

# Android Privacy

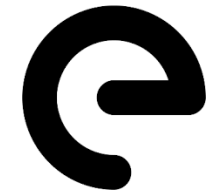
CorkSec, 2019-11-12

Johannes Ahlmann

microG



FossDroid



/e/ foundation

 **Purism**



GrapheneOS

# Why the long Face?

## *Google Misled Consumers Over Location Tracking, Australia Says*

The company did not disclose the need to disable two different Android settings to stop data collection, regulators said in a lawsuit.

## **CYBER SNOOPER Google SPYING on your real-world movements even if you have Location History turned off**

The tech giant has been exposed for mapping the movements of users who have Location History turned off

REVEALED

[Sean Keach](#)

13 Aug 2018, 16:55 | Updated: 14 Aug 2018, 17:18

## Nokia phones caught mysteriously sending data to Chinese servers



Chris Smith [@chris\\_writes](#)

March 21st, 2019 at 5:33 PM

Share

Tweet

[Never Settle] OnePlus found to be collecting personally identifiable analytics data from phone owners



Corbin Davenport

Oct 10, 2017

222



SECURITY

## Google knows where you live, work and your 'secret interests', new 'Shadow Profile' report says

John Rolfe, News Corp Australia Network

March 13, 2019 9:42am



## Google Maps is rolling out 'incognito mode' for Android users that stops company from hoovering up your search and location history data

- Google is rolling out its private mode for Google Maps for Android users
- The mode will turn off collection on search history, location, and more
- Google continues to make overtures to users concerned with their privacy

By [JAMES PERO FOR DAILYMIL.COM](#)

PUBLISHED: 18:46, 1 November 2019 | UPDATED: 19:55, 1 November 2019



## Flashlight Apps

Super-Bright LED  
Flashlight

Brightest  
Flashlight Free

Tiny Flashlight  
+ LED

Flashlight

Flashlight

Brightest LED  
Flashlight

Color Flashlight

High-Powered  
Flashlight

Flashlight HD  
LED

Flashlight: LED  
Torch Light

### Permissions

retrieve running apps

modify or delete the contents of your USB  
storage

test access to protected storage

take pictures and videos

view Wi-Fi connections

read phone status and identity

receive data from Internet

control flashlight

change system display settings

modify system settings

prevent device from sleeping

view network connections

full network access

approximate location (network-based)

precise location (GPS and network-based)

disable or modify status bar

read Home settings and shortcuts

install shortcuts

uninstall shortcuts

control vibration

prevent device from sleeping

write Home settings and shortcuts

disable your screen lock

read Google service configuration

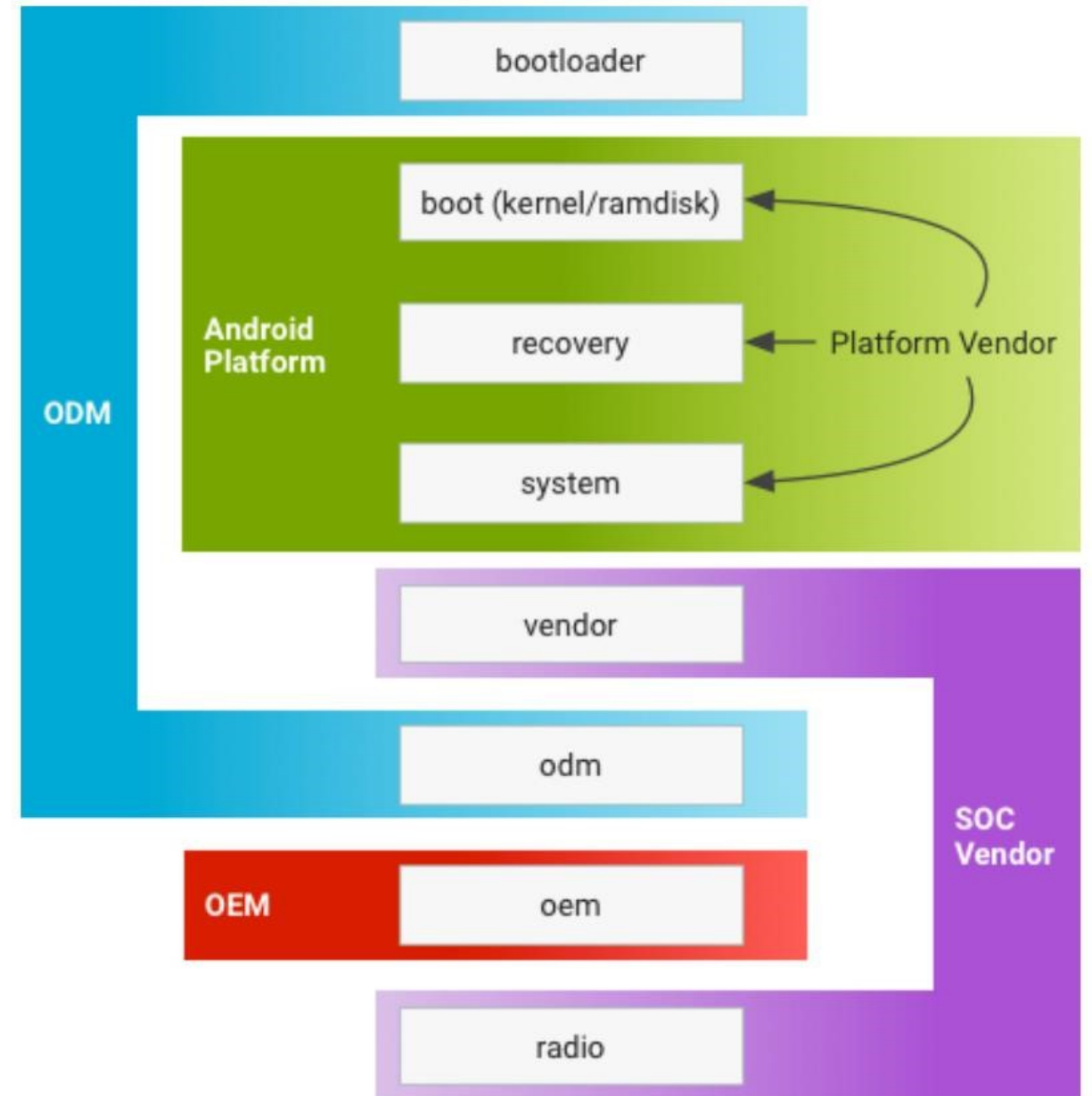
# What is Android?

