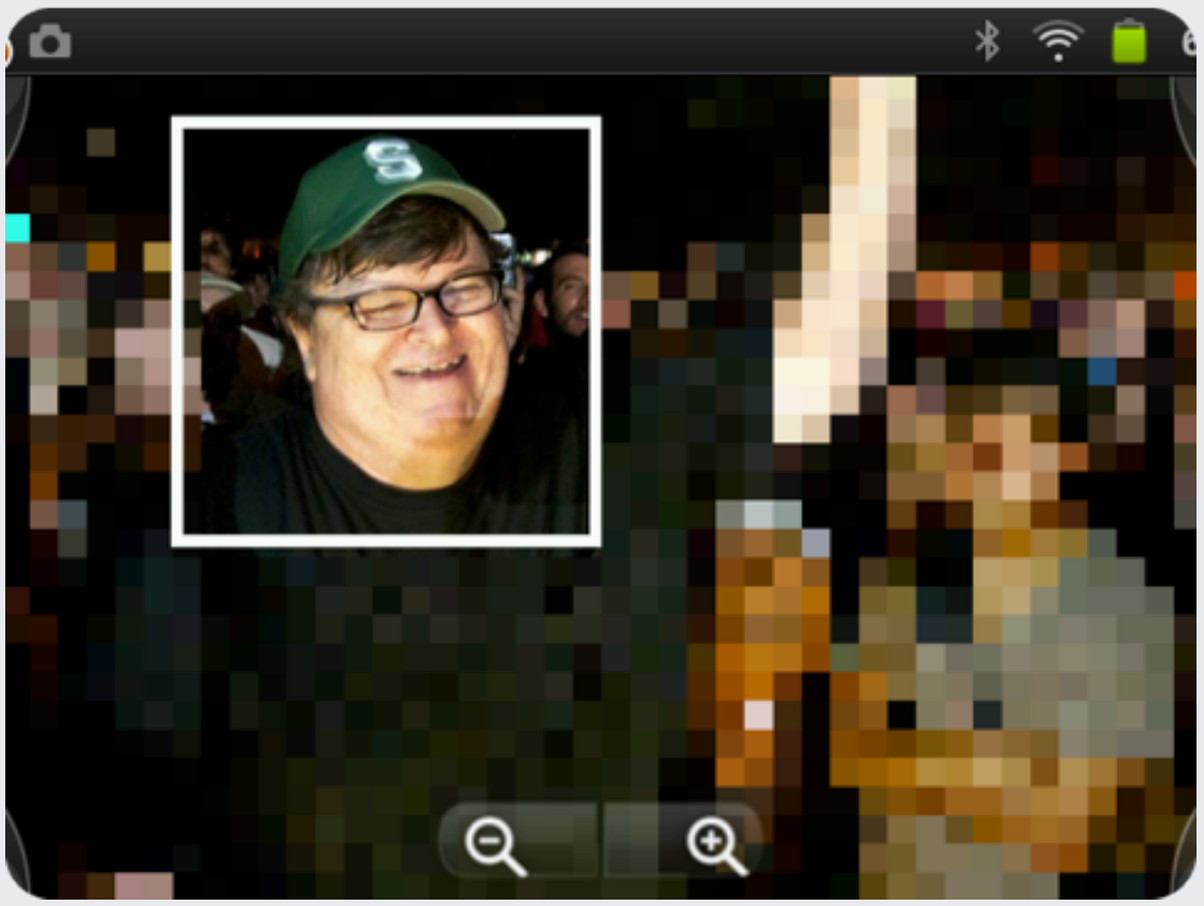
CROWDPIXEL

- From the edit menu select CrowdPixel



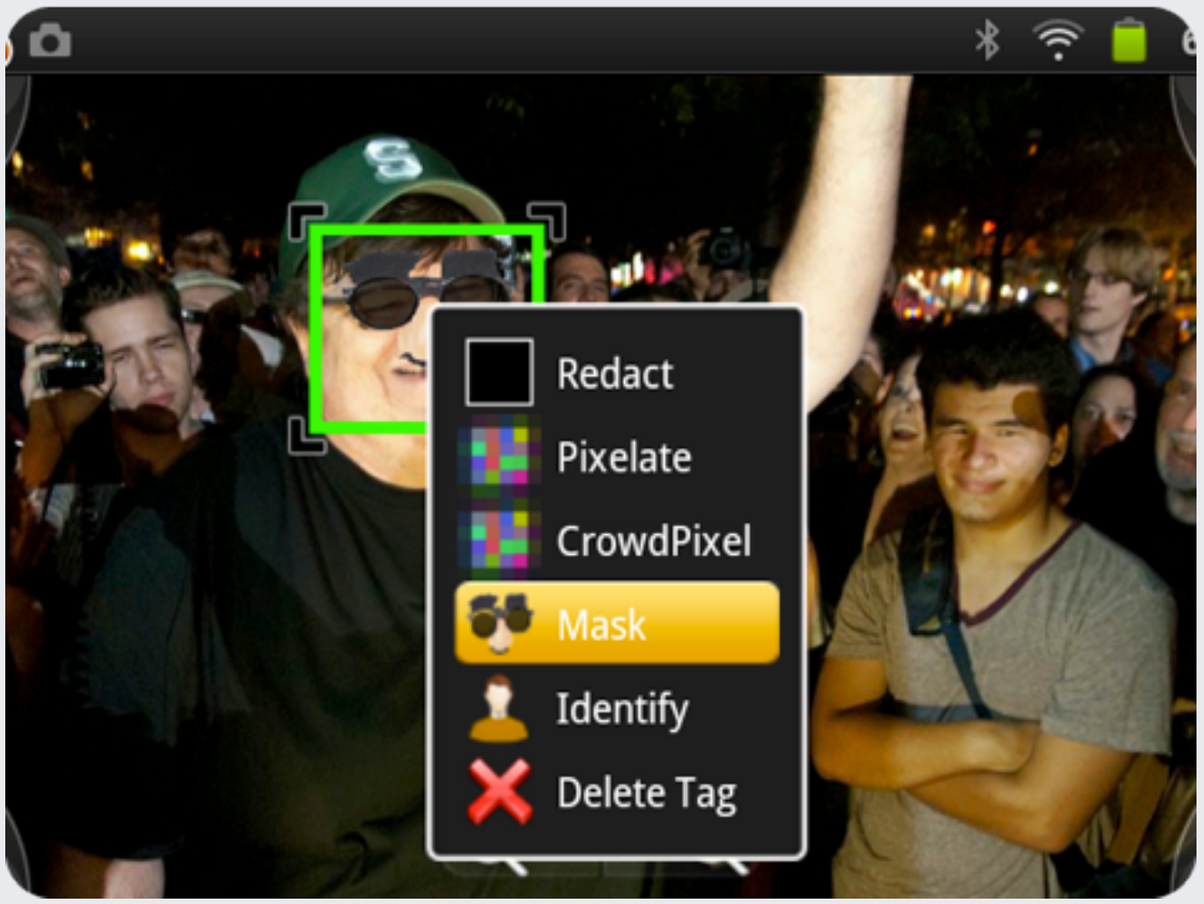
CROWDPIXEL

- Everything OTHER THAN the selected region will be pixelated



MASK

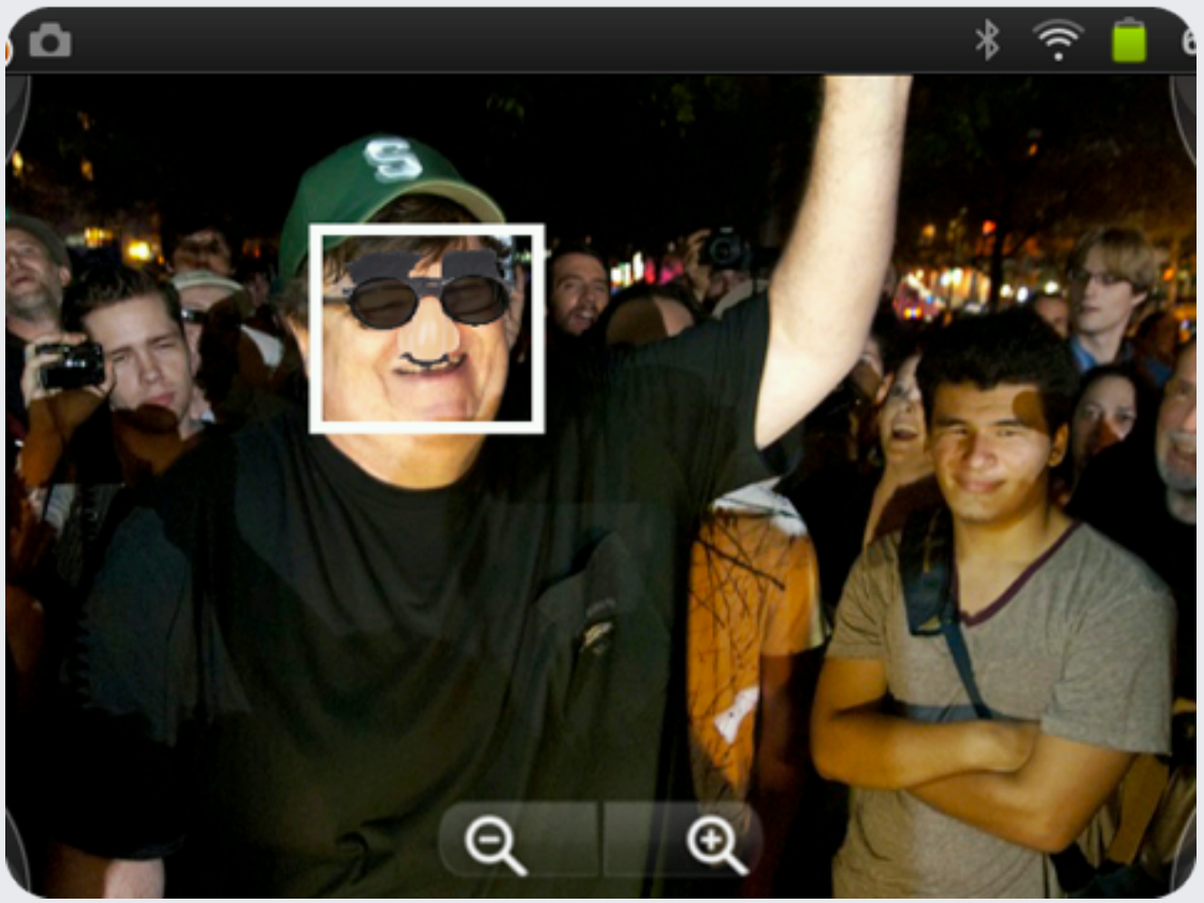
- From the edit menu select Mask



MASK

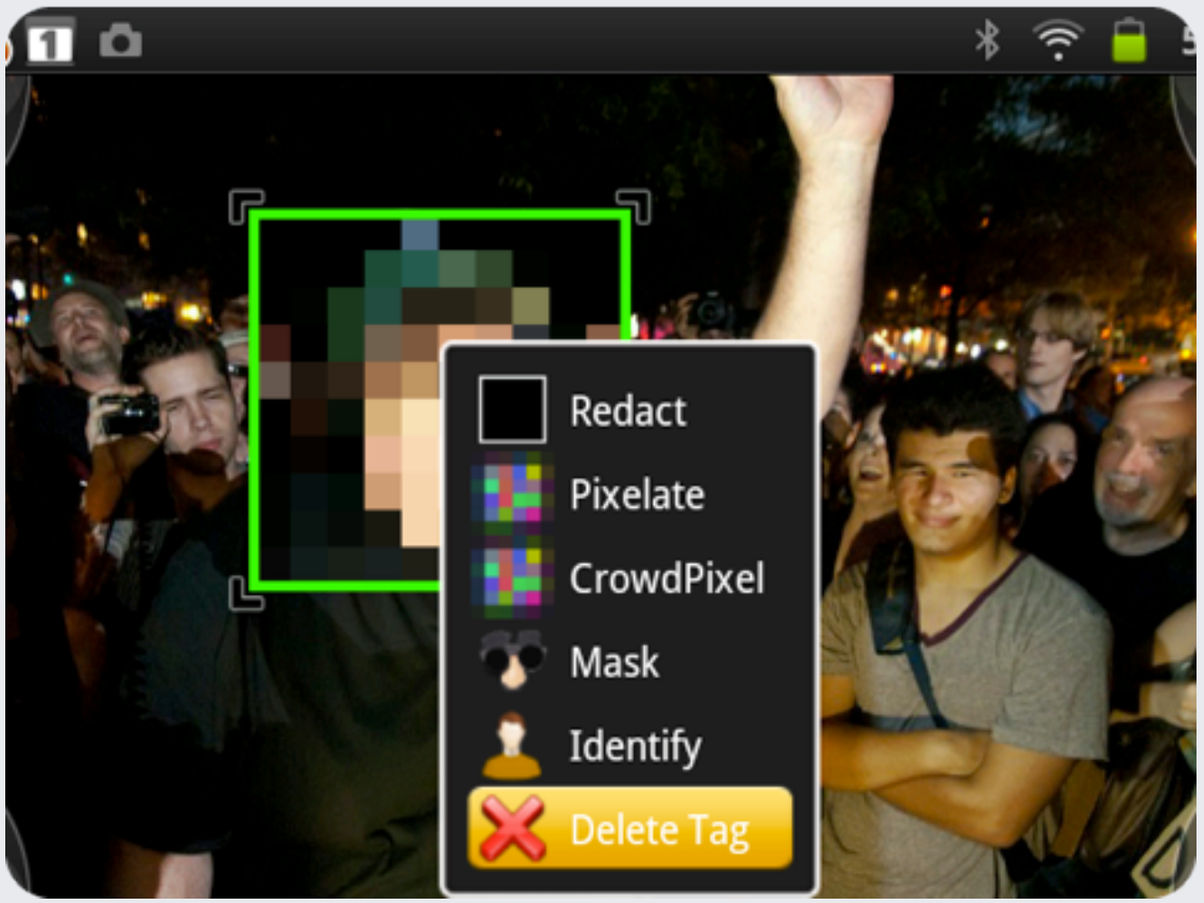
