

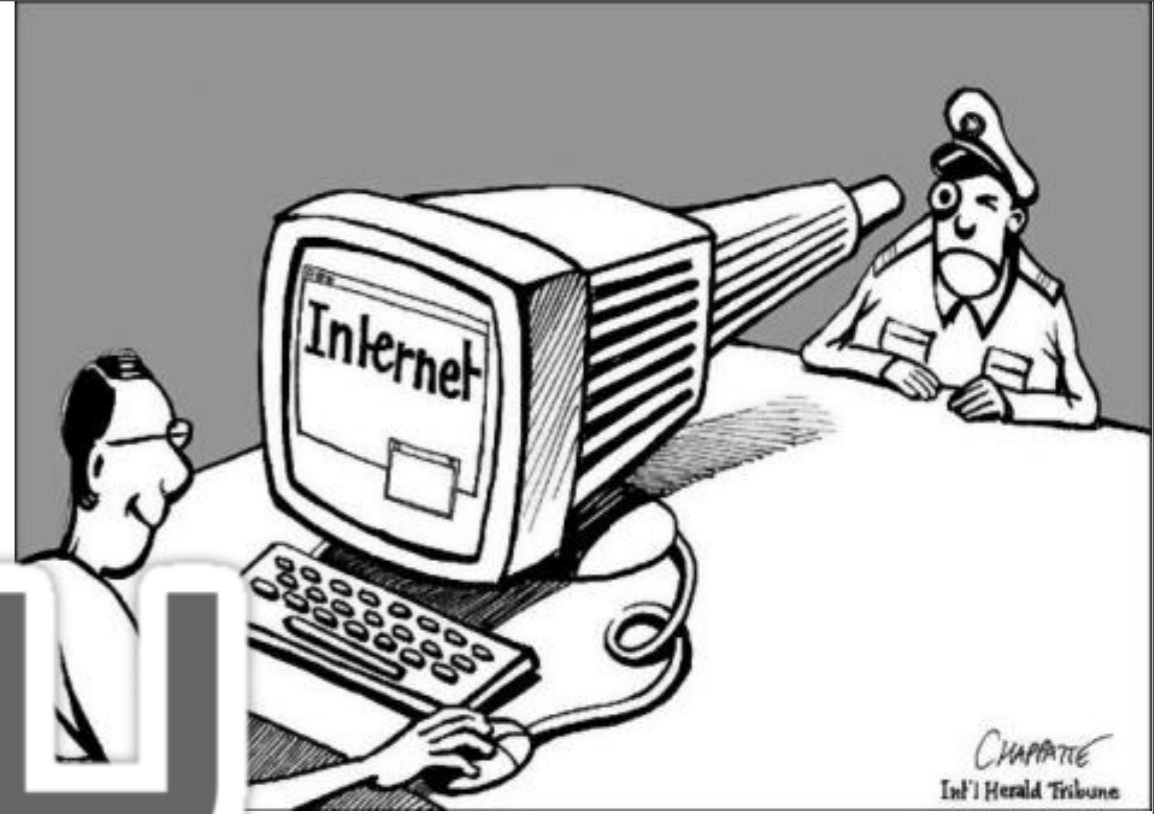
Building the private, secure,  
and unblockable app store



