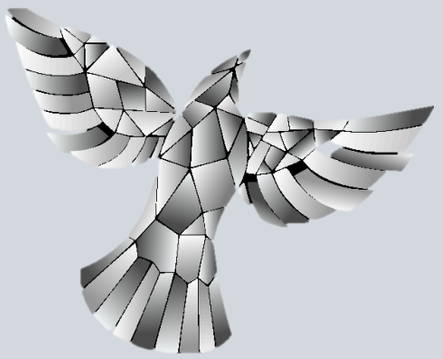
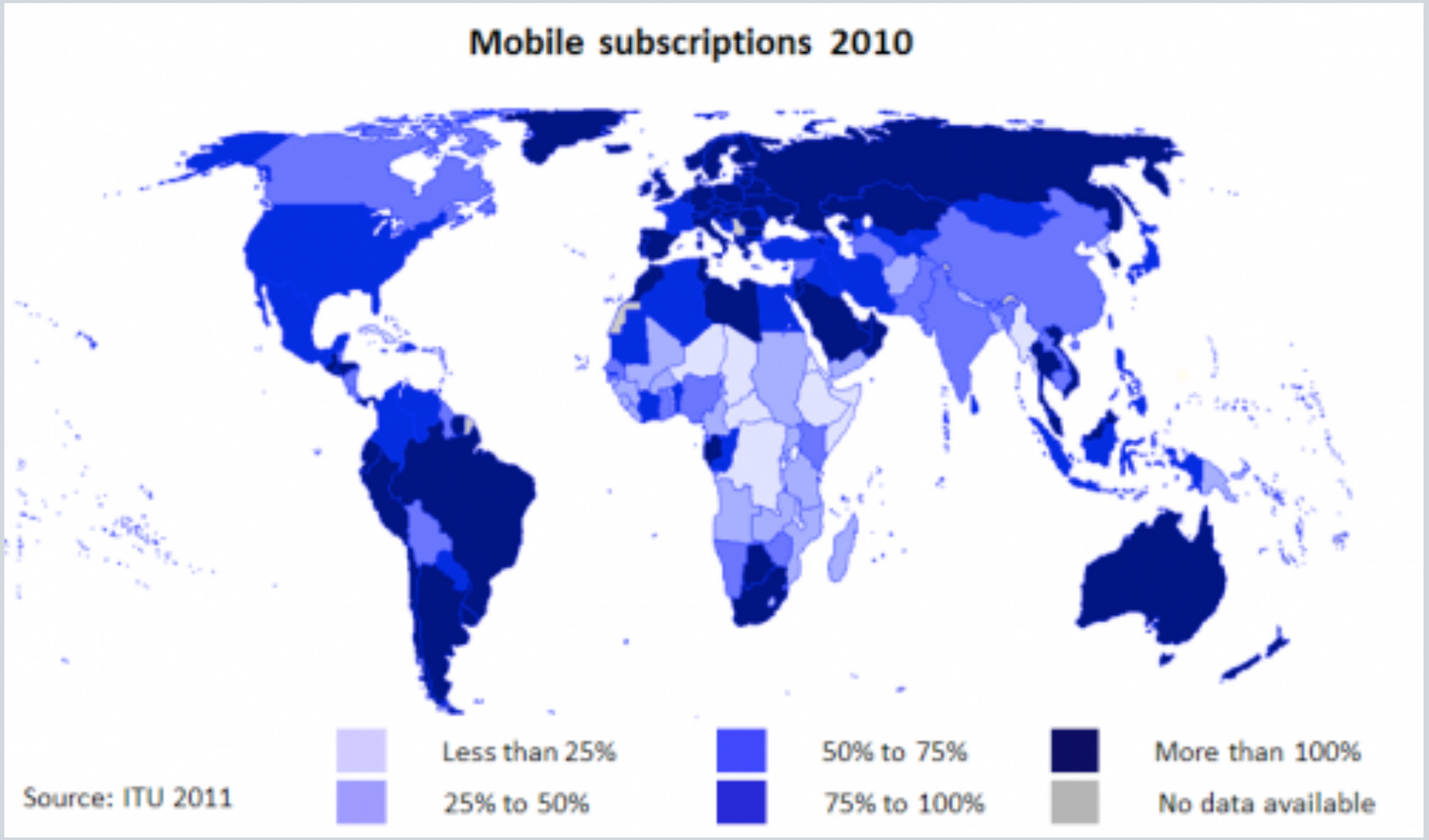
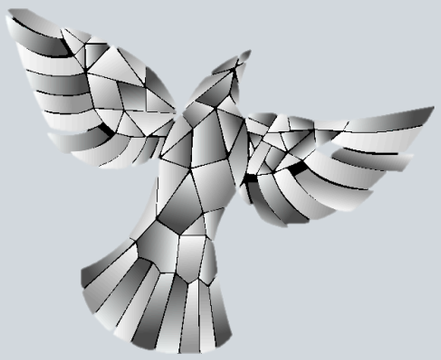
THE GUARDIAN PROJECT