- A mask will partially cover the center of the selected region

- NOTE: Mask will NOT protect anonymity but will defeat automatic face recognition i.e. Facebook



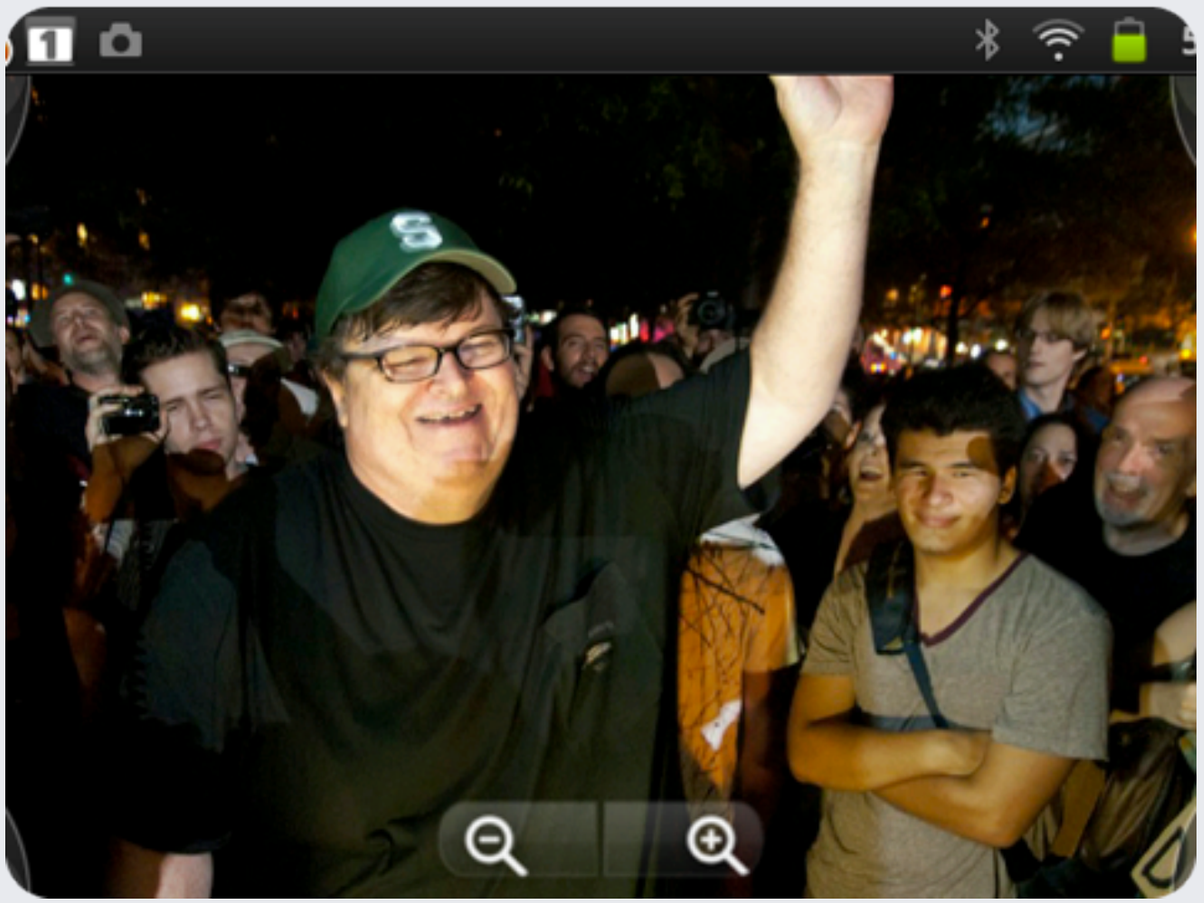
DELETE TAG

- From the edit menu select Delete Tag



DELETE TAG

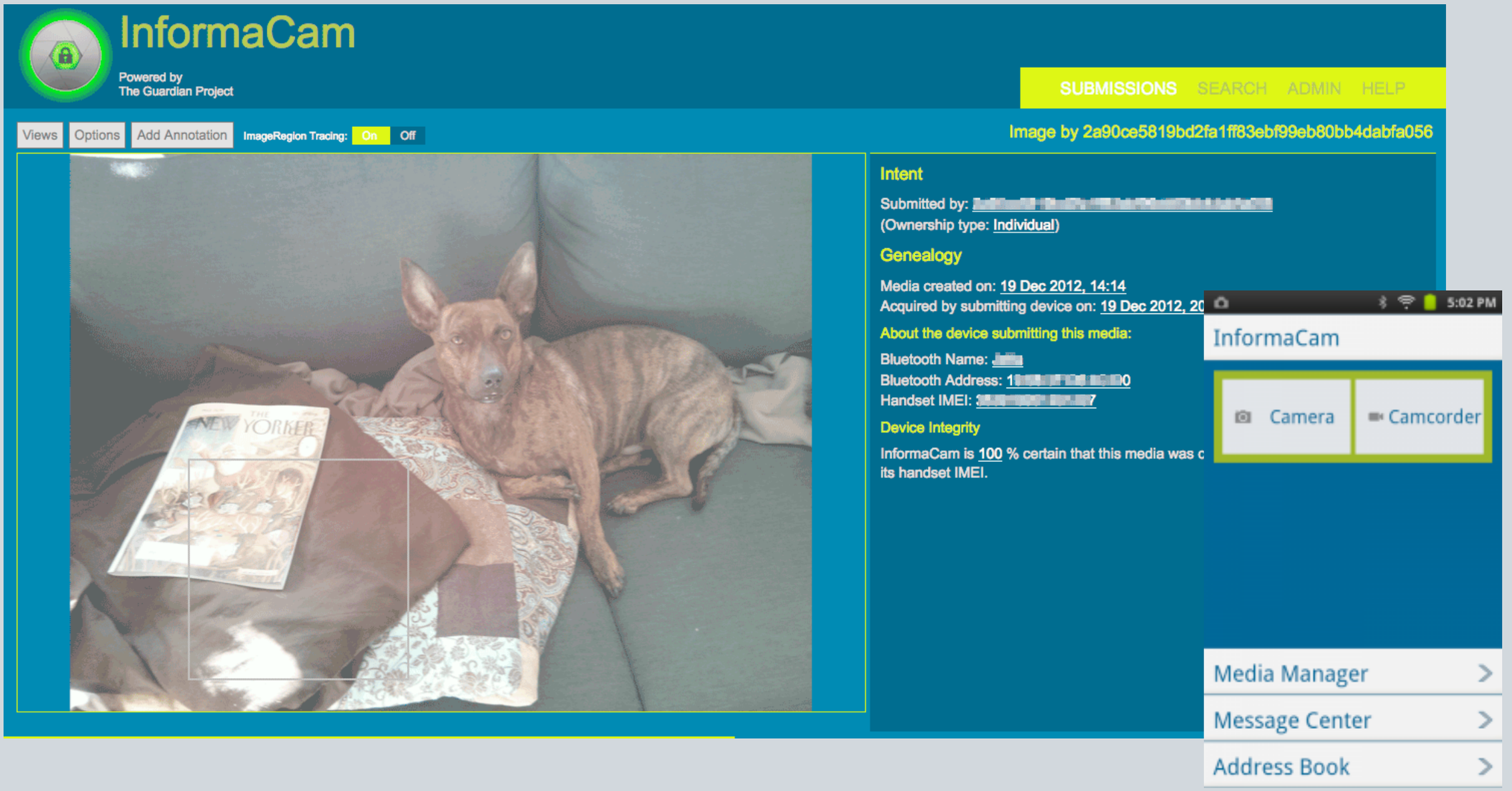
- Deleting Tag will remove the selected region and leave it un-obfuscated