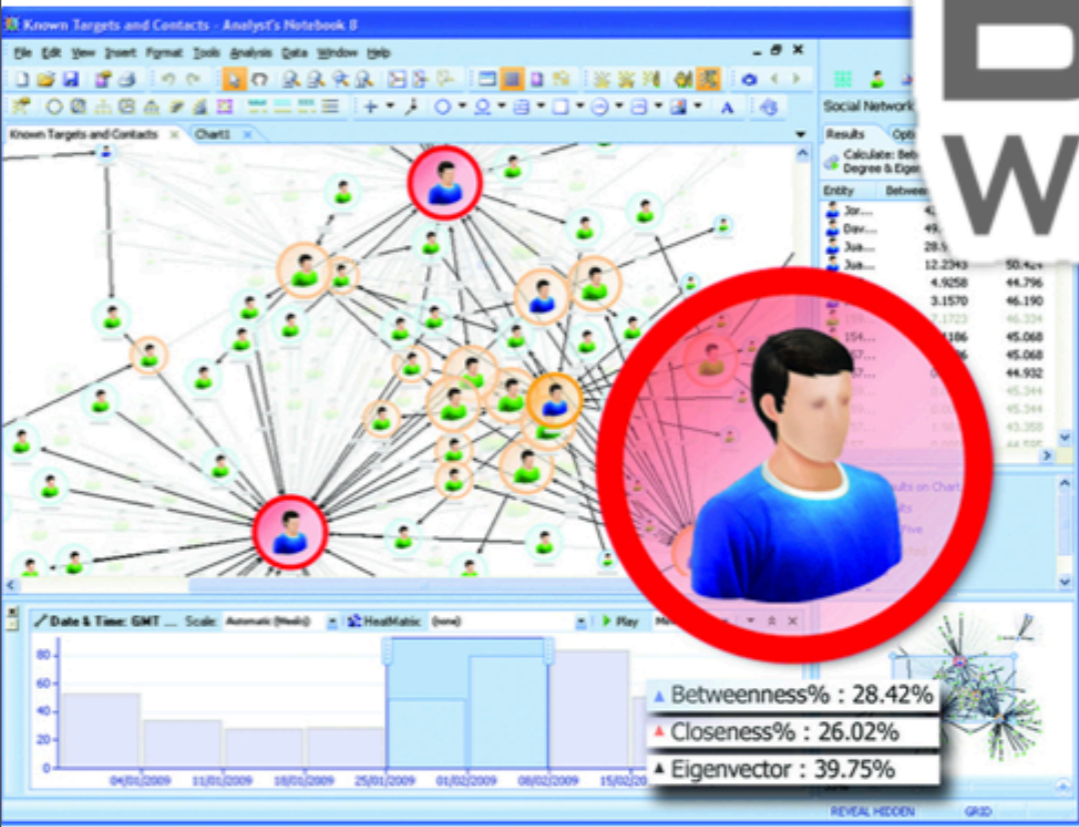
GUARDIAN  
PROJECT  
<https://guardianproject.info>

free software swat team for privacy

people behave differently  
when being watched



YOU  
ARE  
BEING  
WATCHED



Who is listening to what?



