Smartphones With Popular Qualcomm Chip Secretly Share Private Information With US Chip-Maker

19-24 minutes

Summary

During our security research we found that smart phones with Qualcomm chip secretly send personal data to Qualcomm. This data is sent without user consent, unencrypted, and even when using a Google-free Android distribution. This is possible because of proprietary Qualcomm software which provides hardware support also sends the data. Affected smart phones are Sony Xperia XA2 and likely the Fairphone and many more Android phones which use popular Qualcomm chips.

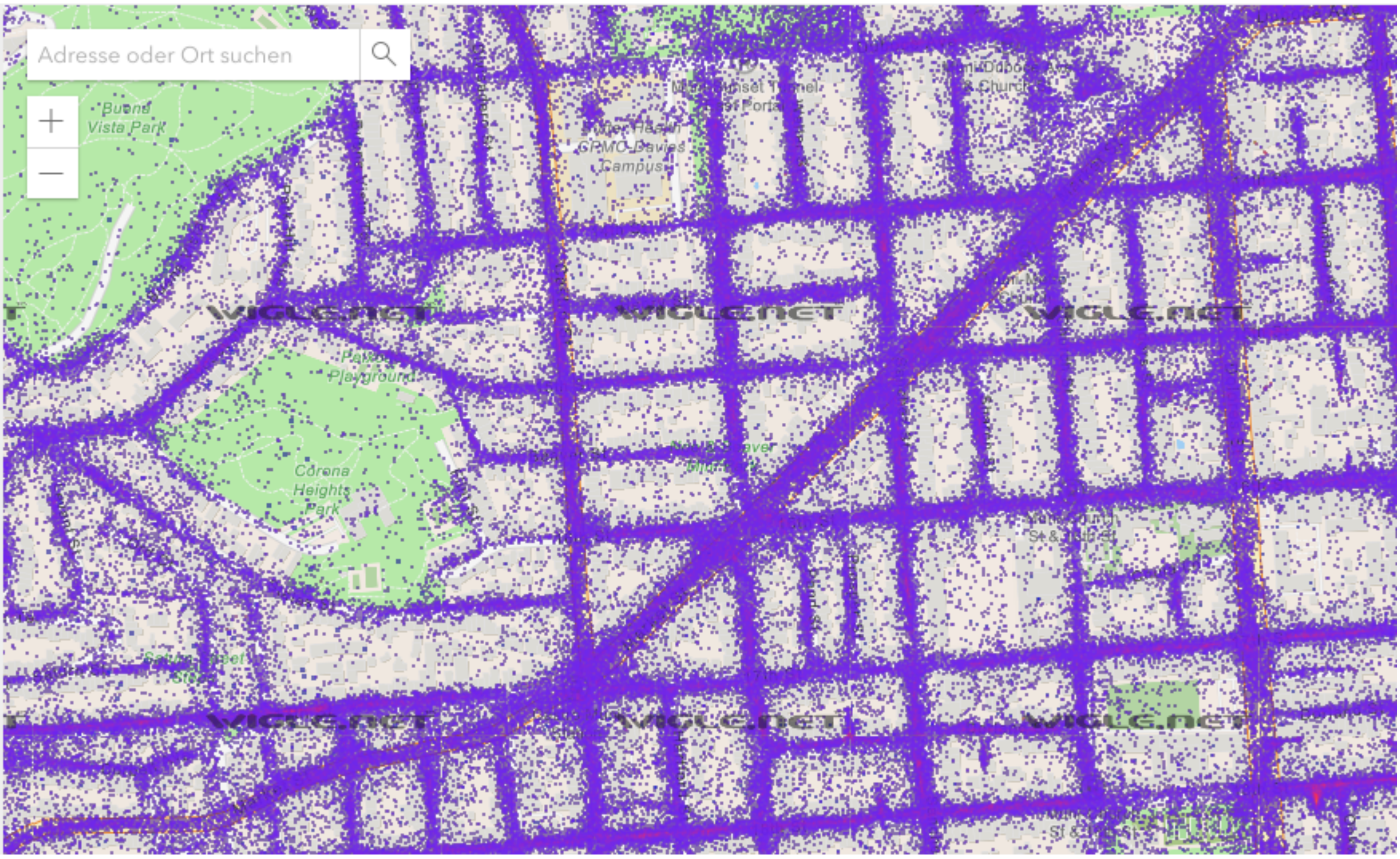
Introduction

The smartphone is a device we entrust with practically all of our secrets. After all, this is the most ubiquitous device we carry with us 24 hours per day. Both Apple and Android with their App Store and Google Play Store are spying on its paying customers. As a private alternative some tech-savy people install a Google-free version of Android on their ordinary smartphone. As an example we analyzed such setup with a Sony Xperia XA2 and found that this may not protect sufficiently because proprietary vendor software, different from the (open source) operating system, sends private information to the chip maker Qualcomm. This finding also applies to other smartphone with a Qualcomm chip such as the Fairphone.

What is a de-Googled Android phone?

A deGoogled Android phone is one that has been modified to not include any of Google’s proprietary (closed-source) apps or services. This usually involves installing a custom ROM that replaces the standard Android software with an open source Android that doesn’t come with any of Google’s apps. You can either install such an Android yourself or buy a phone that already has this done for you (e.g. NitroPhone).

Google surveillance & tracking tools are everywhere but most of this ‘evil’ is located inside the Google Play Services, which is closed-source. Millions of lines of code that include things like constantly scanning your surroundings for Bluetooth and WiFi devices, using WiFi signal triangulation, then matching the visible WiFi antennas with Google’s database of all geographic locations of all WiFi access points they collect in order to know your precise location at all times. This all works without connecting to the detected WiFi networks and even when your GPS is turned off. This method is similar to how the CIA tracked down Pablo Escobar in the 1990s but is now used on a massive scale to track every citizen around the globe.



Sample of wireless access point geolocation database www.wigle.net