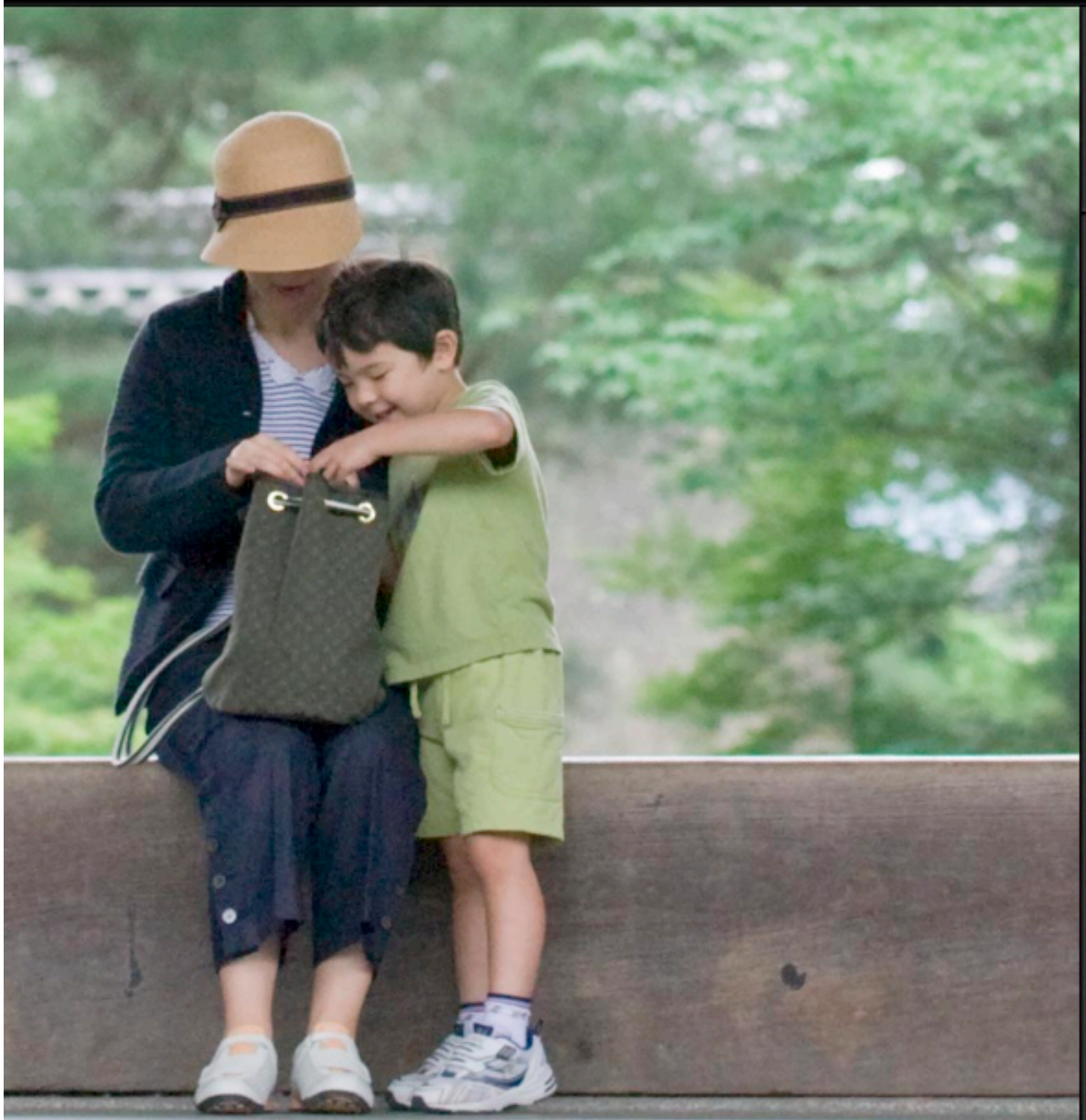
- witness.org
- guardianproject.info

Hurricane Sandy?

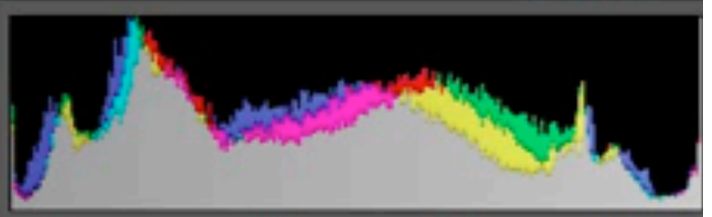
INFORMACAM



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 ƒ / 3.5 1/500 sec

Jeffrey's View — Metadata

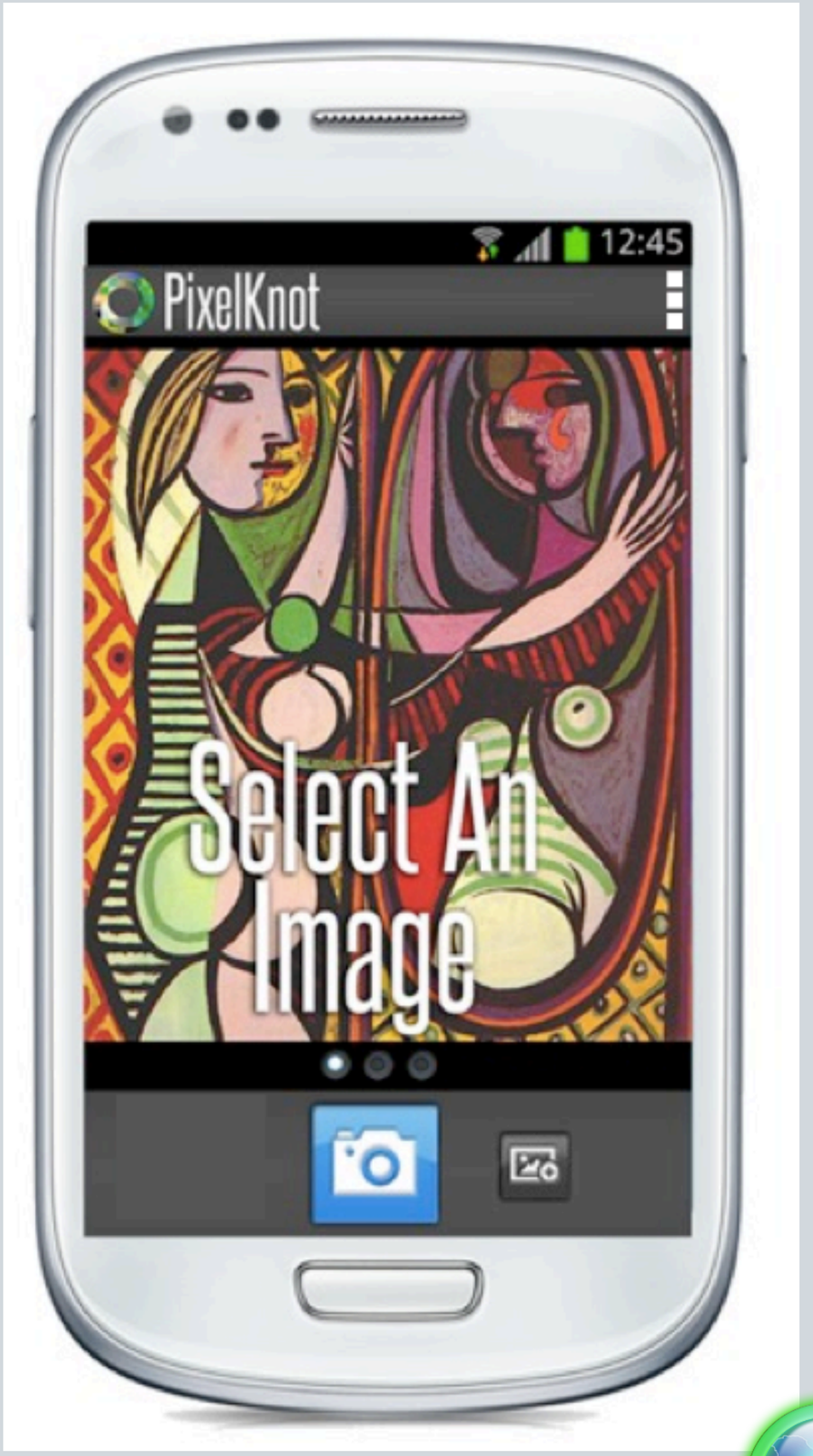
Preset	None
File	JEF_031786.NEF
Folder	10-Nanzenji-Walk
Rating	· · · · ·
View Name	
Title	
Caption	Anthony looks for goodies in Fumie's purse while visiting Nanzenji.
Scene	Stroll at Kyoto's Nanzen Temple
Blog URL	http://regex.info/blog/2007-06-10/486
Artist	Jeffrey Eric Francis Friedl
Copyright	Copyright 2007 Jeffrey Eric Francis Friedl
Date	June 10, 2007
	9:43:11 AM
Size	3872 x 2592
Exposure	1/500 sec at ƒ / 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