we put privacy first

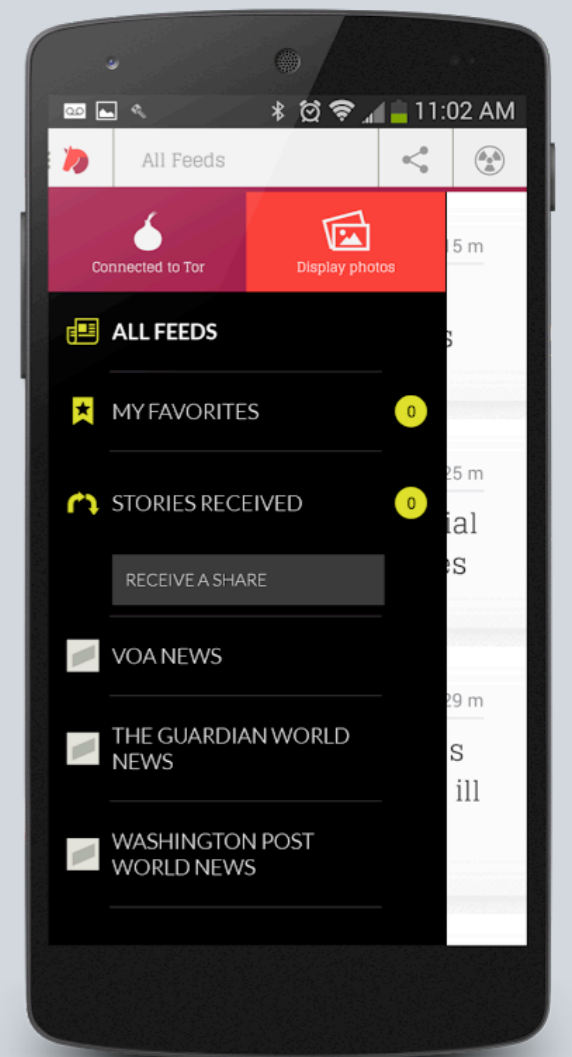
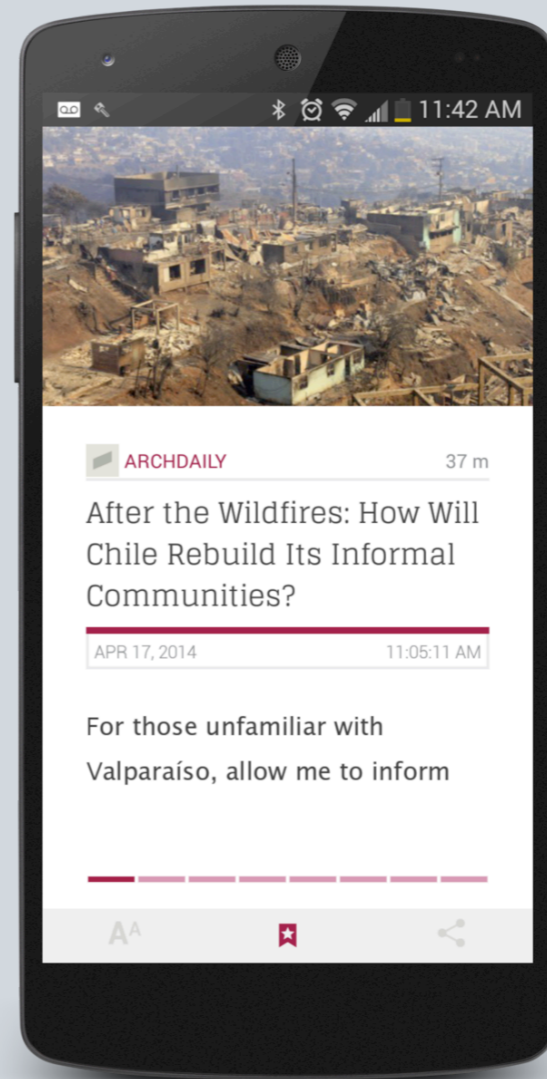
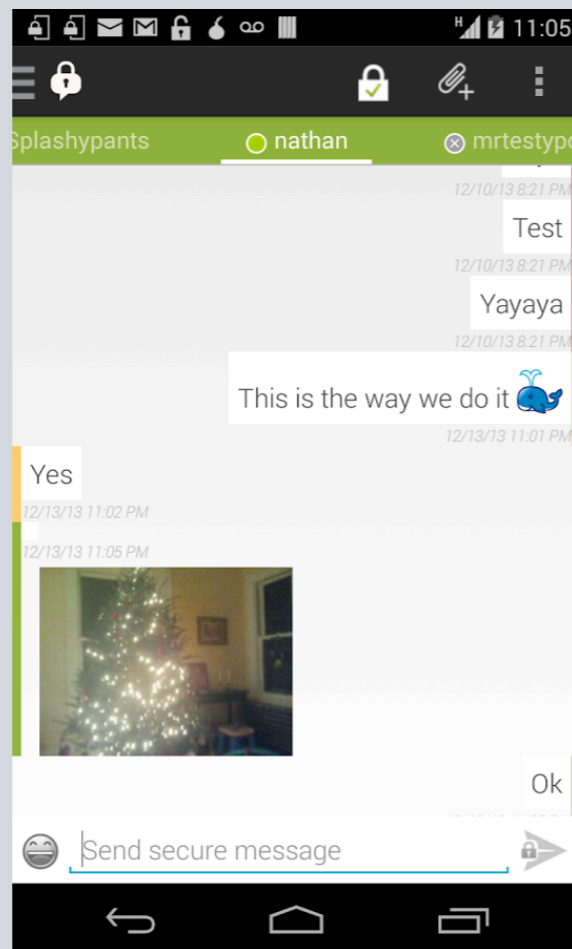
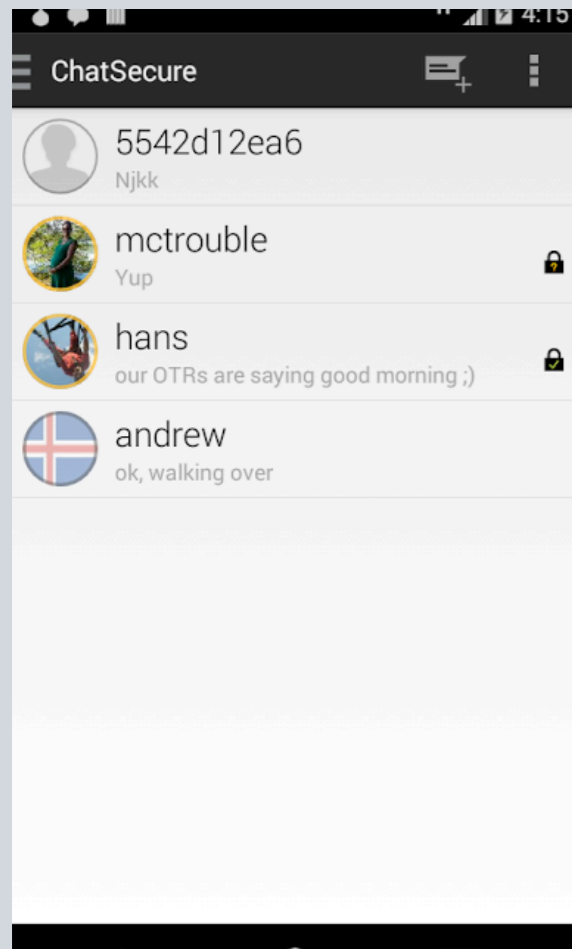