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

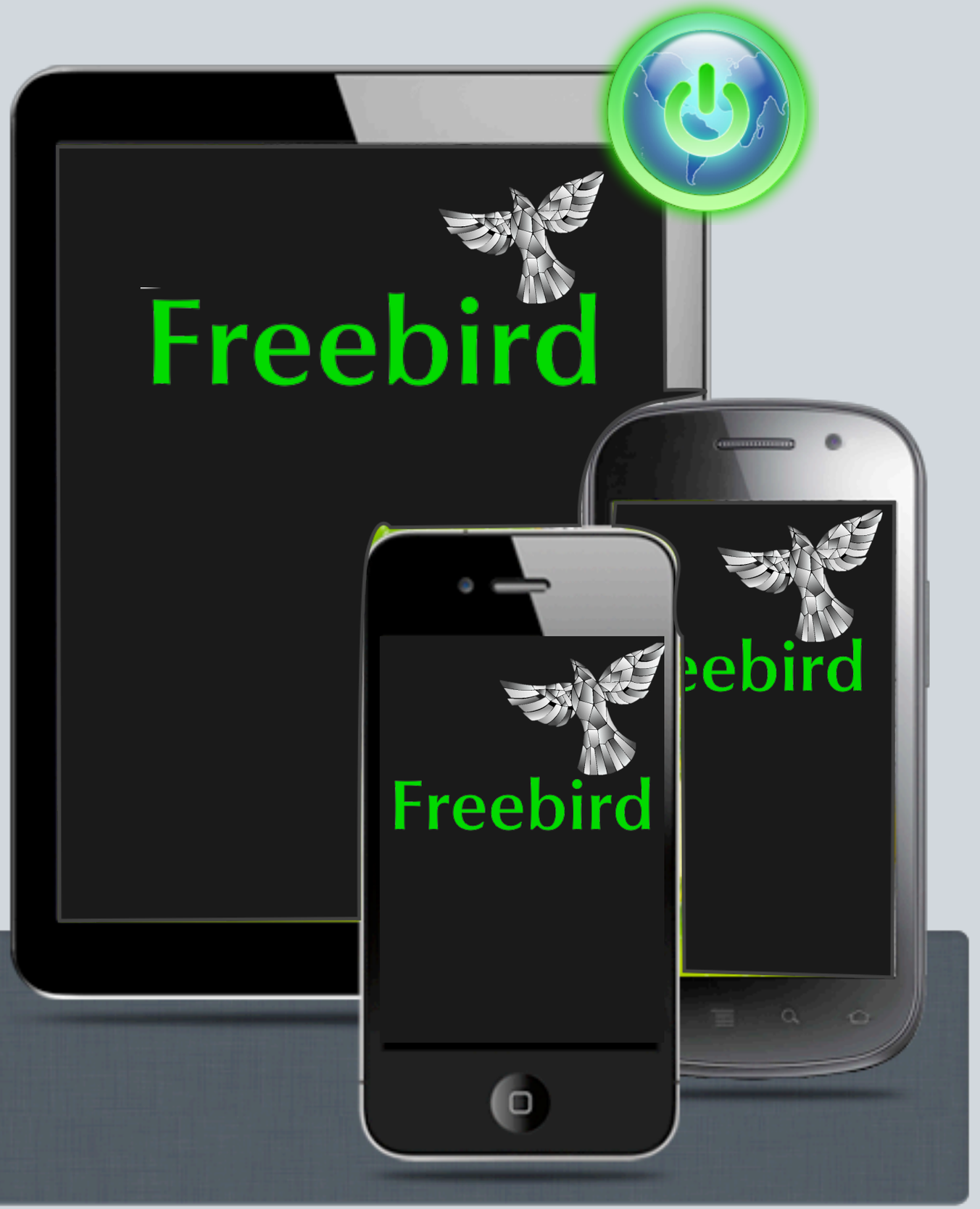
OPEN SOURCE

- 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.



