## **EDUCATIC**

Las ventajas de usar F-Droid frente a Google Play: un par de Apps imprescindibles para la privacidad

Luis Fajardo

17:30 - 17:55



## **EDUCATIC**

Las ventajas de usar F-Droid frente a Google Play: un par de Apps imprescindibles para la privacidad

Luis Fajardo

17:30 - 17:55 Vigo, 25 de junio de 2022 - esLibre 2022





## ¿De qué vamos a hablar?

- 1. Por qué liberar el móvil
- 2. Opciones existentes
- 3. La alternativa fácil: F-Droid
- 4. Ejemplo: usando Conversations
- 5. Apps recomendadas para privacidad
- 6. Conclusiones



#### F-Droid frente a Google Play: Apps imprescindibles para la privacidad.

Luis Fajardo López - @lfajardo@txs.es



Un informe demuestra la obtención de datos personales masivamente en Android https://www.scss.tcd.ie/doug.leith/privacyofdialerandsmsapps.pdf La AEPD se propone intervenir ado de la UC3M se deduce, según informa la ... ☑ ☆ Tamaño automático \$

#### An Analysis of Pre-installed Android Software

Julien Gamba $^{*\dagger}$ , Mohammed Rashed $^{\dagger}$ , Abbas Razaghpanah $^{\ddagger}$ , Juan Tapiador  $^{\dagger}$  and Narseo Vallina-Rodriguez $^{*\S}$ \* IMDEA Networks Institute, † Universidad Carlos III de Madrid, ‡ Stony Brook University, § ICSI

#### Abstract

The open-source nature of the Android OS makes it possible for manufacturers to ship custom versions of the OS along with a set of pre-installed apps, often for product differentiation. Some device vendors have recently come under scrutiny for potentially invasive private data collection practices and other potentially harmful or unwanted behavior of the preinstalled apps on their devices. Yet, the landscape of preinstalled software in Android has largely remained unexplored, particularly in terms of the security and privacy implications of such customizations. In this paper, we present the first largescale study of pre-installed software on Android devices from more than 200 vendors. Our work relies on a large dataset of real-world Android firmware acquired worldwide using crowd-sourcing methods. This allows us to answer questions related to the stakeholders involved in the supply chain, from device manufacturers and mobile network operators to thirdparty organizations like advertising and tracking services, and social network platforms. Our study allows us to also uncover relationships between these actors, which seem to revolve primarily around advertising and data-driven services. Overall,

end up packaged together in the firmware of a device is not transparent, and various isolated cases reported over the last few years suggest that it lacks end-to-end control mechanisms to guarantee that shlpped firmware is free from vulnerabilities [24], [25] or potentially malicious and unwanted apps. For example, at Black Hat USA 2017, Johnson et al. [82], [47] gave details of a powerful backdoor present in the firmware of several models of Android smartphones, including the popular BLU R1 HD. In response to this disclosure, Amazon removed Blu products from their Prime Exclusive line-up [2]. pinpointed as responsible for this incident. The same report also discussed the case of how vulnerable core system services (e.g., the widely deployed MTKLogger component developed by the chipset manufacturer MediaTek) could be abused by co-located apps. The infamous Triada trojan has also been recently found embedded in the firmware of several low-cost Android smartphones [77], [66]. Other cases of malware found (ransomware), which were spotted in the firmware of various high-end phones [6].

#### What Data Do The Google Dialer and Messages Apps On Android Send to Google?

Tamaño automático 💠

Douglas J. Leith Trinity College Dublin, Ireland 28th Feb 2022

bstract-We report on measurements of the data sent to Google y the Google Messages and Google Dialer apps on an Android andset. We find that these apps tell Google when message/phone alls are made/received. The data sent by Google Messages ncludes a hash of the message text, allowing linking of sender A company named Shanghai Adups Technology Co. Ltd. was ind receiver in a message exchange. The data sent by Google Dialer includes the call time and duration, again allowing linking of the two handsets engaged in a phone call. Phone numbers are also sent to Google. In addition, the timing and duration of other iser interactions with the apps are sent to Google. There is no opt out from this data collection. The data is sent via two channels, (i) the Google Play Services Clearcut logger and (ii) Google/Firebase Analytics. This study is therefore one of the first to cast light on the actual telemetry data sent by Google Play Services, which pre-installed include Loki (spyware and adware) and Slocker to date has largely been opaque. We informed Google of our findings and delayed publication for several months to engage with them. On foot of this report Google say that they plan to make multiple changes to their Messages and Dialer apps.

2) When a phone call is made/received the Google Dialer app similarly logs this event to Google servers together with the time and the call duration.

... ♥ ☆

aidad no es

→ III/

EDUCATIC

This data is sufficient to allow discovery of whether a pair of handsets are communicating.