# privacy through user experience



\* we get paid to address high risk use cases, and spin out tools and knowledge to raise the bar for all

# modern design with privacy is possible



- apps with transparent Tor support
- \* encrypted local storage
- \* hardened network encryption
- \* end-to-end encrypted messaging

# 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.

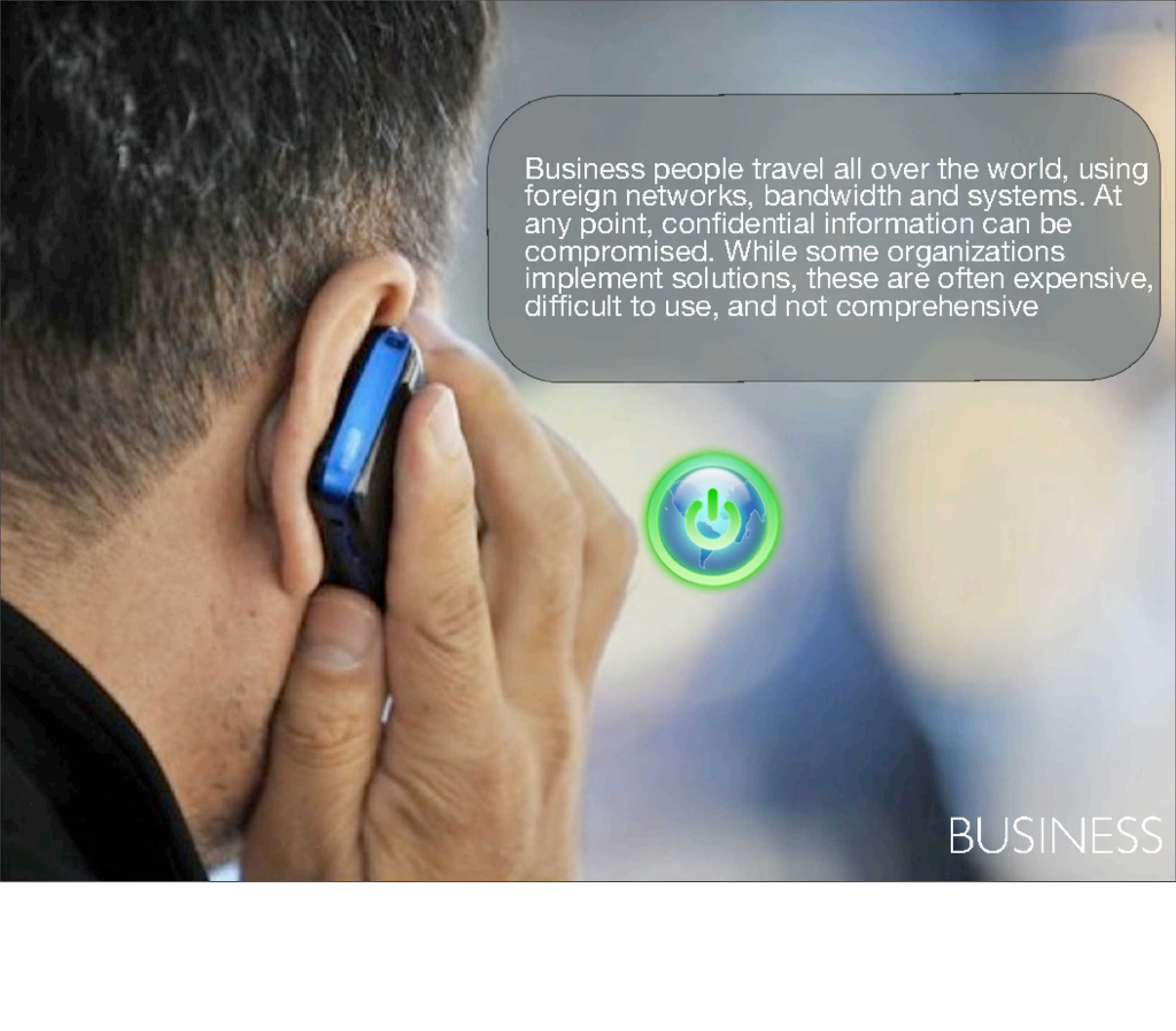




Reporters in the field can use Guardian apps to stay in touch with their safety networks, while safeguarding information on contacts, story notes and captured digital media, enabling a new, secure "reporter's notepad". In addition, high-resolution cameras of new Android hardware meet the quality standards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