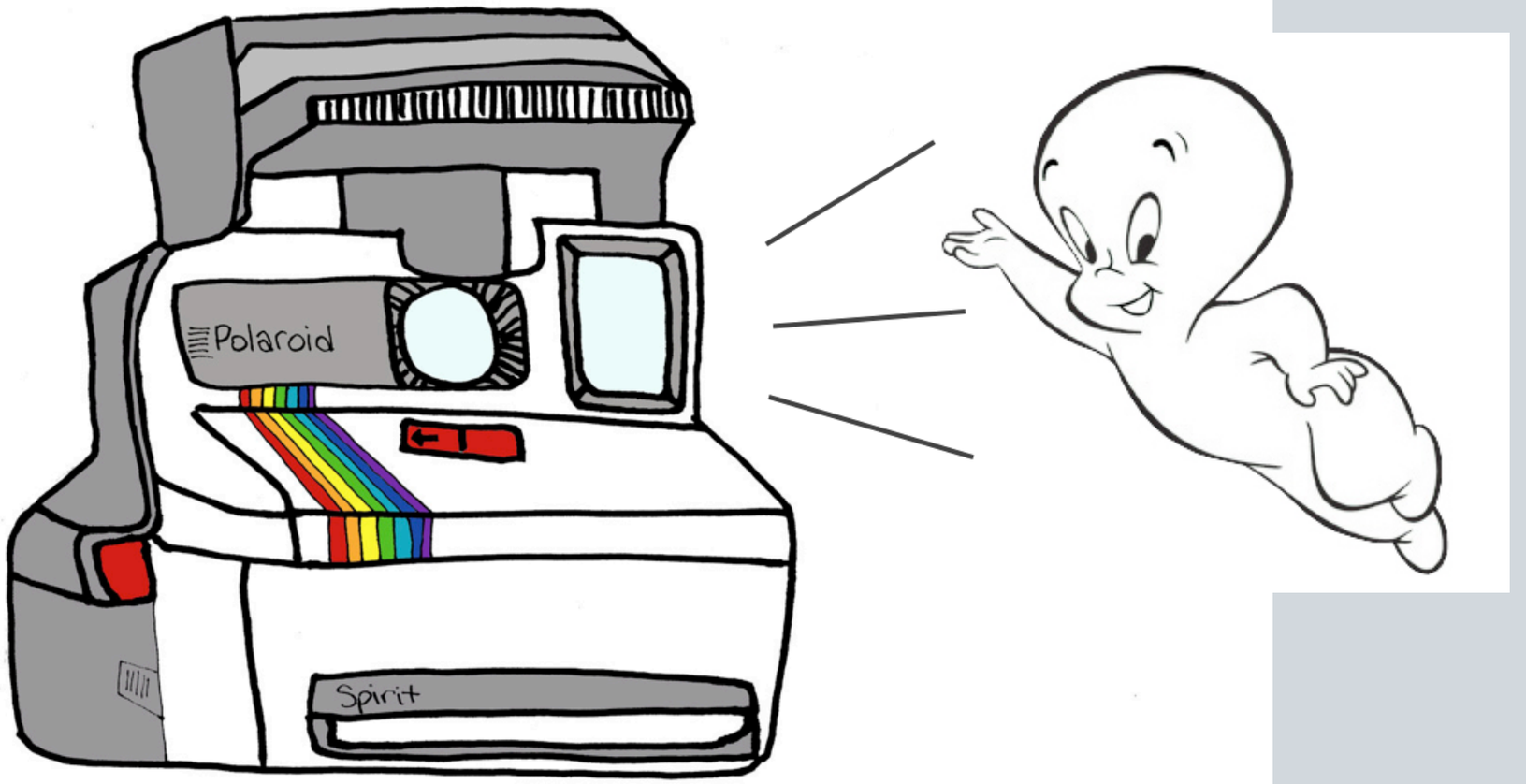
Sync Settings | Sync Metadata

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





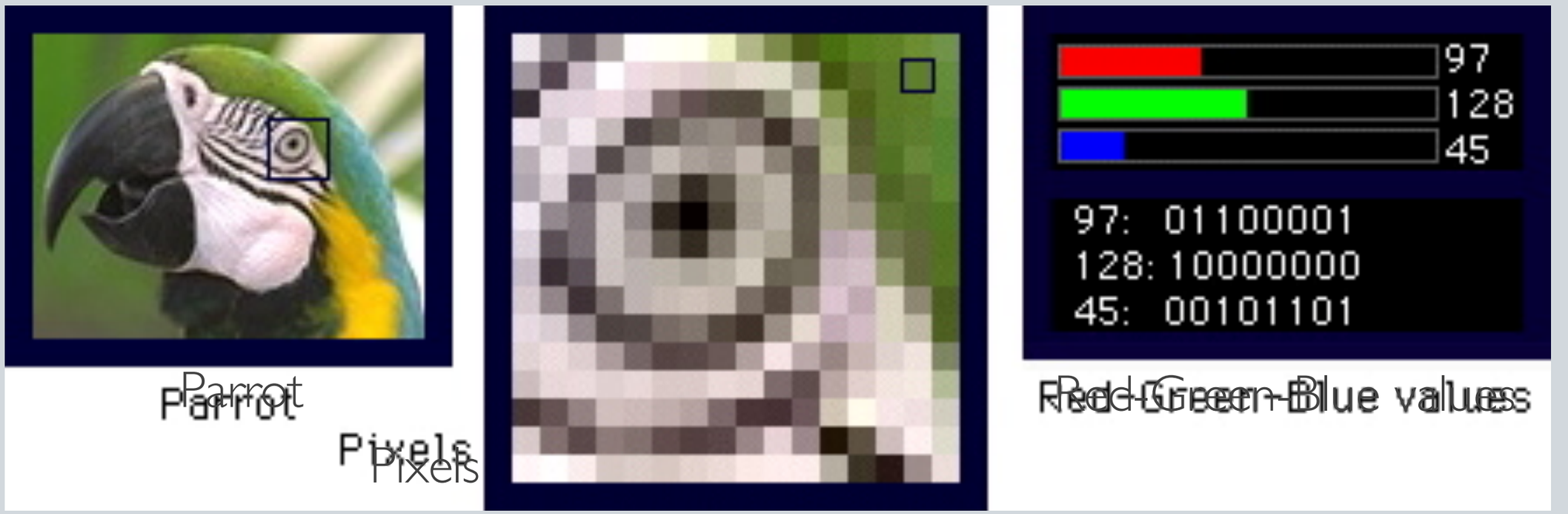
MODERN IMAGE STEGO

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.