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**

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

USER TOOLS

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

ORBOT

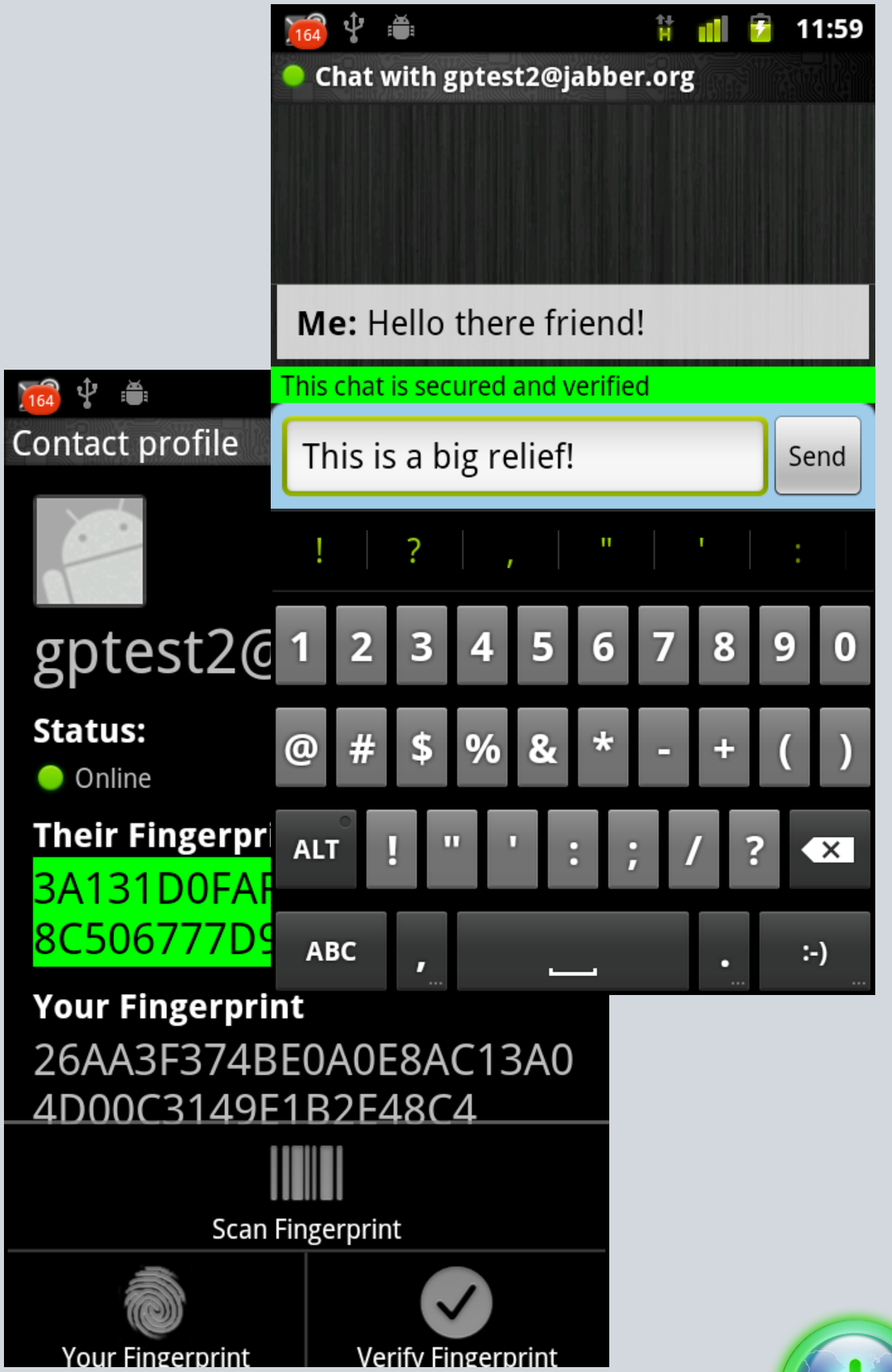
Tor on Android: providing free software and an open network that helps defend against network traffic analysis - a form of surveillance that threatens personal freedom and privacy