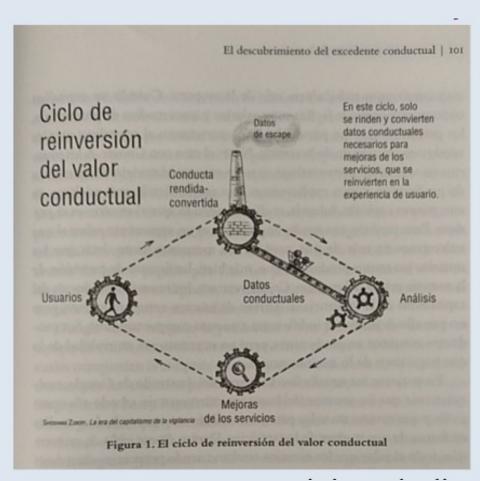
The data sent to Google is tagged with the handset Android ID, which is linked to the handset's Google user account and so often to the real identity of the person involved in a phone call or SMS message. For example, a working phone number is required to create a Google account, and if the person has paid for an app on the Google Play store or uses Google Pay then their Google account is also linked to their credit card/bank details. In this way real-world identities of the pair of people communicating may be revealed to Google.

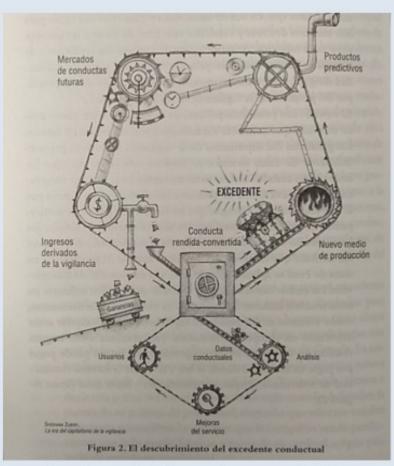
#### F-Droid frente a Google Play: Apps imprescindibles para la privacidad.

Luis Fajardo López - @lfajardo@txs.es

# EDUCATIC esLibre os explican)

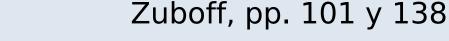
## 1.2.- La realidad (...y los expertos explican)





El descubrimiento del excedente conductual

El capitalismo de la vigilancia comienza con el descubrimiento del excedente conductual. Se proveen más datos conductuales de los estrictamente requeridos para las mejoras del servicio. El excedente resultante alimenta la inteligencia de máquinas —el nuevo medio de producción—, que fabrica predicciones de la conducta del usuario. Estos productos se venden a clientes comerciales en unos nuevos mercados de futuros conductuales. El ciclo de reinversión del valor conductual queda supeditado así a esta nueva lógica.





# EDUCATIC esLibre

# 1.3.- Conclusión: porqué liberar el móvil

- 1. La realidad (que todos sospechamos)...
- ...y los expertos llaman capitalismo de la vigilancia
  - Programas "espías" → https://encanarias.info/posts/12078 (UC3M)
  - Android monitoriza → https://txs.es/@lfajardo/108174818388167644 (TCD.ie)
  - Nadie vela por el cumplimiento normativo → i 5G!
  - **Polarización:** Valores sociales vs. necesidades de "la red" Shoshana Zuboff, Surveillance capitalism. RODRÍGUEZ ÁLVAREZ y FAJARDO, "La defensa de las libertades ante el tratamiento masivo de datos" [vídeo]
- 2. Actuaciones: construcción social:
  - ¿Autoprotección?
  - ¿Eludir plataformas del capitalismo de la vigilancia?
  - ¿Ejemplarizar?
  - Cuestión colectiva: tan fuerte como el eslabón más débil





## 1.4.- Porqué liberar el móvil ¿la ley?

# ¿Dejamos que lo arregle la Ley?

- **RGPD** → ha servido de poco (ejemplos anteriores)
- Próximas normas europeas →
  - "Ley" sobre la Inteligencia Artificial entre valores democráticos y la competitividad global
  - "Ley" de Mercados Digitales: evita programas preinstalados interoperabilidad activa
  - "Ley" de Servicios Digitales: control a contenidos ilícitos y nocivos ¿retirada? ¿cómo? garantías en comercio electrónico





# 2.- Opciones existentes

- 1. Sistemas operativos libres (escasos)
- 2. Android sin Google (Flashear LineageOS o aprovisionar https://h-mdm.com/ -control parental-)
- 3. Usar software libre (bloquear el que viene por defecto)
  - Desde el repositorio seguro F-Droid:
  - Distinción Repos / App:
    - F-Droid.Org

Repos: https://forum.f-droid.org/t/known-repositories/

- G-Droid (https://gitlab.com/gdroid/gdroidclient/)
- Amazon AppStore
- Aptoide
- Aurora Store



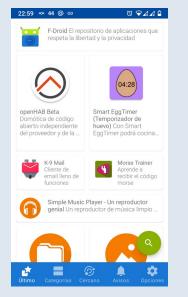


### 3.- La alternativa fácil: F-Droid



- ¿Qué es F-Droid?
- F-Droid es un catálogo instalable de aplicaciones de software libre (FOSS, «Free and Open Source Software») para Android. El cliente facilita la navegación, la instalación y el seguimiento de las actualizaciones en tu dispositivo.

