USER CONTROLS FOR AD PERSONALISATION ON ANDROID

INTRODUCTION

The purpose of this technical note is for users to know what the advertising IDs are for their devices, why they are used and what control options can be implemented on them. Concretely, the *Android Advertising ID (AAID)*[1] is being analysed, making it clear that the option Android offers users to prevent ad personalisation does not prevent the user's personal data from being communicated to third parties. Developers, content providers and all agents involved in the process should verify user configuration with regard to not receiving personalised advertising and not being profiled, respecting this choice and avoiding any type of processing of the user's personal data in this regard, including even compiling or transmitting them.

ANDROID ADVERTISING ID

In 2014, with the launch of KitKat, Android introduced an advertising ID known as AAID, in line with the *Identifier for Advertisers* (IDFA) that Apple had already been using for some time. This identifier is also known as the *Google Advertising ID (GAID).*

IDFA and AAID are identifiers solely for advertising, which in the case of Android is provided by the Google Play services, which users can change at any time from their mobile devices. The use of other unique device identifiers, such as IMEI, the MAC address or the device serial number, needed to be completely replaced by the use of identifiers such as AAID and IDFA. The programme policy for Google Play[2]developers establishes that, for any advertising purpose, the advertising ID must be used on all updates and new apps uploaded to Google Play, and not other device identifiers, whatever they could be.

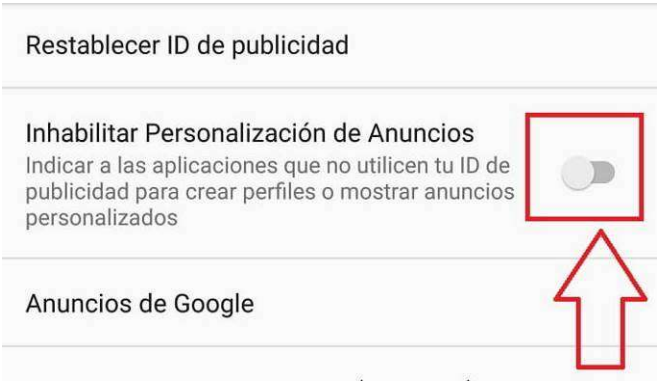

Figure 1

The objective alleged by Google for introducing the *AAID* is to provide users with better controls over their privacy, as well as giving developers a system that lets them continue obtaining income from their apps. The improvement for users basically consists of being able to change ('re-establish' in Google speak) the ID, which would let them disassociate the device from previously compiled

[1] https://support.google.com/googleplay/android-developer/answer/6048248?hl=es

[2] Google Play Developer Program Policies

data, as well as disabling the personalised ads on Google Play applications.

To find out what the AAID is, change it or disable personalised ads, go to Settings->Google->Advertisements, as shown in Figure 1.

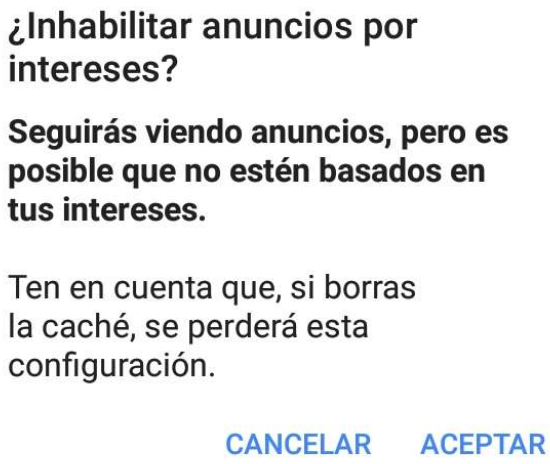

Figure 2

The reality is that the possibility of re-establishing the *AAID* is unknown to the large majority of users, including its existence and use.

With regard to the effects of disabling personalised ads, this is a setting that is transferred to entities that produce the advertising, and it depends on the entities whether or not they respect users' preferences. However, this does not prevent the *AAID* from being sent by some apps and, thus, it does not prevent a continued construction of a profile based on users' interests or tastes to, for example, use it in the future when the personalisation of ads could be active again. By disabling ad personalisation, Google itself warns that if the user deletes the cache, advertising personalisation would be activated again and also warns of the ineffectiveness of the measure by also stating that it is possible that ads will not be based on the user's interests, but not guaranteeing this in either case. See Figure 2. For example, after resetting a device to factory values (Nexus 5, Android 6.0.1), ad personalisation is enabled by default again. Users must do something to disable them via the menu set out above, and not the opposite, which is what should happen pursuant to the default privacy policy of the GDPR.