- 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

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

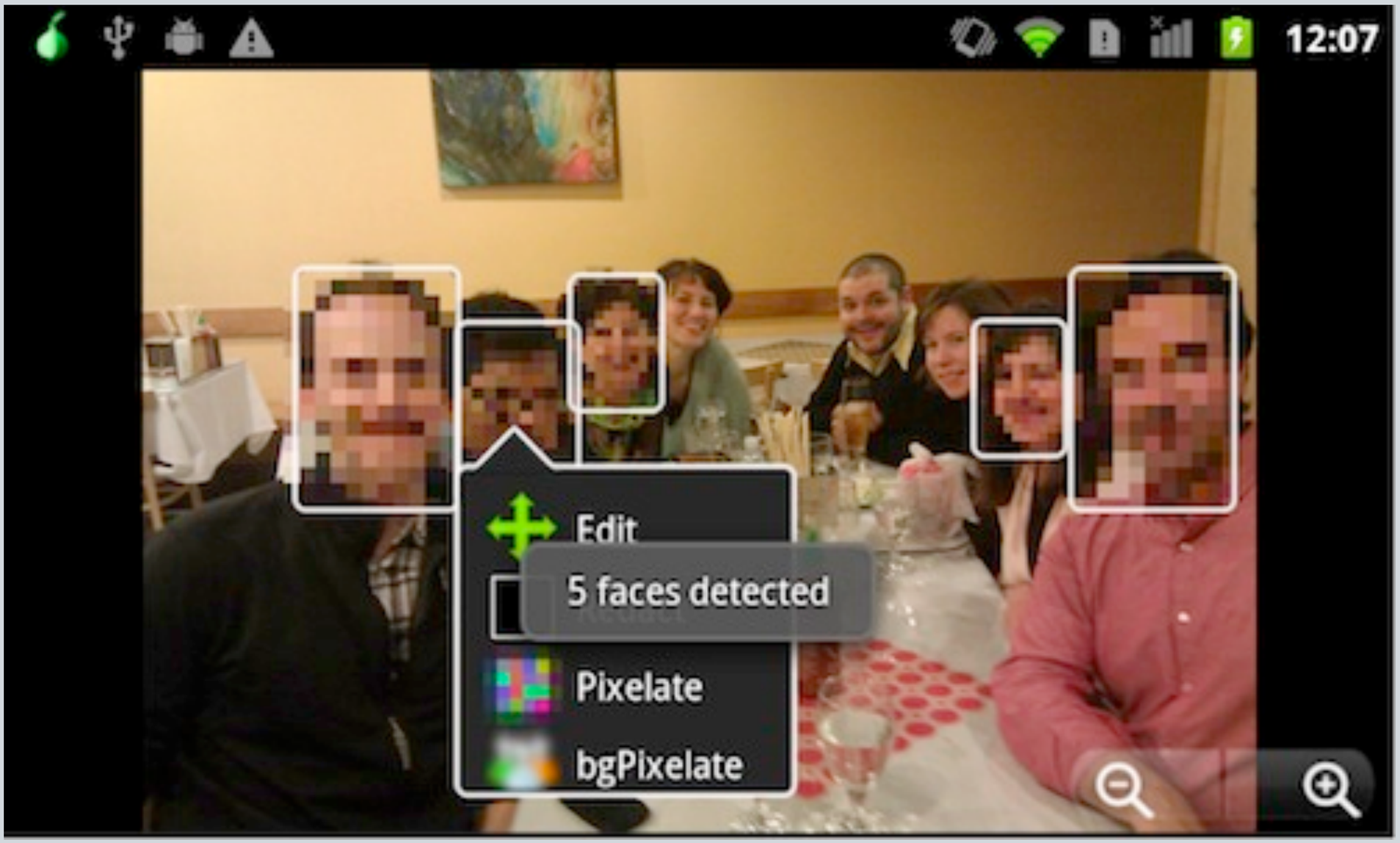


CHATSECURE

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

OBSCURACAM

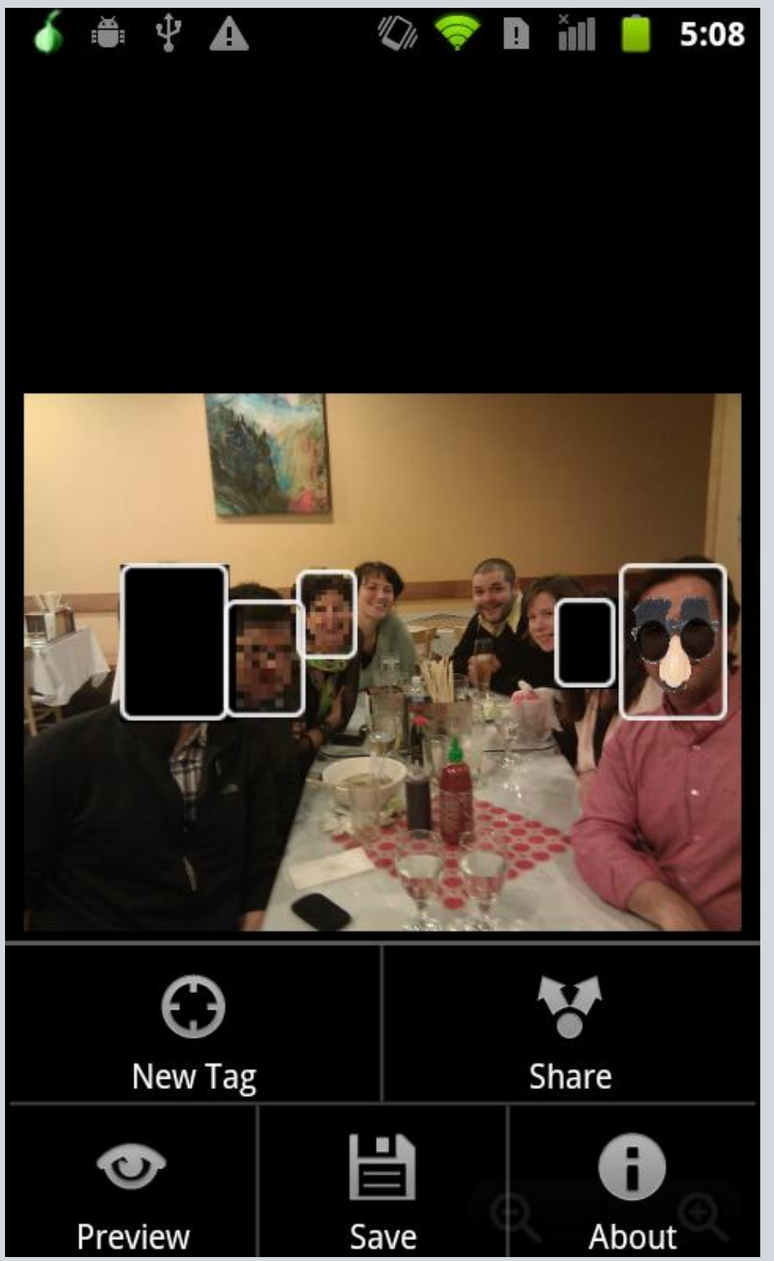


A secure camera application being developed with WITNESS, to help improve visual privacy, secure human rights media content, and innovate in software camera tools for activists.