To get rid of the almighty powerful Google and Apple and its 24 hour tracking & surveillance tools one approach is to use a de-Googled Android phone. As a result, your deGoogled phone will not have the Google Play Services and Google Play Store but will instead use an alternative open-source store app that offers the same apps. You can also avoid the use of a store altogether by downloading your apps (with the APK file extension) directly from the software vendor's website. This is just as you would when downloading a program to install on your PC.

Analyzing a DeGoogled Phone

In this test, we decided to try /e/OS, a de-Googled open-source version of Android that is privacy-focused and designed to give you control over your data. /e/OS claims that they do not track you and don't sell your data. Let's find out.

We installed /e/OS on a Sony Xperia XA2 smartphone. After installation, the phone boots into the /e/OS setup wizard. It requested us to turn on GPS location service, but we purposely left it off because we do not need it now.

We also didn't place a SIM-card in the phone either so it could only send and receive data over the WIFI network which we are monitoring with Wireshark. Wireshark is a professional software tool which allows us to monitor and analyze all traffic being sent over the network.

After we provided our WiFi password in the setup wizard, the router assigned our /e/OS de-Googled phone a local IP address and it started generating traffic.

The first DNS requests we see:

```
[2022-05-12 22:36:34]    android.clients.google.com
[2022-05-12 22:36:34]    connectivity.ecloud.global
```

Surprisingly, the deGoogled phone's first connection is to *google.com*. According to Google, the host *android.clients.google.com* serves the Google Play Store for periodical device registration, location, search for apps and many other functions. This is strange because we have a deGoogled phone without the Google Play

Store. Later we found out that this request originates from microG, an open source re-implementation of Google's proprietary core libraries and applications.

Then it connects to *connectivity.ecloud.global* which, according to /e/OS, replaces Android's Google server connectivity check *connectivitycheck.gstatic.com*.

Two seconds later the phone started communicating with:

```
[2022-05-12 22:36:36]    izatcloud.net
[2022-05-12 22:36:37]    izatcloud.net
```

We are not aware of any company or service with the name *izatcloud.net*. Therefore we started searching through the /e/OS legal notice and privacy policy but found no mention of data sharing with the Izat Cloud. The /e/OS privacy policy clearly states *"We do not share any individual information with anybody"*. We then searched through the /e/OS source-code they make available on Gitlab and we were unable to find any references to the Izat Cloud.