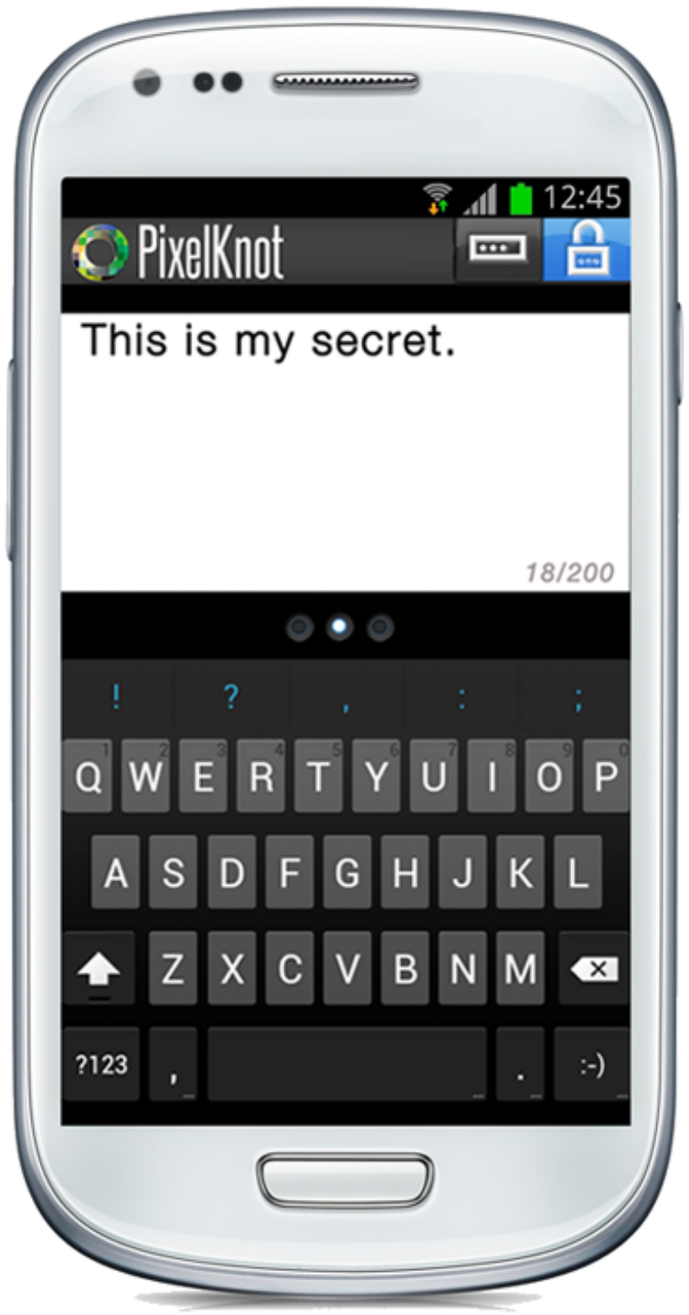
FUTURE SOLUTIONS

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

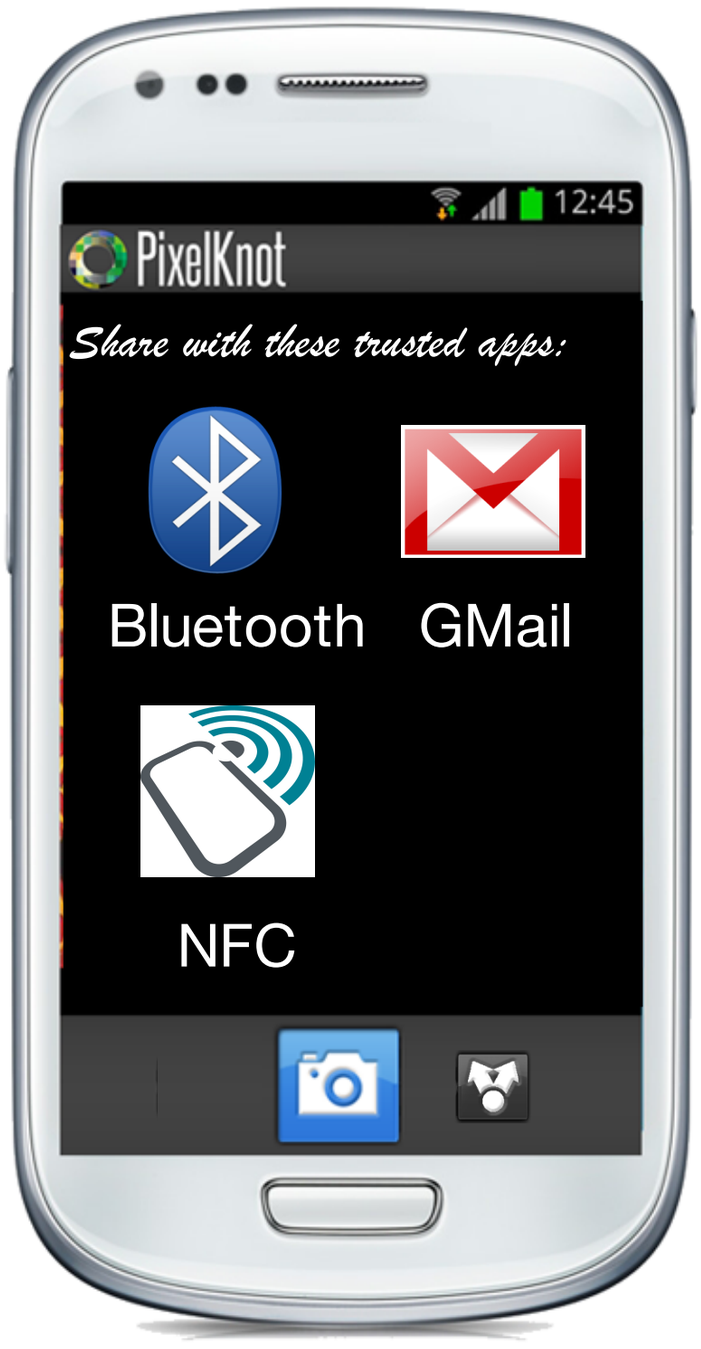
SOCIAL MEDIA INTEGRITY

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.


12:45
PixelKnot
Select An Image

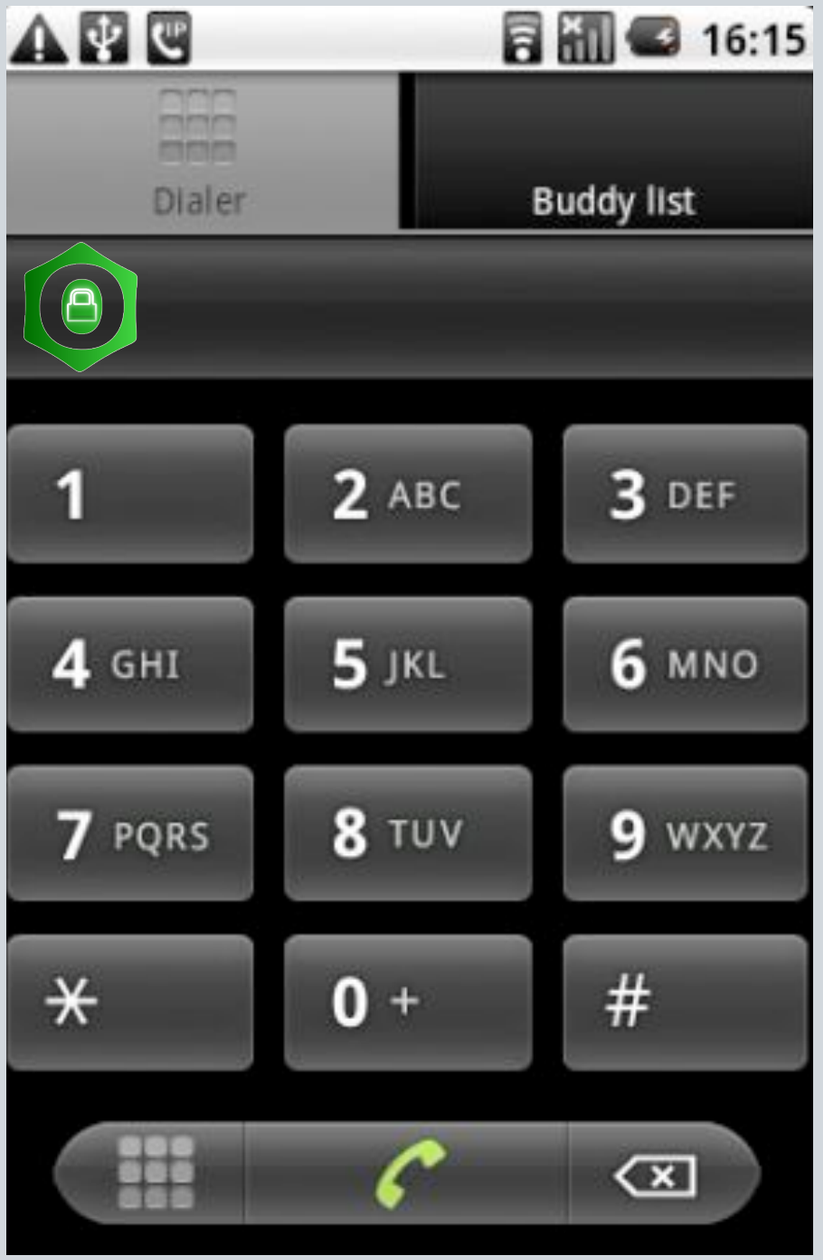

12:45
PixelKnot
This is my secret.
18/200
! ? , : ;
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
?123
:-)


12:45
PixelKnot
Cat's Paw
Loading...


12:45
PixelKnot
Share with these trusted apps:
Bluetooth
GMail
NFC

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.



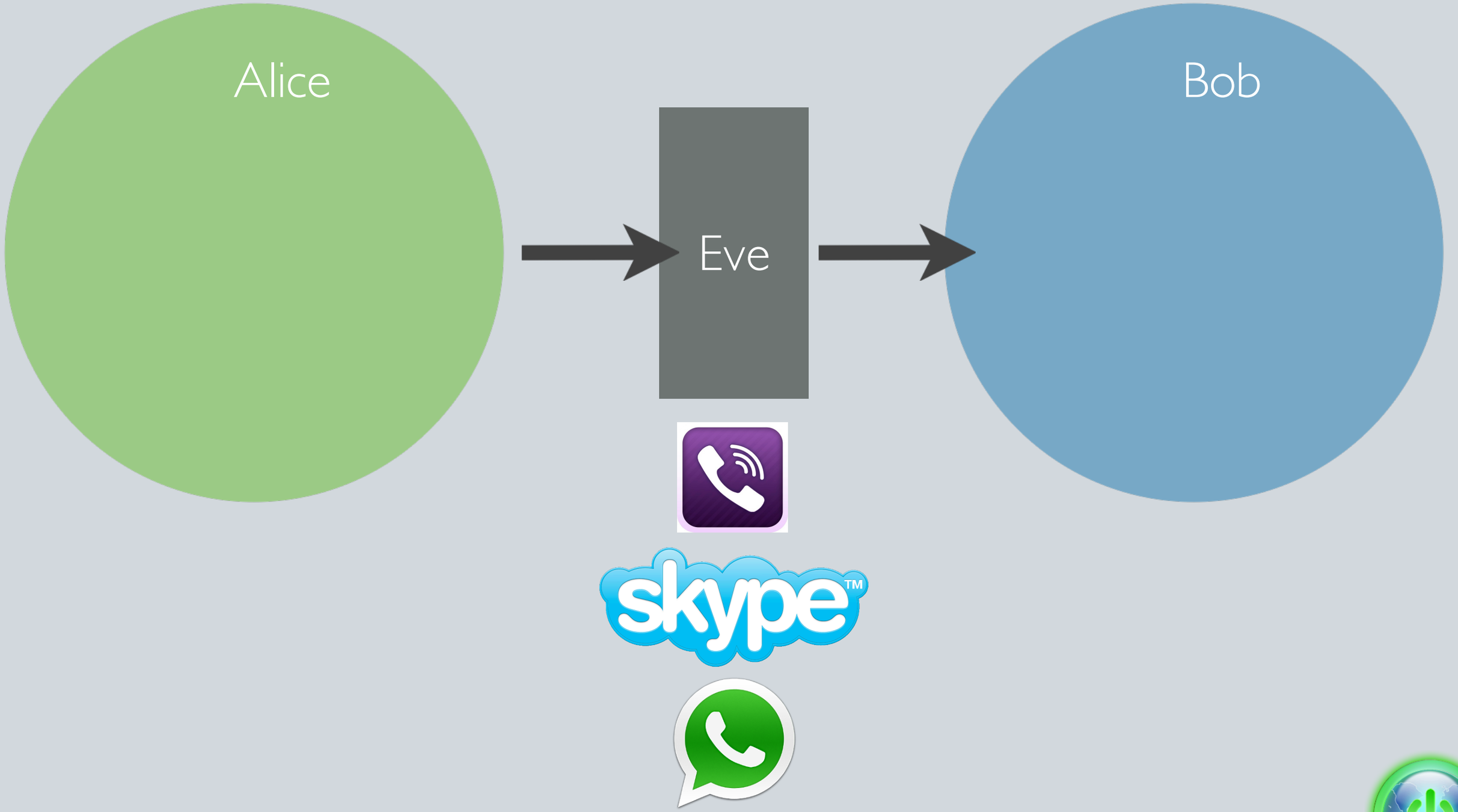
- Built-in public key encryption with ZRTP
- A network of compliant server/service instances
- Client software on mobile and desktop
- Currently functioning on Android, iPhone, Blackberry, PC & Linux
- https://ostel.me