FRONTLINE REPORTERS



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

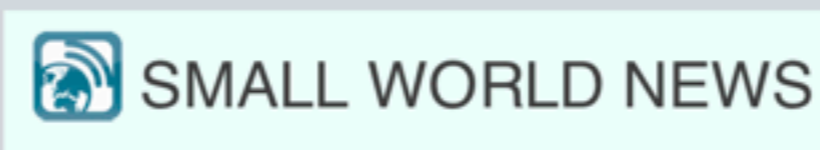


BUSINESS

# 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.





# 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.





F-Droid

an community run Android app store  
that distributes verified Free Software

inspired by



**debian**  
GNU/Linux

on the forefront of security  
community run

# F-Droid has solid security

- only HTTPS connections
- pinned TLS certificate
- signed metadata (e.g. Debian apt model)
- offline signing machines
- Android APK signatures secure updates

trust requires difficult decisions





make computers verify  
to make trust decisions easier

# what most app stores know

- your login/account
- everything you search for in the app store
- everything you look at in the app store
- everything you download, install, uninstall
- which apps you launch and use
- where you are
- your preferred language
- and more...

What must app stores know?

how to give you  
the files you request

# how to give you the files you request

- app indexes
- app descriptions and icons
- the app itself
- the client does the rest

no logins, user names, analytics  
solid transport security  
Tor and other proxy support

# most app stores have terrible security



there are many around the world  
do not even use HTTPS  
FBI vs. Apple  
companies are fighting hard so they don't need to comply

# prevents targeted attacks



when users cannot be targeted, malware is visible to all  
public auditing then becomes feasible

garbage in means garbage out

if your app includes malware, your reputation will be destroyed  
devs do not have good security practice  
Google recommendations are bad (signing key on regular dev machine)  
XCodeGhost



# reproducible builds!



large scale exploits like XCodeGhost

# now it is secure

- targeted attacks very difficult, even if f-droid.org fully collaborates
- anyone can verify the builds using F-Droid verification server or other methods
- software publicly audited by Cure53
- you do not need to use f-droid.org

public auditing then becomes feasible  
research project on the future of infrastructure that you can use

# chain of trust from source code to your phone

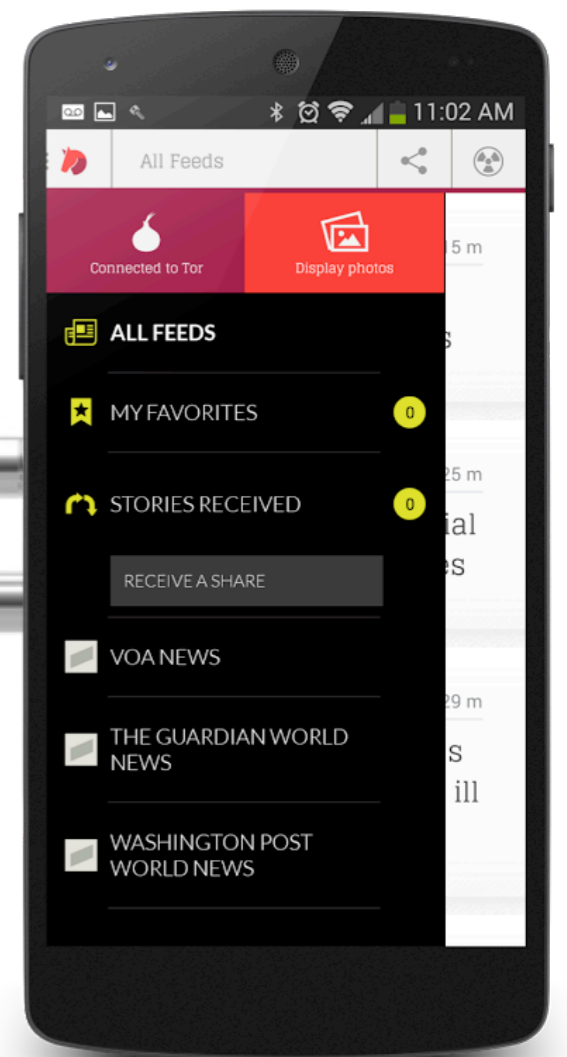
```
public class AlarmUpdater extends Activity {
    private Notification createNotification(PendingIntent intent, int minutes, int seconds, boo
    // Set the icon, scrolling text and timestamp
    NotificationCompat.Builder builder = new NotificationCompat.Builder(this);

    // Set notification text labels
    builder.setContentTitle(getString(R.string.app_name));
    builder.setContentText(getString(R.string.countdown_complete));
    builder.setTicker(getString(R.string.elapsed_time, minutes, seconds));

    if (small) {
        builder.setSmallIcon(R.drawable.notification_icon);
    } else {
        builder.setSmallIcon(R.drawable.icon);
    }

    builder.setContentIntent(intent);
    return builder.build();
}

public static class UpdateService extends Service {
    @Override
    public int onStartCommand(Intent intent, int flags, int startId) {
        notifyStatusBar();
        stopSelf();
        return START_NOT_STICKY;
    }
}
```