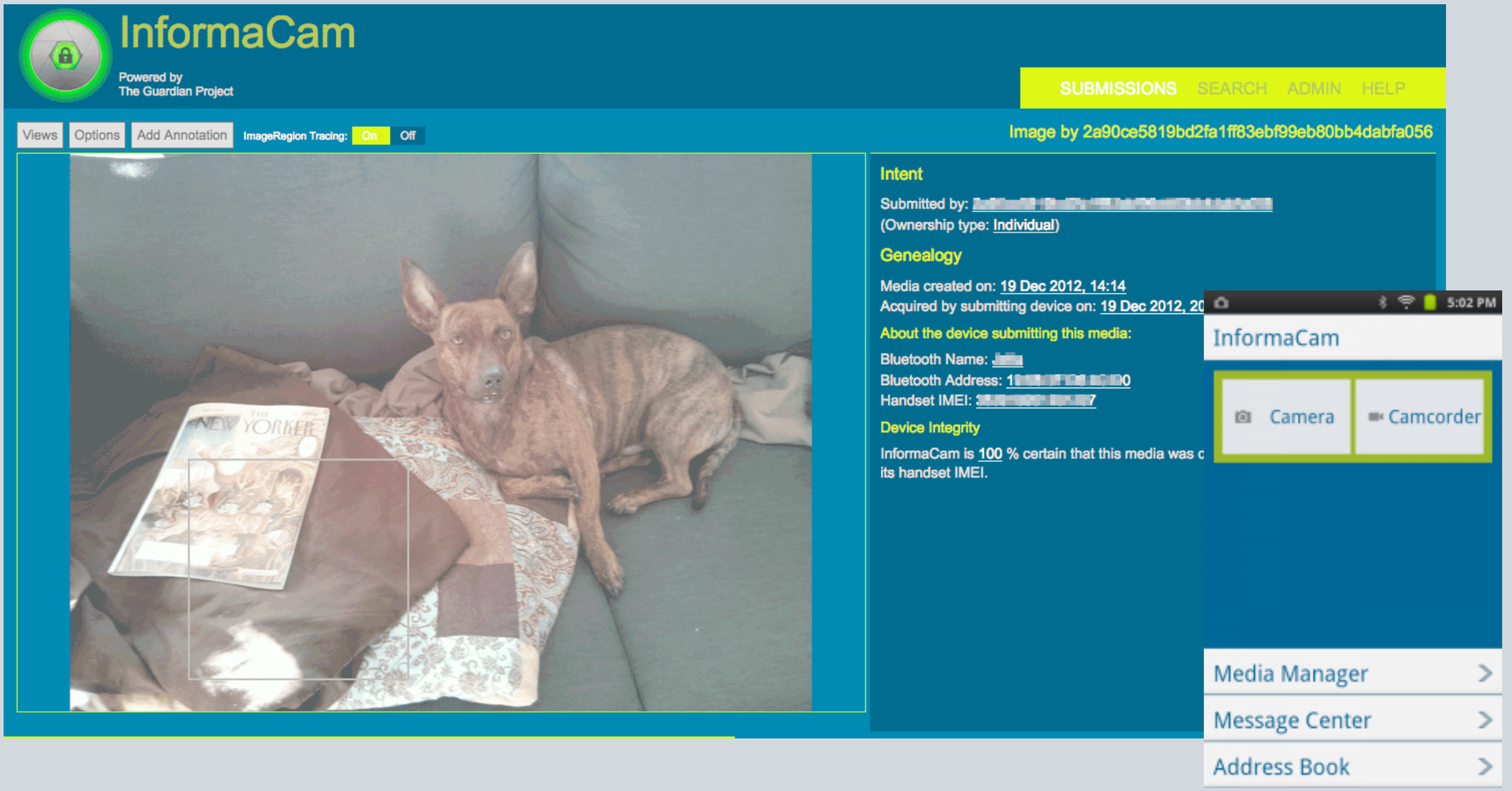
SECURE SMARTCAM

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



INFORMACAM

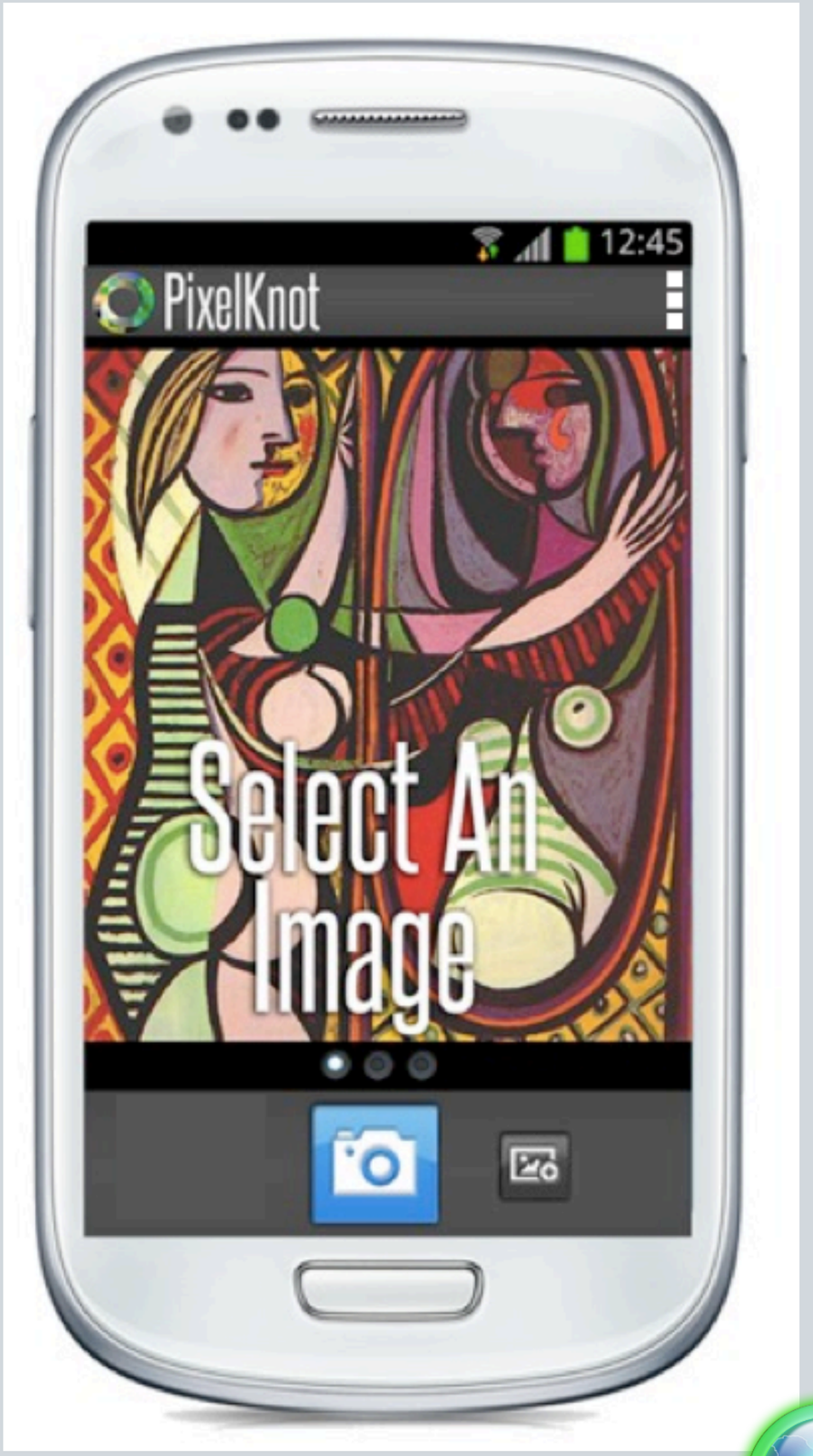


A secure camera application being developed with WITNESS, to help improve visual