**DESCARGAR F-DROID** Firma PGP





3. Actualizar repositorio (lista)







4.- (opcional) Añadir repo de CollaboraOffice

1. Descargar la App de https://F-Droid.Org

2. Instalarla (autorizar lo que haga falta, no

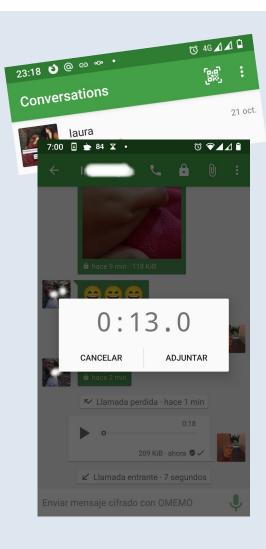
aceptar optimizaciones de batería ni red)

#### F-Droid frente a Google Play: Apps imprescindibles para la privacidad.

EDUCATIC esLibre

Luis Fajardo López - @lfajardo@txs.es

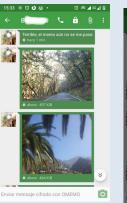
## 4.- Ejemplo: usando Conversations



- Instalar Conversations. Abrirlo.
  No aceptar optimizaciones de batería / red (en PC, Gajim – en iOS, Siskin)
- 2. Crear cuenta de usuario (web / App)
- 3. Añadir contactos / grupos
- 4. Activar cifrado (OMEMO / GPG)

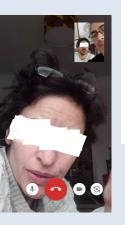


















## 5.- Apps recomendadas para privacidad



K-9 Mail + OpenKeychain → PEP correo.txs.es docs.txs.es









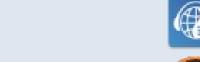


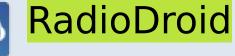






DAVx5 Collabora Office(\*)















FFUpdater (Chromium / Firefox Klar)









Fedilab: txs.es / encanarias.info / tuvideo.encanarias.info







UntrackMe 🚺 Twidere 💍 SkyTube 🧔 SpotiFly









## Conclusiones

### 1. ii Disfruta de tu software y tu privacidad !!

## 2. ¿Cómo elegir software? (propuesta para debate)

- 1) Ser libre facilita pero no garantiza la privacidad
- 2) Gratis ¿datos, colectivo, o servicio freemium?
- 3) Asegurar el futuro: estándares, federable: libre.

### 3. Valoración final:

- 1) La privacidad es un valor colectivo
- 2) Contribuir a la privacidad de todos es fácil y posible
- 3) La ley podrá ayudar (y vienen buenos tiempos (?)), pero es insuficiente





# Créditos y agradecimientos

#### ii Gracias!!

mailto: lfajardo@txs.es | https://txs.es/@lfajardo

#### Citas:

FAJARDO, Un informe demuestra la obtención de datos personales masivamente en Android, https://encanarias.info/posts/12078

VV.AA., An Analysis of Pre-installed Android Software, UC3M, 2019

CLABURN, Android's Messages, Dialer apps quietly sent text, call info to Google, The Register, 21/3/22 LEITH, What Data Do The Google Dialer and MessagesApps On Android Send to Google?, Trinity College Dublin, marzo 2022

RODRÍGUEZ ÁLVAREZ, J.L., y FAJARDO LÓPEZ, L., "

La defensa de libertadesante la vigilancia y tratamiento masivo de datos", XII Congreso Nacional de la Abogacia 2019, CGAE.

FAJARDO LÓPEZ, L., "¿Hacia un feudalismo de los datos?¿Derecho otecnología?", Congreso esLibre 2020, Universidad Rey Juan Carlos

ZUBOFF, La era del capitalismo de la vigilancia

#### Cita:

FAJARDO, Luis, Ventajas de usar F-Droid: un par de Apps imprescindibles para la privacidad, esLibre, junio 2022, https://docs.txs.es/s/mGN8w4H5bGigPRr



# EDUCATIC esLibre ropia imagen

## Licencia, protección de datos y propia imagen

Esta obra está bajo una licencia Creative Commons Atribución 3.0



Prohibida su distribución en redes sociales "chupadatos" (que su modelo de negocio sea la captación de datos) donde sin embargo sí se podrá distribuir un enlace.

-RS+E

Más info: https://encanarias.info/posts/35500