A quick WHOIS lookup shows us that the *izatcloud.net* domain belongs to a company called Qualcomm Technologies, Inc. This is interesting. Qualcomm chips are currently being used in ca. 30% of all Android devices, including Samsung and also Apple smartphones. Our test device for the /e/OS deGoogled version of Android is a Sony Xperia XA2 with a Qualcomm Snapdragon 630 processor. So there we have a lead.

Is Qualcomm spying on us?

Investigating this further we can see that the packages are sent via the HTTP protocol and are not encrypted using HTTPS, SSL or TLS. That means that anyone else on the network, including hackers, government agencies, network administrators, telecom operators, local and foreign can easily spy on us by collecting this data, store them, and establish a record history using the phone’s unique ID and serial number Qualcomm is sending over to their mysteriously called Izat Cloud.

The data sharing with Qualcomm is not being mentioned in the terms of service from Sony (the device vendor) or Android or /e/OS either. Qualcomm does this without user consent.

We believe this is against the General Data Protection Regulation (GDPR) to collect user data without their consent and contacted Qualcomm's legal counsel about the matter. A few days later they answered and informed us that this data collection was in accordance with the Qualcomm Xtra privacy policy and they shared us a link to their XTRA Service Privacy Policy. So it appears to be that this Izat Cloud we never heard of is part of the XTRA Service we’ve never heard of either. We have the impression that Qualcomm likes to keep things mysterious, hence the name Izat Cloud and the XTRA Service.

Looking at the link Qualcomm sent us, the ‘XTRA Service’ privacy policy states:

> “Through these software applications, we may collect location data, unique identifiers (such as a chipset serial number or international subscriber ID), data about the applications installed and/or running on the device, configuration data such as the make, model, and wireless carrier, the operating system and version data, software build data, and data about the performance of the device such as performance of the chipset, battery use, and thermal data.
>
> We may also obtain personal data from third party sources such as data brokers, social networks, other partners, or public sources.”

They do not mention IP address but we assume they collect that as well. After our research was completed they’ve updated the privacy policy and now added that they do also collect the device's IP address. They also added the information that they store this data for 90 days for ‘quality purposes’.

To clarify, here a list of the data Qualcomm may collect from your phone according to their privacy policy:

1. Unique ID
2. Chipset name
3. Chipset serial number
4. XTRA software version

5. Mobile country code
6. Mobile network code (allowing identification of country and wireless operator)
7. Type of operating system and version
8. Device make and model
9. Time since the last boot of the application processor and modem
10. List of the software on the device
11. IP address

Digging a little deeper we'll find out that the 'XTRA Service' from Qualcomm provides Assisted GPS (A-GPS) and helps provide accurate satellite positions to a mobile device.

What is Assisted GPS (A-GPS), and why do I need it?

GPS was initially developed exclusively for military usage, guiding planes, personnel, and bombs. Receivers were typically positioned in open regions with line-of-sight access to satellites. Since GPS became available for commercial usage, however, new applications have increased the system's requirements.

These new uses required GPS signals to penetrate overhead obstructions, such as trees and roofs. Thus, the "assisted GPS" or A-GPS solution was born. With A-GPS the phone downloads various files containing orbits and statuses of satellites with the approximate GPS satellite locations for the next 7 days to help quickly determine phone's location.

Proprietary device drivers are problematic

The largest part of Android is published as open source and can therefore be analysed regarding potential security and privacy issues. But usually smart phone vendors include additional proprietary software such as device drivers, firmware blobs, system services and apps. The apps are directly visible by the user and can change the system to such an extend that it reminds of a PC of the 90s shipped with Windows 95 and a lot of so called bloat ware.