NOKIA

Linux™

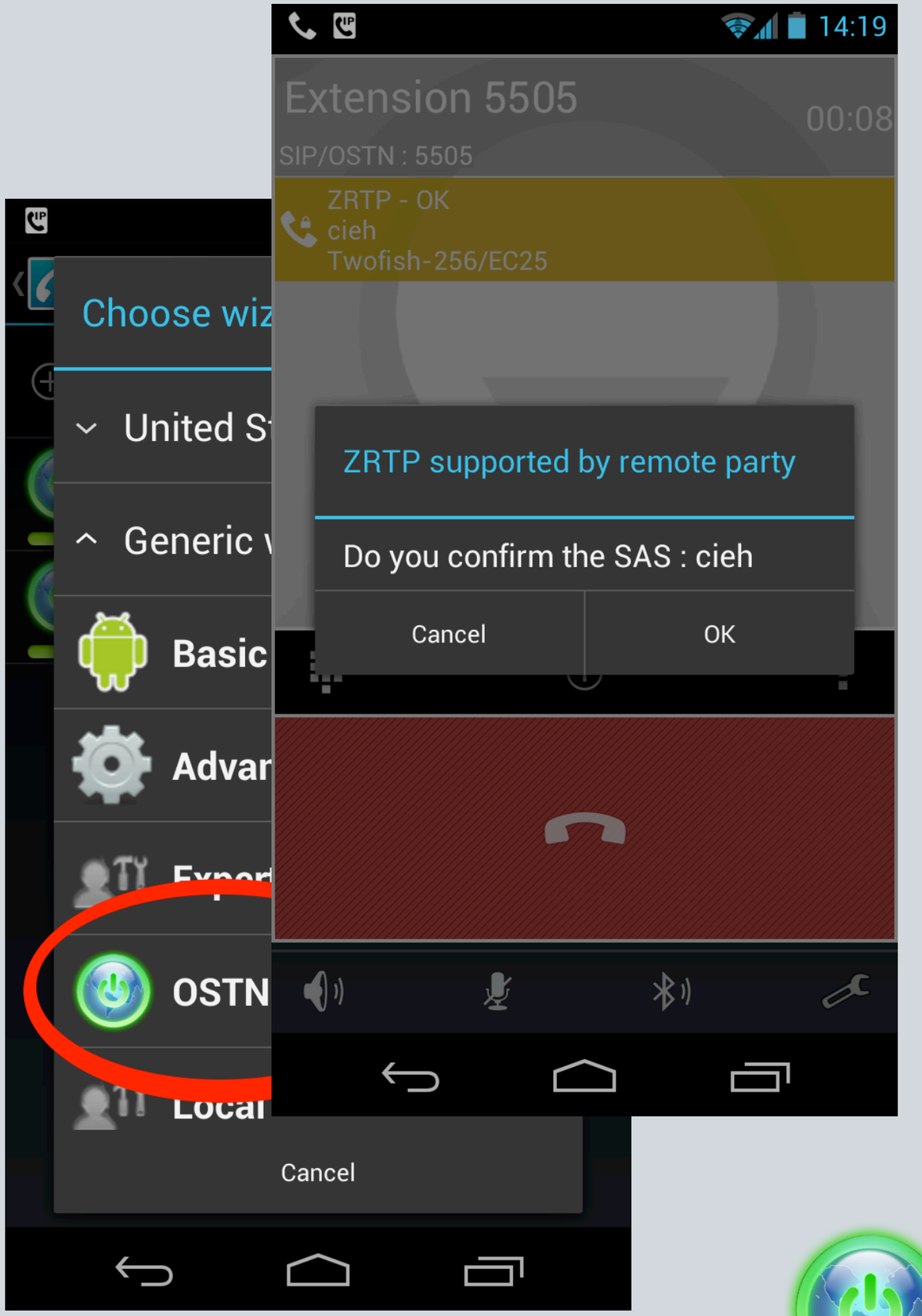
Windows®

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.



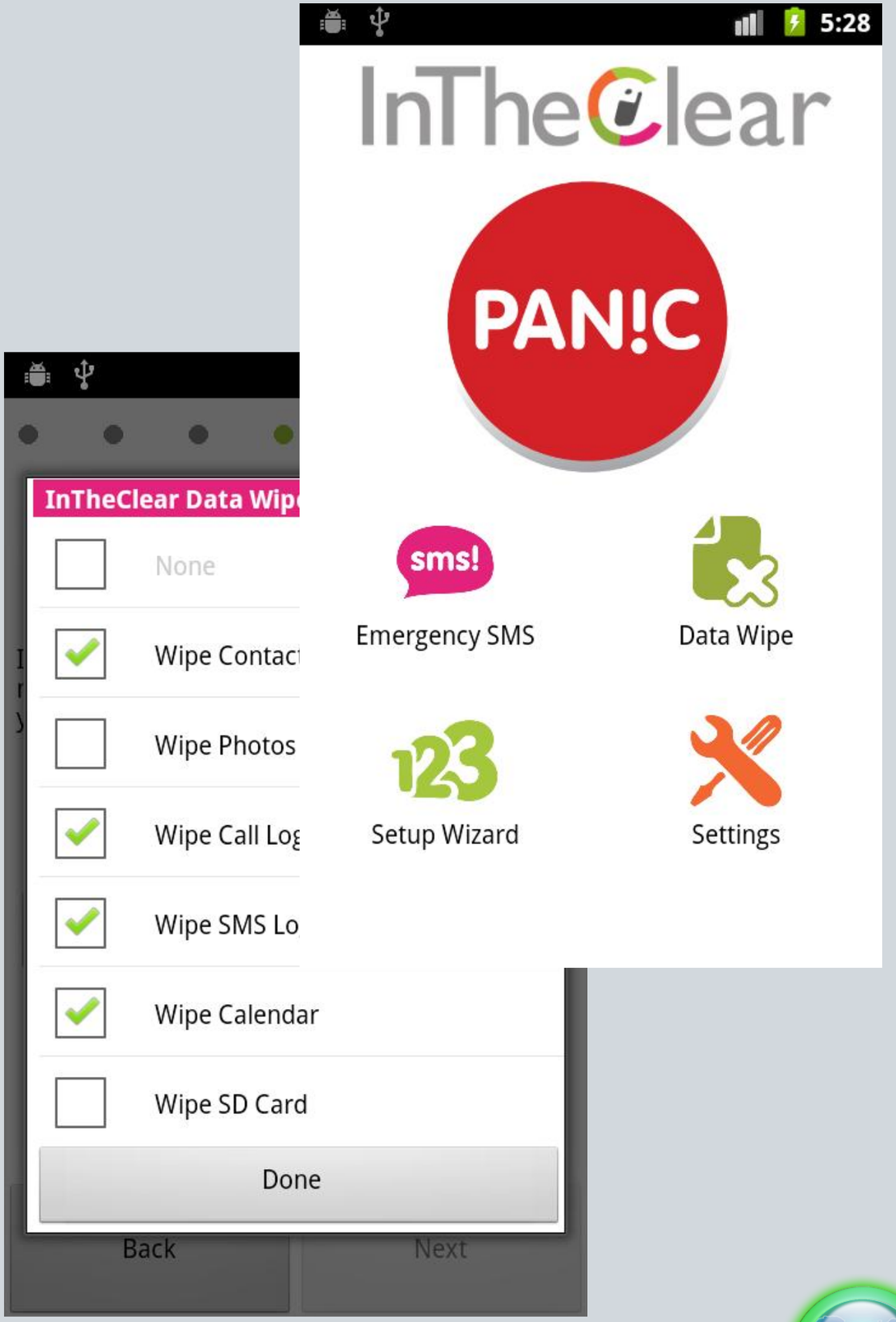
OSTEL.ME

TOR AND OTHER PROBLEMS

IN THE CLEAR

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

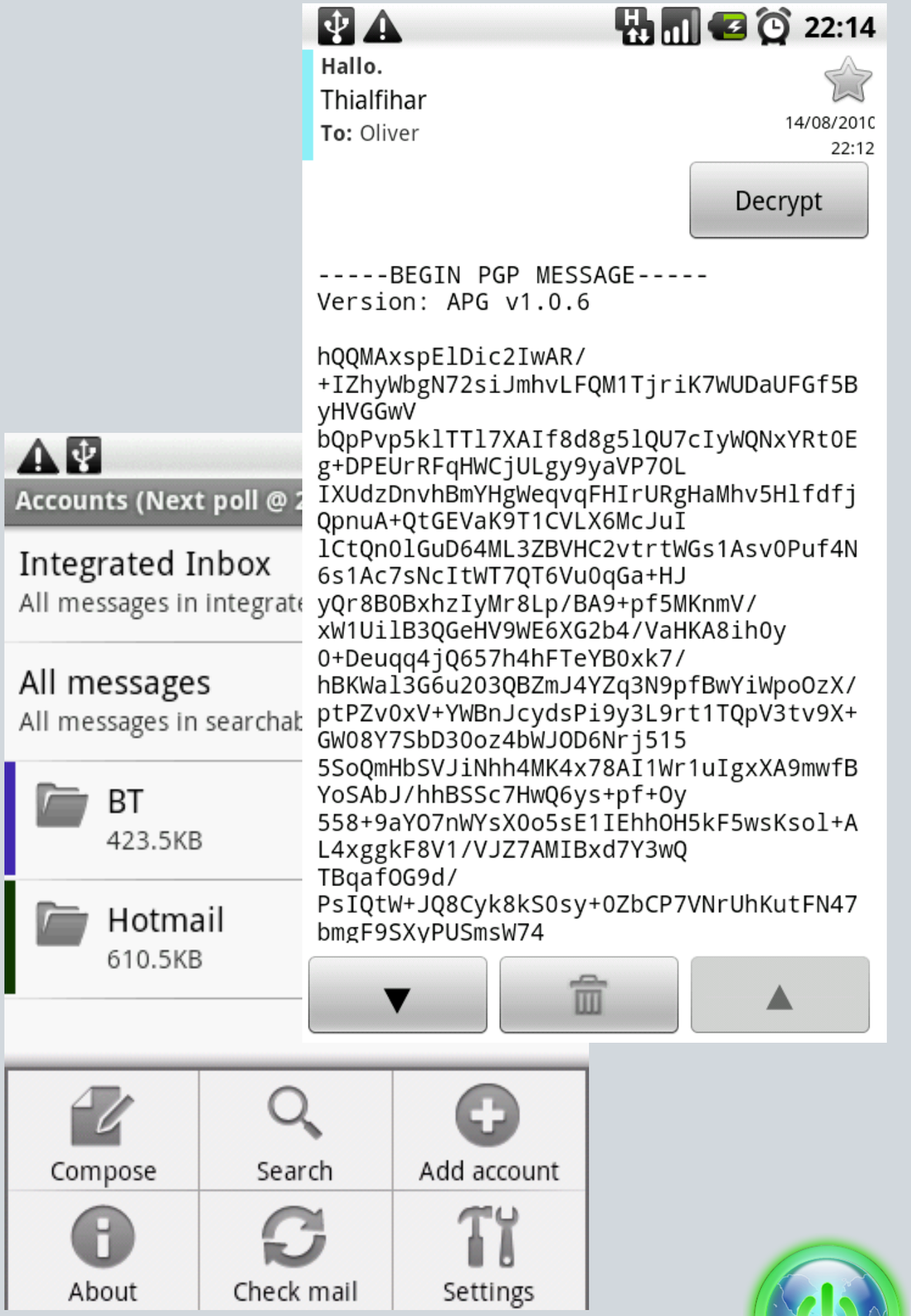
- Quick, one-touch activate
- Wipe data across different Android apps and external storage / SD Card
- Emergency SMS sends in background repeatedly with location and cell network dataAlso available on Blackberry and Java (Nokia, etc) phones