privacy, secure human rights media content, and innovate in software camera tools for activists.

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.

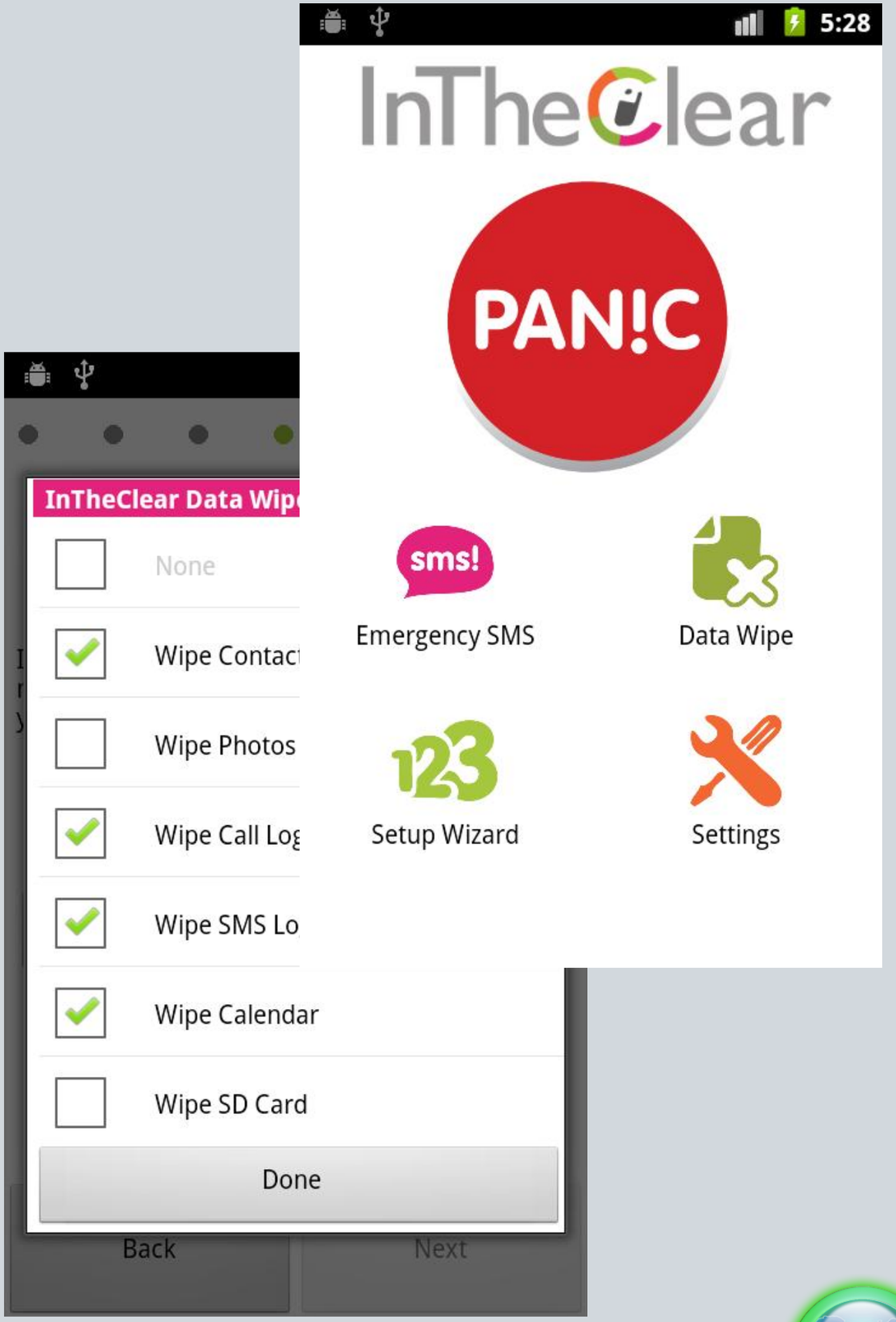
- Secure & Encrypted messages
- F5 Steganography algorithm