Obviously also Google-free Android distributions require device drivers to support a given hardware. These drivers are usually proprietary software which gets executed by the operating system and can not only provide the required hardware support but also perform undesired behaviour. The consequences are that even with a deGoogled device we still have no full control on our privacy and which personal identifiable information (PII) is being shared because of this closed-source vendor software that is sharing our private data.

This is why Nitrokey in general is dedicated to open source which is inevitable in order to achieve a secure system. Open source software (and hardware) is the only way to allow verifying a system's behaviour and guarantee its security.

Are other smartphones affected?

Another popular option which is frequently chosen for its privacy is the Fairphone. The Dutch company produces excellent phones allowing users to maintain the phone and replace parts themselves when broken. In spite of its reputation for bolstering users' privacy, all Fairphone models contain a Qualcomm chip probably execute Qualcomm's software. The Fairphone has therefore the same issue with sharing of personal data with the Qualcomm XTRA Service. Although not tested, we suspect that the same privacy issues affect many other choices of smartphone brands that use Qualcomm processors, including so called encrypted phones or crypto phones.

NitroPhone is secure

Nitrokey’s NitroPhone does not contain the Qualcomm chipset and our tests confirm that when GPS is turned-off, no requests for A-GPS are being made. When GPS is turned-on, to prevent Google from obtaining and storing your IP address, the NitroPhone's GrapheneOS contacts and downloads the A-GPS files from *google.psds.grapheneos.org*, a proxy server supplied by GrapheneOS to protect users’ privacy. And unlike Qualcomm, GrapheneOS does not share any personal information with the GrapheneOS proxy servers, nor with Google or Qualcomm.

Furthermore, GrapheneOS allows you to disable the feature to request A-GPS files (opt-out) or, if you prefer, to use Android’s standard servers *agnss.goog*. At the moment, neither /e/OS, Lineage, or Sailfish OS nor any other phone we could find, supports this feature or provides this level of freedom.

Conclusion

Qualcomm’s proprietary software is not only downloading some files to our phone to help establish the GPS location faster, but also uploads our personal data, such as the devices’ unique ID, our country code (Germany in this case), our cellphone operator code (allowing identification of country and mobile operator), our operating system and version and a list of software on the device. This creates a completely unique signature of us enabling behavioral tracking and decreasing user’s privacy significantly. No matter if we have GPS turned-off.

The fact that Qualcomm collects a large amount of sensitive data and transmits it via the insecure and outdated HTTP protocol shows us that they do not care about users’ privacy and security. This doesn’t require to speculate of Qualcomm collaborating with various government spy agencies, but also creates a risk when the traffic is potentially intercepted also by dictators and other suppressive governments not even requiring a collaboration with Qualcomm. Not only drones make frequent use of location information to target people. There are cases where people’s kidnappings and/or assassinations have been facilitated by the use of the victims location information. A most recent example is Iran where protesters get arrested because of their smartphone location tracking. This even doesn’t require tapping the phone. The cleartext traffic is also hotbed for data brokers which sell people’s data (e.g. shopping centers).

Affected users could try blocking the Qualcomm XTRA Service using a DNS-over-TLS cloud-based block service, or re-route this traffic yourself to the proxy server from GrapheneOS, but this requires technical expertise and does not provide the same level of security as the NitroPhone.

Update, 5/6/2023
GrapheneOS released the 2nd and final part of fixing this issue for their Qualcomm devices.

Update, 5/2/2023

We published this article on 25.4.2023, after which it was heavily discussed in social media (esp. Mastodon). Besides interest and praise, it was also criticized. Some of this criticism was justified but there was also unjustified criticism and misunderstandings. So here is an overview of what happened and our statement to the criticism:

On the same day GrapheneOS responded with a technical critique. However, their statement starts with a criticism of the Reddit post "German security company Nitrokey proves that Qualcomm chips have a backdoor and are phoning home" and not of our article:

> NitroKey did not discover a backdoor. [...] The title used for the post here is editorialized and doesn't match what the article actually states. This is not a backdoor.

GrapheneOS hereby refers to the Reddit post that wrote about an allegedly found "backdoor" and not to our article. Our article does not talk about a backdoor, but the title of the Reddit post (which is not from us) is wrong. Obviously, many people (e.g. on Mastodon) misunderstood this.