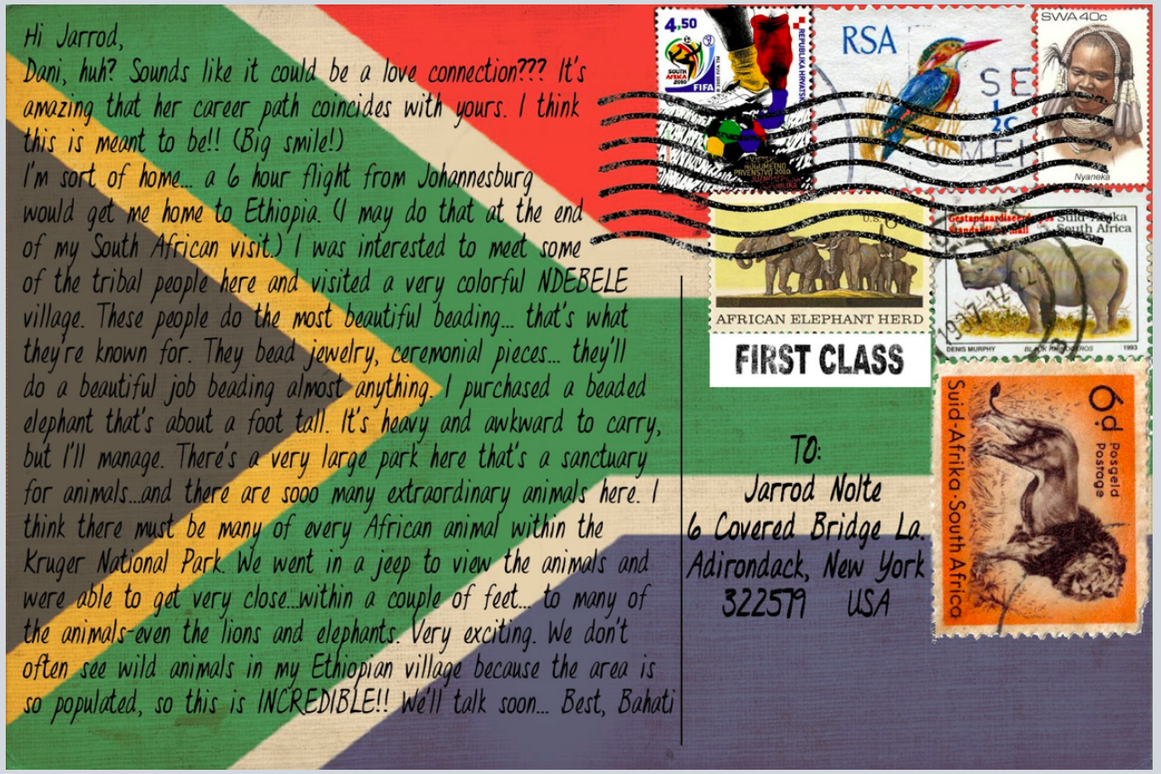


K-9 MAIL

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





POSTCARD Vs. LETTER

POSTCARD Vs. LETTER

WAX SEAL

hello

File Edit View Insert Format Tools Message Help

Send | Cut | Copy | Paste | Undo | Check | Spelling | Attach | Priority | Sign | Encrypt | Offline

To: some@one.com

Cc:

Subject: hello

Arial 10

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0

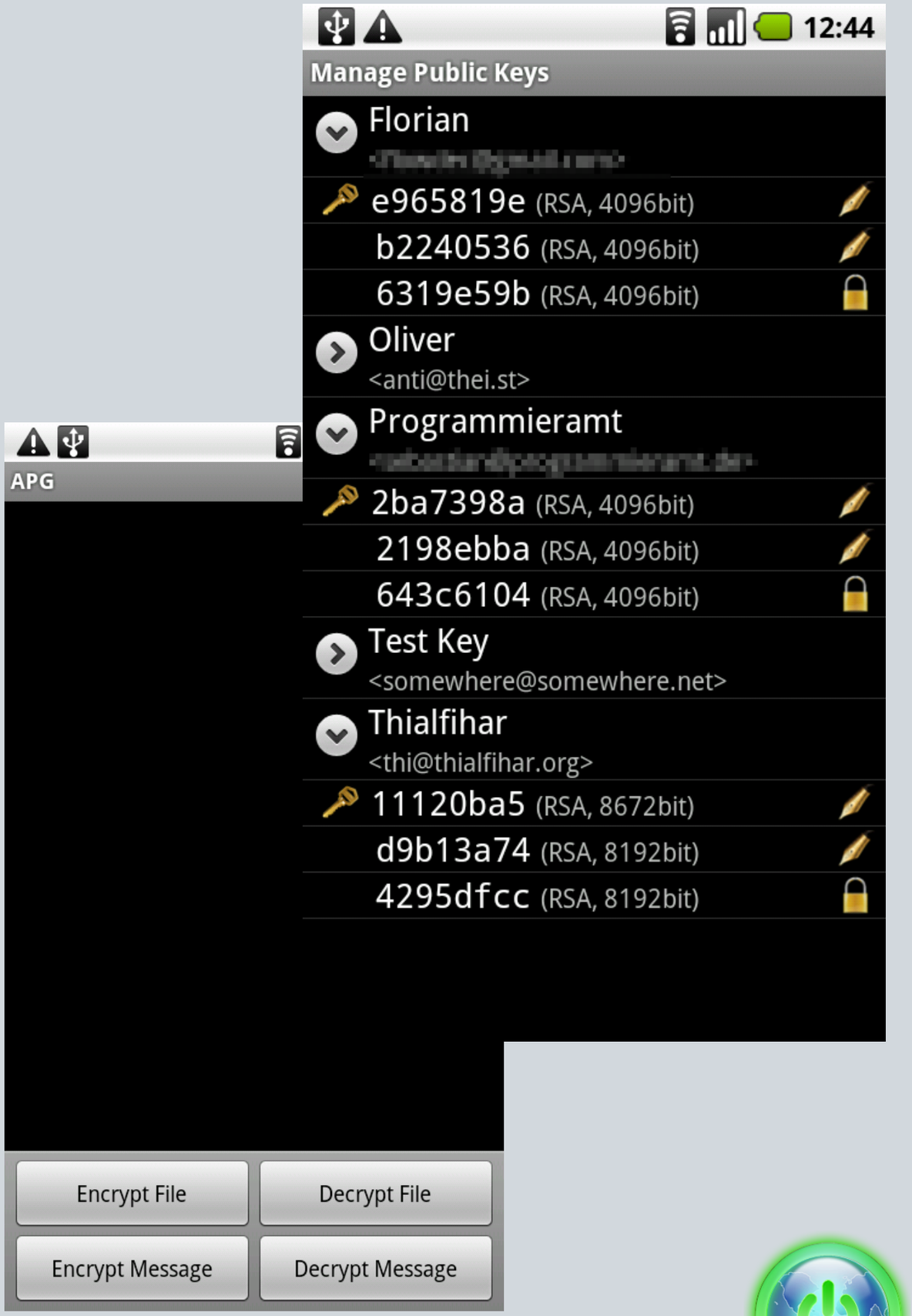
hQEOA76kihKpxmEmEAP9HMUEf8vN7M4i81thj38qTctb15P2jP353UBNippi6K1H
466iArA8UospU3MoVE2WDdNbAfz36QkovArlHdlOODwOsPfVaG7uipWAJpGZ9MsA
Ey/ycMtE+9+rBN/17XpCrg5QG/16jlpasdUFSMx32q0fUdNAOQwo3heLGQ2pqylE
AOsSqhSKQJSOkCWla9fyfH7eD0jDIYZGFJ9by/mXMt5kTsZgtM0+BTNX6gvkE52g
bbVL/man6U2mM+8kyagv6r0d+cmyE52cDPPfkQj6klMNk5ESHM60BwdtKGRkgZmX
nFs4xqMSwTnBlEW4FFVDrYi0iAMV4lk2F9W4clZ9+fWd0lgBuMBNod+V4ga2PAzP
SMdii34Pnqn3ICb7eaz3kYP9o7KVaLxFSYPjE/rYWs1apRKD29O+b4FCosUHZuKo
MmiKYExQulp59RRPETkwF82yNB8VZ0maReBj
=5LFa
-----END PGP MESSAGE-----

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.