IN THE CLEAR

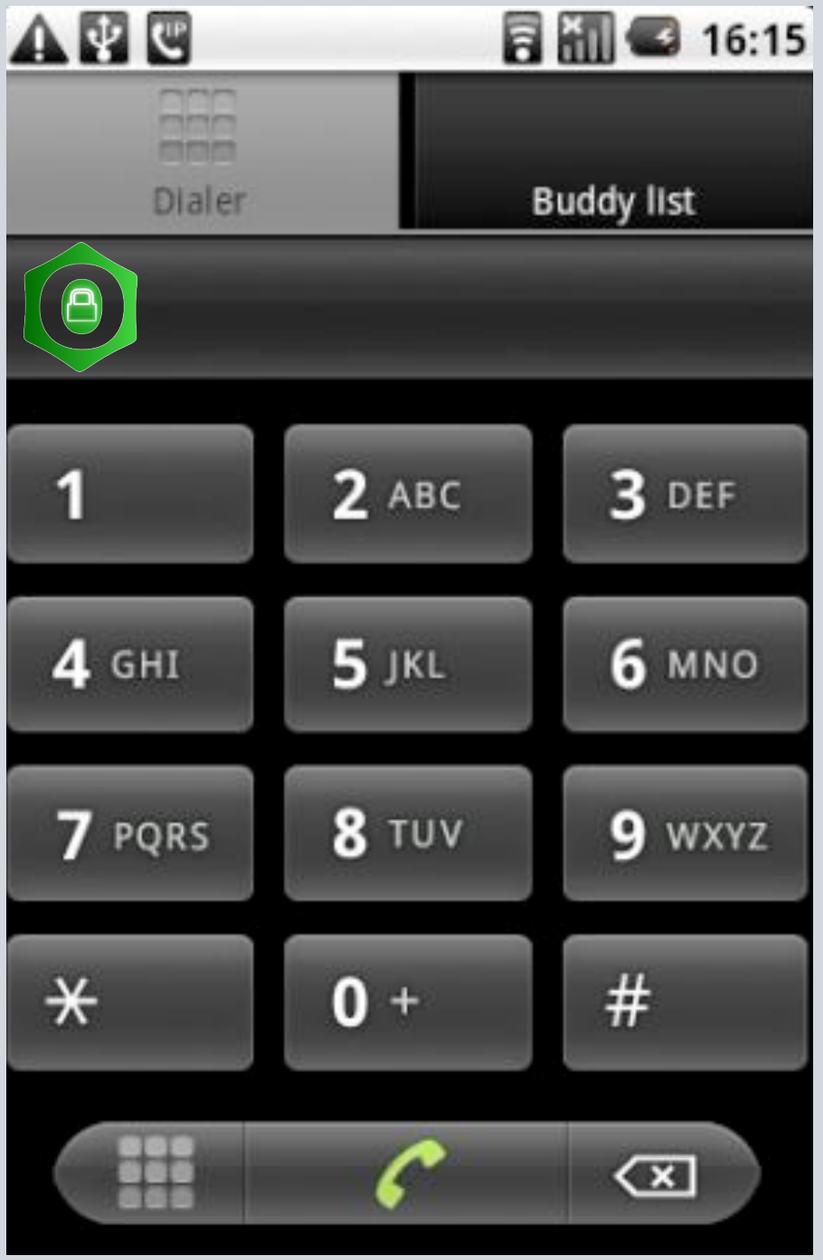
A "poison pill" app data wipe and emergency SMS distress beacon.