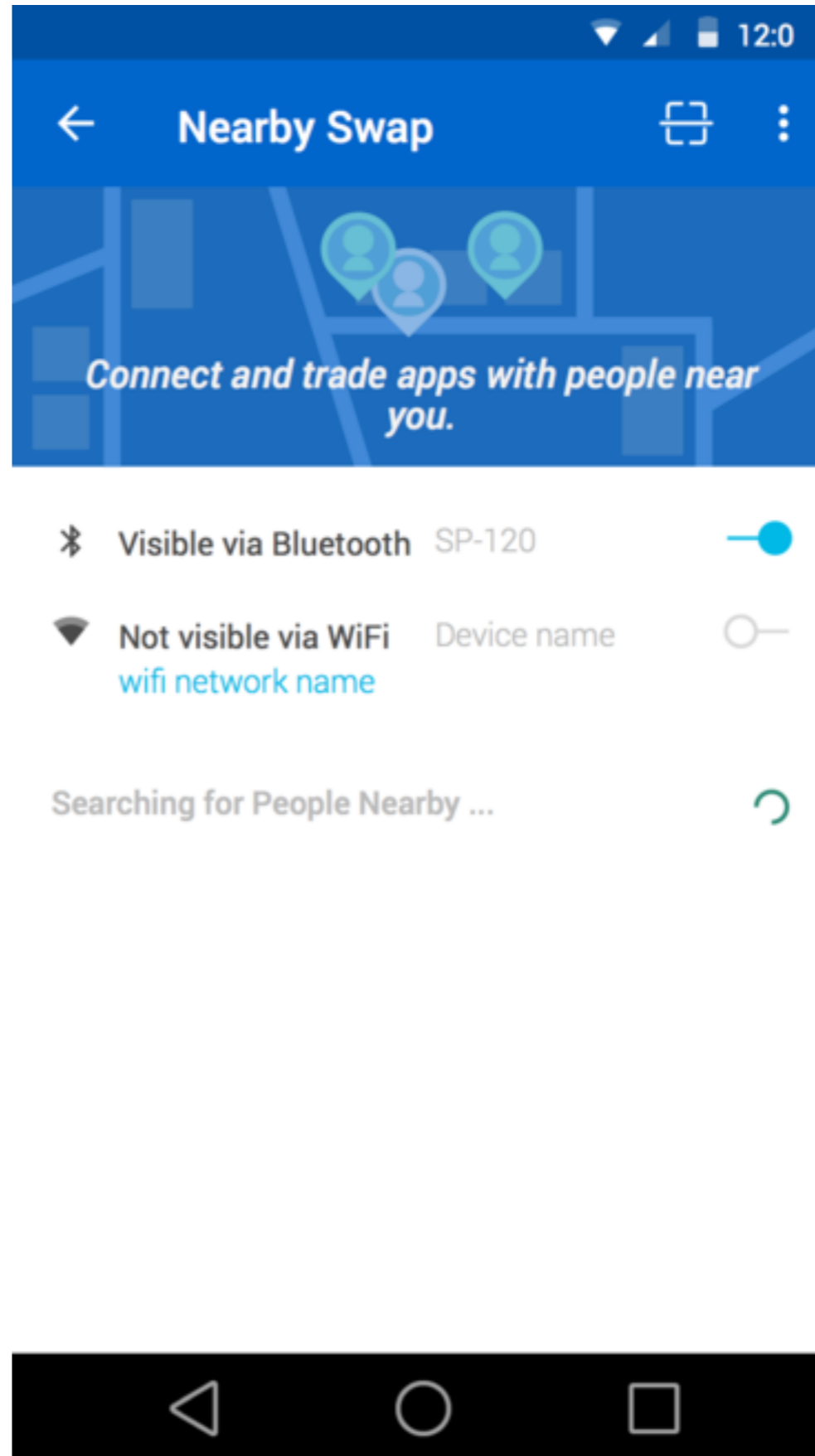
now you only have to trust the original author

getting apps, no matter what



Tor  
auto-mirror failover  
swap

swap apps:



Tor  
auto-mirror failover  
swap

# coming soon!

- all prototyped, now we are polishing it up
- media handling (audio, video, e-books, etc.)
- “collateral freedom” support (github, S3)
- app store “curation” tools

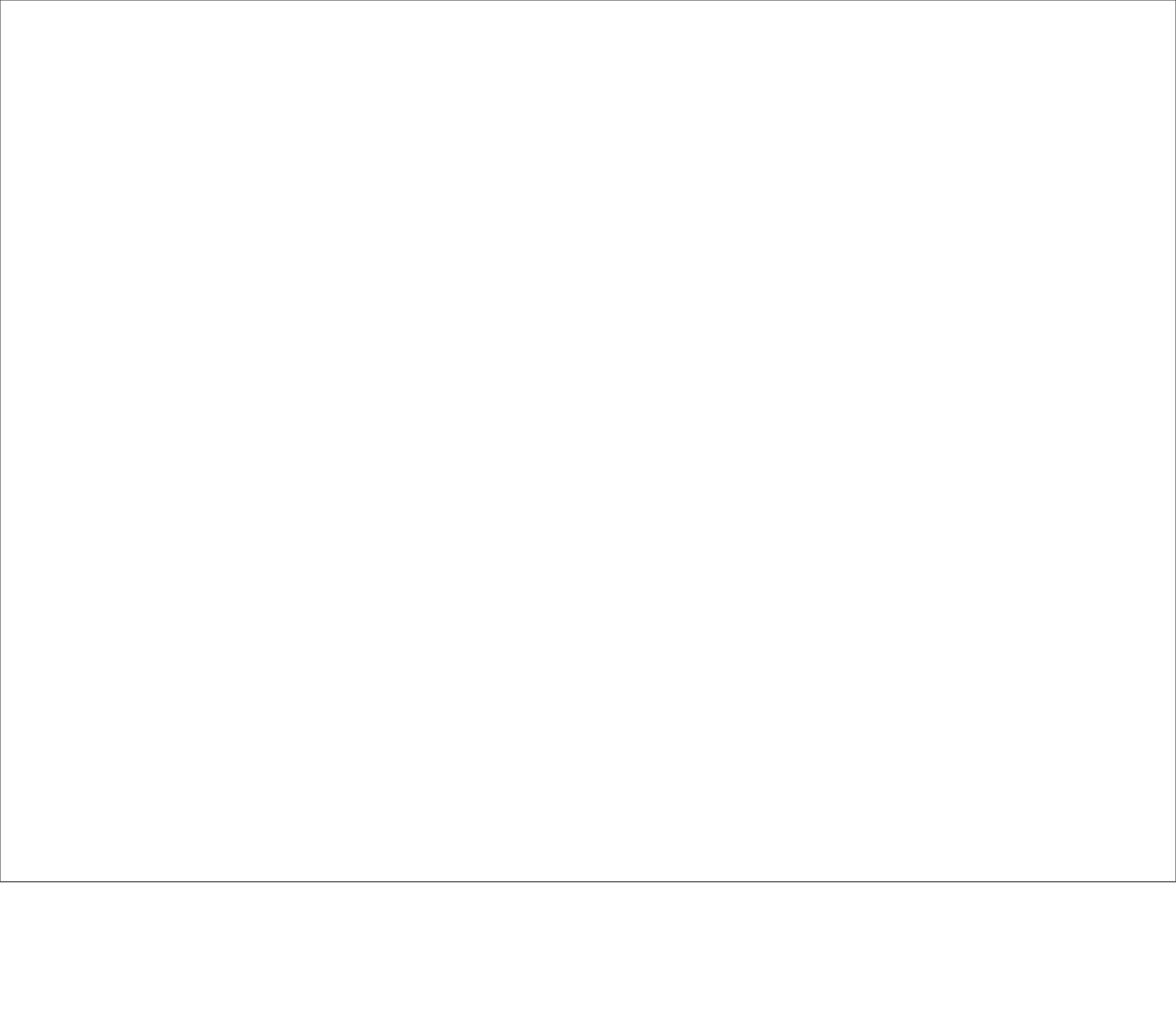


GUARDIAN  
PROJECT  
<https://guardianproject.info>

Hans-Christoph Steiner

[hans@guardianproject.info](mailto:hans@guardianproject.info)