Sources: truste.com | mylookout.com | pewinternet.org | Google Insights Survey | GfK NOP

lookout™
MOBILE SECURITY

HOT OR NOT?

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

TRANSLATION

Help us speak your language.
transifex.com

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

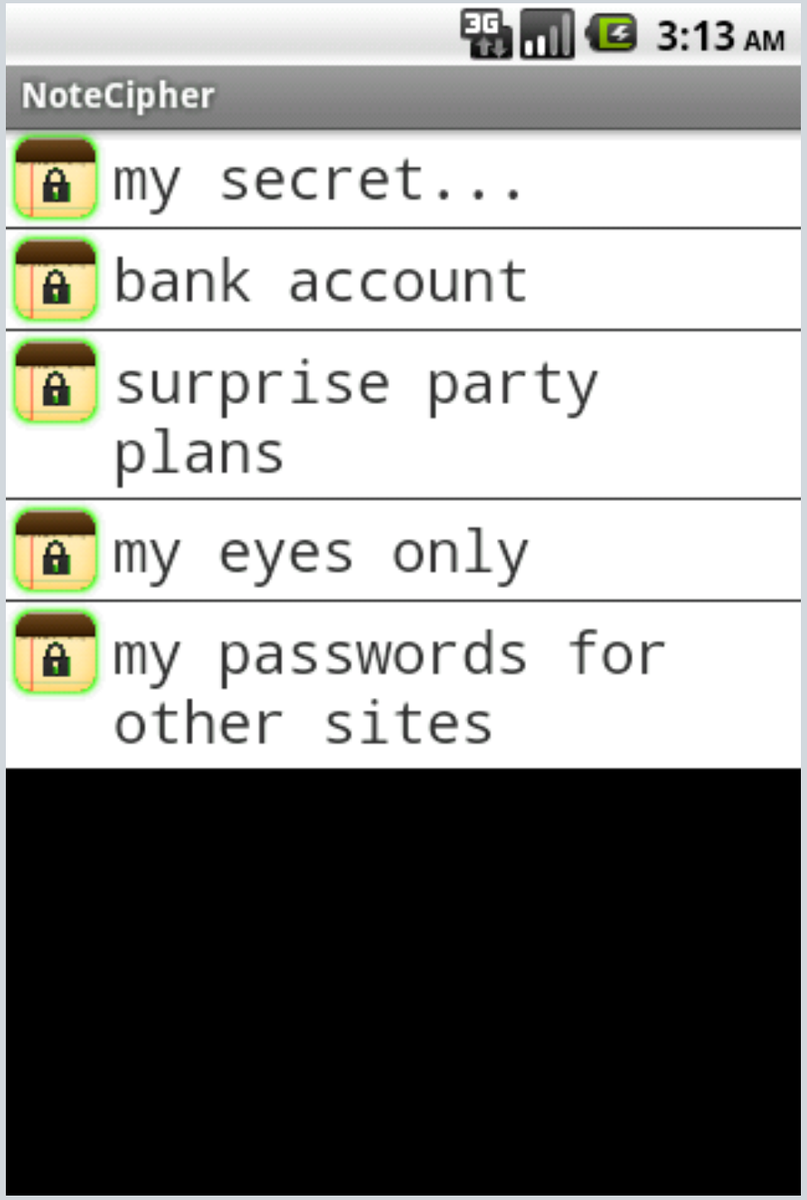
Transparent encrypted virtual disks for Android. This allows Android app developers to use the familiar and well documented android.database.* API to build in encrypted storage into their apps

- 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

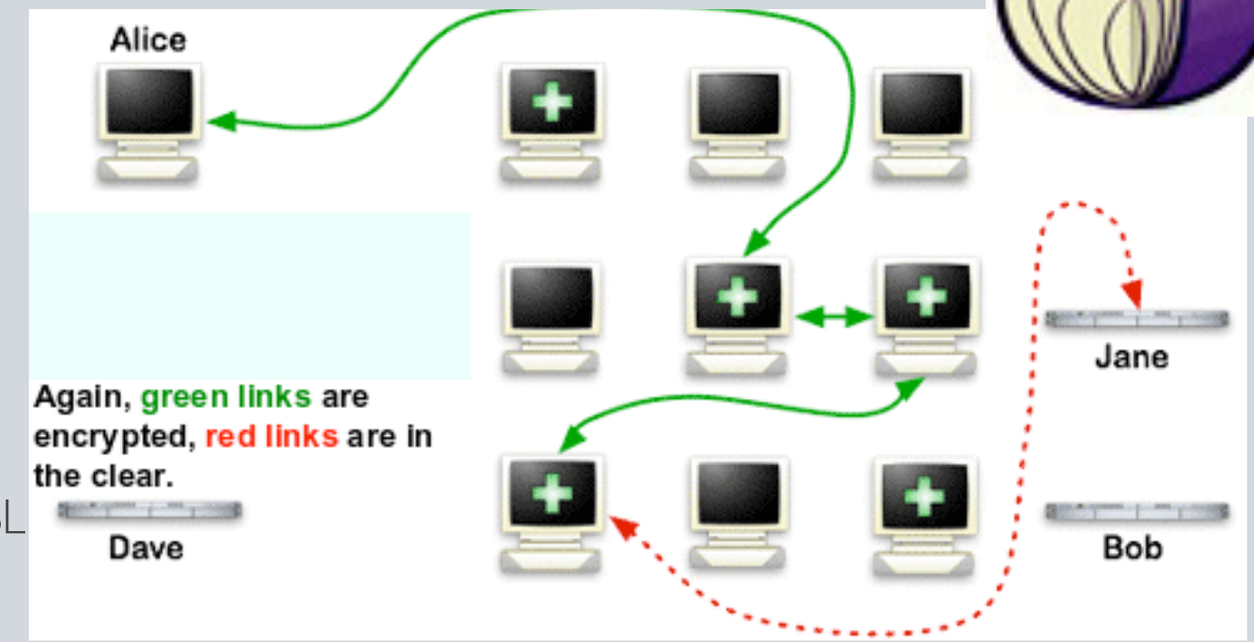
SQLCipher is an SQLite extension that provides encryption of per-app database files.

- 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

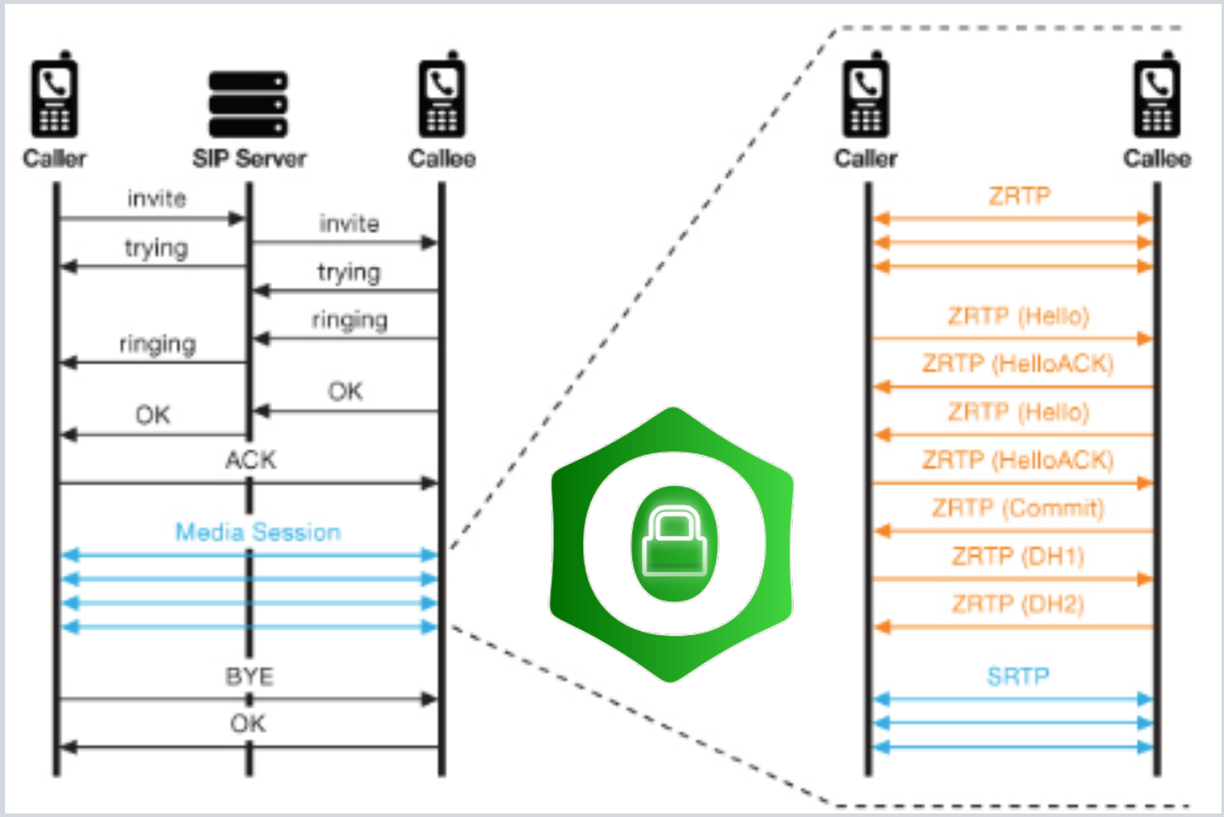
Enabling secure and anonymous network proxying. This is an Android Library for use by any application that wishes to route its network traffic through Orbot/Tor.



- 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 HTTP/S 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

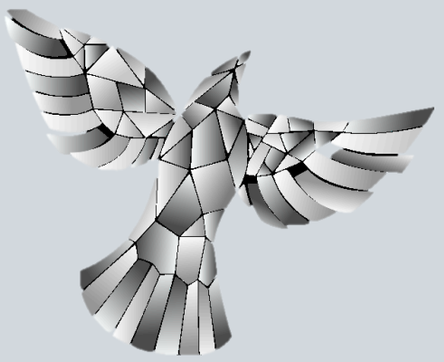
Partner in advocacy and awareness campaigns on mobile security & privacy

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