For example:

- Google is the Android platform vendor
- Qualcomm is the SoC Vendor
- Samsung is the OEM/ODM

"Lots of privacy and security is tied to firmware and hardware rather than the OS running on it" - D. Micay

Wifi and cellular SoC have to be considered as their own operating systems.



# What is Android?

- GCM  
(Google Cloud Messaging)
- Google Play, Play Protect
- App Store Purchases
- FOTA  
(Firmware Over The Air)
- Binary Blobs, Drivers, Blobs



\*Android Open Source Project

<sup>1</sup> <https://www.abiresearch.com/press/4q-2014-smartphone-os-results-android-smartphone-s>

# What is the Threat Model?

Who do we want to keep our data from?

- Google, Apple
- State Actors
- Advertisers
- Remote Attackers

Physical Access

- juice jacking
- lost and found

Network-Based  
(Cellular, WiFi)

- exploits
- vendor attacks

ODM, OEM,  
AOSP

- Samsung
- Google
- Apple

Web-Based  
Remote

Cloud

- iCloud
- Google

Apps



# Security - Smartphone vs. Laptop?

## What you need to know about the newly-discovered wifi bug that lets hackers snoop on your devices

By Keith Collins • October 16, 2017

```
› Frame 1331: 633 bytes on wire (5064 bits), 633 bytes captured on interface 0
› Ethernet II, Src: SamsungE_6e:6b:20 (90:18:7c:6e:6b:20), Dst: 08:00:27:00:00:00
› Internet Protocol Version 4, Src: 192.168.100.60, Dst: 62.210.16.14
› Transmission Control Protocol, Src Port: 37140, Dst Port: 80
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
› Form item: "grant type" = "password"
› Form item: "username" = "lala@test.com"
› Form item: "password" = "secrestpassw0rd1"

0230  0a 0d 0a 67 72 61 6e 74 5f 74 79 70 65 3d 70 61 ..
0240  73 73 77 6f 72 64 26 75 73 65 72 6e 61 6d 65 3d ss
0250  6c 61 6c 61 25 34 30 74 65 73 74 2e 63 6f 6d 26 la
```

A demonstration of how KRACK could be used to steal login credentials.

## QualPwn vulnerabilities in Qualcomm chips let hackers compromise Android devices

Patches for the QualPwn vulnerabilities have been released earlier today by both Qualcomm and the Android team.



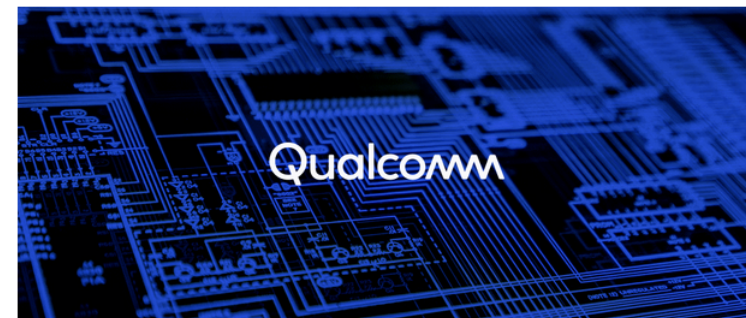
By Catalin Cimpanu for Zero Day | August 6, 2019 -- 00:11 GMT (01:11 BST) | Topic: Security

Recommended Content:

### Tools & Templates: Information security incident reporting policy

Make sure your employees know how to spot potential security breaches and how they should respond. This policy describes the signs that might point to a security incident and offers guidelines on the steps they should take. From the policy: ...