> The post is very sensationalized and it's unfortunate they didn't run this by us first.

They are right and we'll learn by this mistake and ensuring more qualitative publications in the future.

In addition, GrapheneOS expressed justified criticism of our article, which incorrectly assumed that the criticized functionality is executed in the chip's firmware. Instead, this functionality is executed in the Xtra Daemon in user space. We corrected this in the article on 27th April. Furthermore, we corrected that day that microG is responsible for calling android.clients.google.com.

Also on 25th April, Martijn Braam responded with a critique. Among other things, he criticized the article for being too lurid. From the perspective of an IT expert, for whom the facts described have been known for a long time, this may be perceived that way. However, this article is also aimed at non-experts. And yes, in order to communicate a technically demanding topic widely, it is sometimes necessary to summarize it in a single point.

> There's no claims being made by NitroKey that their phone doesn't provide any of this [Cell network, WiFi and network geolocation].

Although this is less of a criticism, here's a clarification: NitroPhones (resp. GrapheneOS) doesn't use such geolocation services.

> This system does not actually send any of your private information like the title of the article claims.

Here we disagree and this is the key point of our article. See below. This issue has been found with Fairphone already.

> This feature is not breaking laws, it's not unethical, it's not even made for eeeevill.

We stand by our conviction that collecting device IDs and IP addresses without user consent cannot be considered legitimate or ethical; regarding what breaks the law, multiple courts rulings led us to the legitimate doubt that Qualcomm may be in contrast with the GDPR with this data collection, but since we're no lawyers we reported it to Noyb, a non-profit organization committed to the legal enforcement of European data protection laws.

On 26th and 27th April, respectively, The Register and Computer Base published a Qualcomm statement and an analysis of our article. Unfortunately, these reports focus on the above-mentioned and already corrected error in our article. At the same time, they confirm that the device ID and IP address, as well as other personal information, are transmitted to the manufacturer.

Qualcomm downplays this and contradicts itself in the process:

> [...] the relevant Qualcomm technologies use non-personal, anonymized, technical data to enable device manufacturers to provide their customers location-based apps and services [...]

Unfortunately Computer Base doesn't challenge the necessity of transmitting the data but agrees with us on the following point:

> Encrypted connection would be appropriate

The Register assesses the risk as follows:

> Mobile device data transmissions may pose a problem in high-risk environments because network identifiers such as IP addresses can be considered personal data, particularly when paired with hardware identifiers or other sorts of data.

And likewise confirmed on 27th April by GrapheneOS:

> NitroKey is correct that xtra-daemon has support for sending information on the device including device model, serial number, etc. They're also correct that the user is never asked about it.

On 28th April, a DDoS attack of 50 GBits shut down our website for 20 hours. We assume by someone who didn't like our article. It's a pity that people often form opinions based only on headlines or half-truths, and this can have such consequences.

On 29th April GrapheneOS summarized:

> We weren't trying to say that anything was wrong with NitroKey's product only that their post has been corrected and the issue they talk about is real, but they got some important details wrong. We think the post needs some more changes and it's unfortunate that their coverage of a real issue got derailed by them making some mistakes about the details and over-sensationalizing it.

On 30th April, GrapheneOS released a software update that partially fixes the privacy issue we pointed out for GrapheneOS.

Unfortunately, the core message of our article has been somewhat relegated to the background in the whole discussion. We stand by our article's statement that Qualcomm collects users' private information in an unauthorized and unnecessary way.

Update, 4/27/2023
The text has been corrected to state that the responsible software is not executed as firmware but in the operating system. Also requests to *android.clients.google.com* originate from microG.

Author
Paul Privacy is an independent security researcher with a focus on privacy and helping others to obtain privacy on their phones and computers. Because privacy is cool. And being spied on is NOT cool. Be private. Be Cool. For a free consult you can contact me at: paulprivacy@posteo.ch or follow me on Twitter at @PaulPrivacyCool