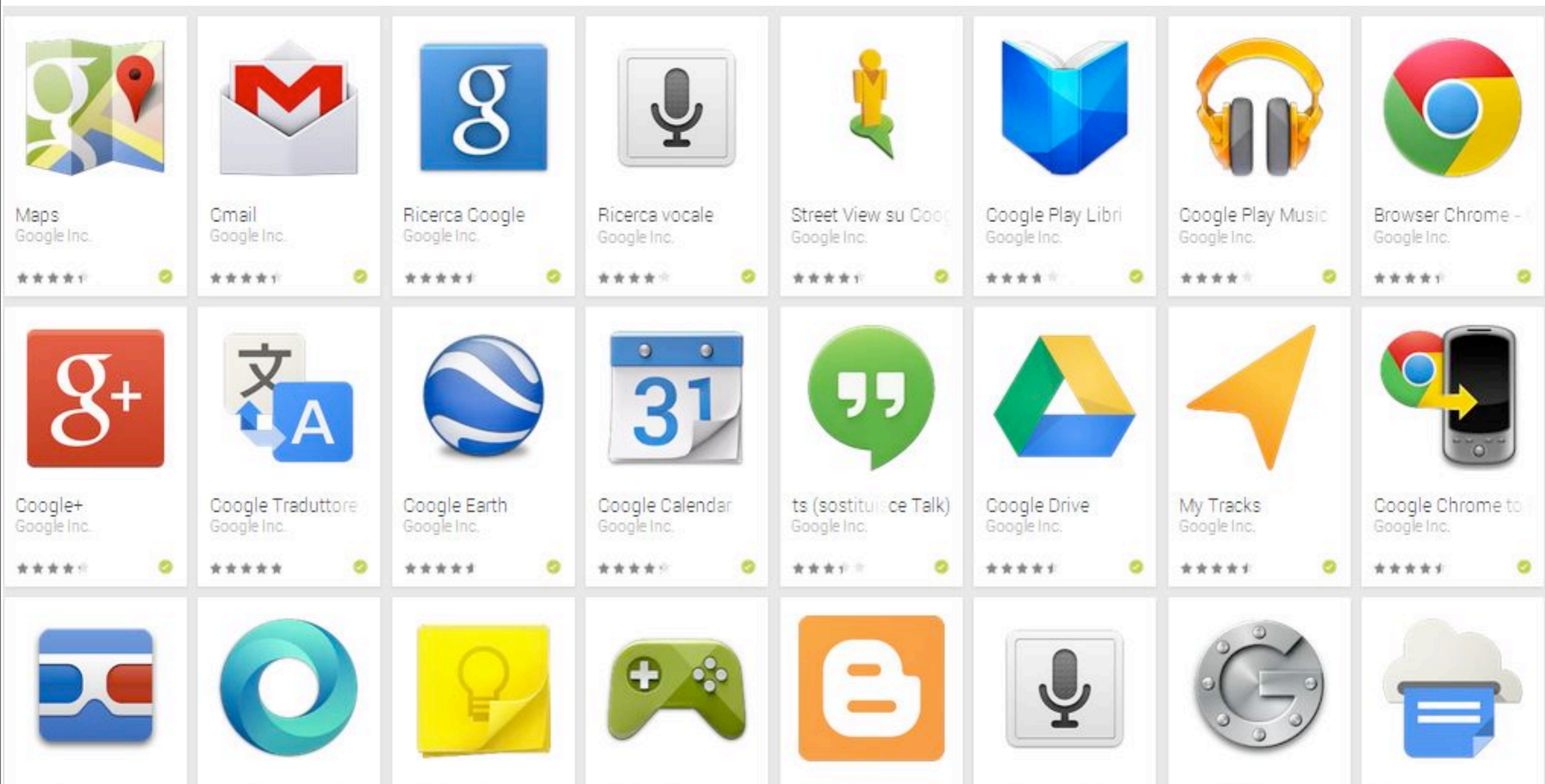
# F-Droid can help you

- resist malware that targets developers, for apps that you distribute in any app store
- avoid large scale exploits like XCodeGhost
- secure your app release builds
- distribute your apps privately

the developer tools improve security no matter which app store you distribute with

# make your own app store!

اپزارد 



make your own app store!

- ▶ regional app stores like CafeBazaar, Baidu
- ▶ custom enterprise solutions

funded by