Download Now



RECOMMENDED FOR YOU

### Identity theft protection policy

Tools & Templates provided by TechRepublic Premium

Download Now

MORE FROM CATALIN CIMPANU



Microsoft  
Microsoft to apply California's privacy law for all US users




Tech Industry  
Study of over 11,000 online stores finds 'dark patterns' on 1,254 sites

# iOS FTW?

## Apple removes VPN apps from the App Store in China

Jon Russell @jonrussell / 9:59 am IST • July 29, 2017

 Comment

TECHNOLOGY NEWS FEBRUARY 24, 2018 / 5:14 AM / 2 YEARS AGO

## Apple moves to store iCloud keys in China, raising human rights fears

Stephen Nellis, Cate Cadell

8 MIN READ



## *Apple Removes New York Times Apps From Its Store in China*

A woman using her phone on a ferry in Xiamen, Fujian Province. Apple removed mobile news apps created by The New York Times from its app store in China late last month. European Pressphoto Agency

By Katie Benner and Sui-Lee Wee

Jan. 4, 2017



HONG KONG POLITICS & PROTEST SCIENCE & TECHNOLOGY

## Taiwan flag emoji disappears from latest Apple iPhone keyboard

5 October 2019 12:22 · Kris Cheng · 3 min read

## *Apple Removes App That Helps Hong Kong Protesters Track the Police*

By Jack Nicas

Oct. 9, 2019



## Apple removes Quartz news app from the Chinese App Store over Hong Kong coverage

*Quartz says its website has also been banned in mainland China*

By Nick Statt | @nickstatt | Oct 9, 2019, 9:00pm EDT



# iOS FTW?

- Consensus that iOS devices provide **better privacy for the average user** by far
- "iOS definitely does still offer better privacy from apps and their services are generally **more privacy respecting** than Play Services" - D. Micay
- Apple's **privacy initiative** is really impressive!
- But we need to **trust Apple** to act in our best interest, and features **can be removed at any time**.
- **Walled Garden** (censorship, future-proofing, side-loading)
- "The only real alternative [to AOSP] is buying an iPhone" - D. Micay
- Snowden never endorsed iOS because of Apple's intense collaboration with intelligence agencies for mass surveillance

# What are our options?

**TIZEN**<sup>™</sup>

**FAIRPHONE**



**postmarketOS**



 **Purism**



**LineageOS**



/e/ foundation



**SAILFISH OS**



**ubuntu**<sup>™</sup>  
touch



**GrapheneOS**

**KaiOS**



- Librem 5 phone - low specs, \$699
- Hardware toggles for wifi, cellular, etc.
- No support for android hardware
- Low app availability
- Hard to catch up on AOSP hardening efforts from stock linux ([source](#))

## Purism's Librem 5 phone starts shipping—a fully open GNU/Linux phone

The crowdsourced \$700 Linux phone is actually becoming a real product.

RON AMADEO - 9/26/2019, 10:28 PM



The Purism Librem 5, the first attempt at a Linux phone in a long time, is ready to leave the factory.

e Foundation,



for microG

Danial Micay:

- Weakens the SELinux policies
- Rolls back mitigations for device porting / compatibility
- Disables verified boot
- Lacks proper update security including rollback protection
- Adds substantial attack surface like FFmpeg alongside libstagefright, etc.
- Merge in huge amounts of questionable, alpha quality code from the Code Aurora Forum repositories too.
- Many supported devices (including Nexus and Pixel phones) also don't get their full firmware updates shipped by LineageOS.
- [InfoSec Handbook review](#)



# GrapheneOS



**Edward Snowden** ✓

@Snowden



If I were configuring a smartphone today, I'd use [@DanielMicay's @GrapheneOS](#) as the base operating system. I'd desolder the microphones and keep the radios (cellular, wifi, and bluetooth) turned off when I didn't need them. I would route traffic through the [@torproject](#) network.

4:24 PM · Sep 21, 2019 · [Twitter Web Client](#)





- Based on AOSP
- Only support Pixel 2 and Pixel 3 devices
- Locked Bootloader, Verified Boot
- It's focused on privacy and security hardening rather than device support ([source](#))
- Can be built "easily" from source and self-signed
- Experience
  - Great apps on F-Droid
  - Aurora app store works great
  - Notifications won't work for most apps
  - Workable as a daily driver



# TL;DR

- Device support is a mess (Lineage, GrapheneOS)
  - Pixel 2 XL: ~150GBP
  - OnePlus 5t: ~150GBP
  - Pixel 3a: ~270GBP (335EUR new)
- With microG notifications work better, but still not perfect
- Are notifications strictly necessary, and are they good for us?
- Its only "encrypted" if you own the keys, or can prove that noone else does!
- Open Source protects us from functionality being taken away from one day to the next, and gives us a modicum of control
- Use stock AOSP/ GrapheneOS on a Pixel 3. Otherwise go with iOS!