- 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



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

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

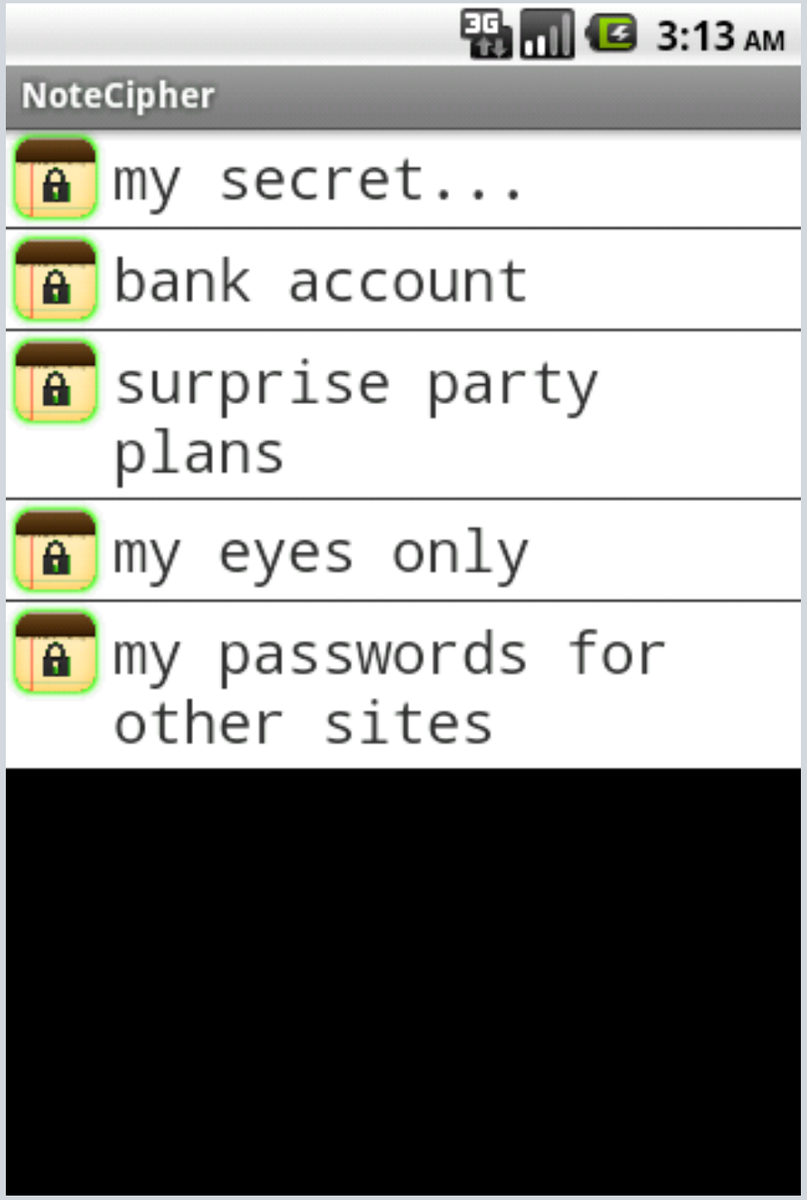
Transparent encrypted virtual disks for Android. This allows Android app developers to use the familiar and well documented android.database.* API to build in encrypted storage into their apps

- 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

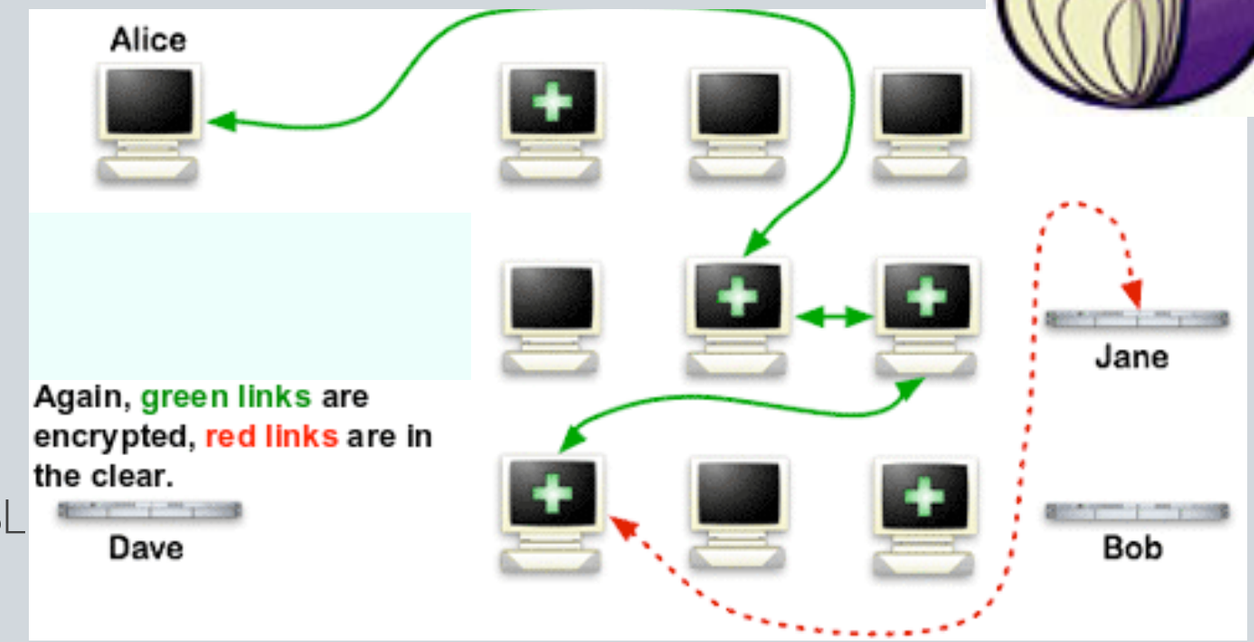
SQLCipher is an SQLite extension that provides encryption of per-app database files.

- 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

THE GUARDIAN PROJECT

WWW.GUARDIANPROJECT.INFO

INFO@GUARDIANPROJECT.INFO