Some studies[3] have revealed how Facebook can track Android users, even users without Facebook accounts. In the study *How Apps on Android Share Data with Facebook,* by *Privacy International,* over 30 apps were analysed, concluding that over 61% of them send data to Facebook when the user opens the app. Other studies[4] claim that up to 42% of free apps on the Google Play Store could be sharing data with Facebook.

How these ad IDs work is relatively simple. While using an app that uses this type of technology, a message is sent with specific information on the event when the user does specific actions, along with the corresponding ID to a specific entity, which can therefore keep a log of events related to a concrete device. Information on the event can be very different depending on each concrete application. We will use the AZ Screen Recorder[5] app as an example, which uses Facebook advertising services, installed on an Android device with ad personalisation enabled. When the application is running, there

[3] How Apps on Android Share Data with Facebook, Privacy International

[4] Measuring third party tracker power across web and mobile: Reuben Binns, Jun Zhao, Max Van Kleek and Nigel Shadbolt 2018

[5] https://play.google.com/store/apps/details?id=com.hecorat.screenrecorder.free&hl=es

are communications with Facebook servers, during which the *AAID* is sent, along with other information, including and meriting mention the app name. The *AAID* is sent via a POST request to graph.facebook.com within the *IDFA*[6] parameter, and the app name in the field *BUNDLE*. See Figure 3.

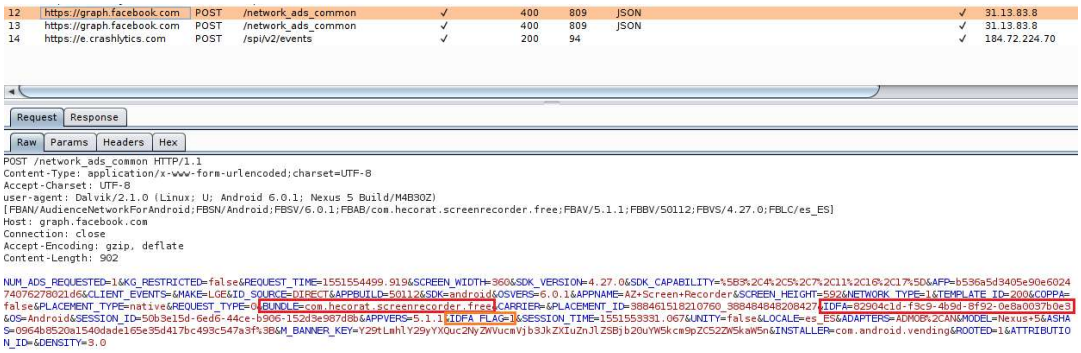

Figure 3

If the same app is run on the same device, but this time with ad personalisation disabled, a very similar POST request is sent, as can be seen in Figure 4.

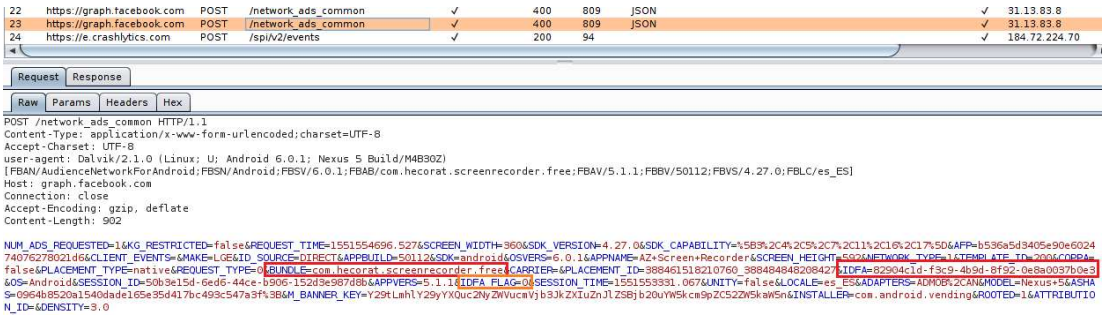

Figure 4

Despite the new setting, the AAID and the name of the app that is being run continue to be sent to graph.facebook.com. The only difference can be found in the *IDFA_FLAG* parameter, whose value in this second case is 0, which is used to tell the Facebook API that the user does not want the ad shown in the app to be based on his or her likes or interests.

This means that the action of disabling advertising based on users' likes and interests for apps only indicates, in this case to Facebook, that personalised ads should not be returned, but does not prevent Facebook from continuing to compile user data and associating them with an advertising ID, such as the name of the app that sent the request, due to which it can continue creating a profile based on the applications that are run. As mentioned above, this data compilation occurs regardless of whether the device user is registered on Facebook.[7]

[6] https://developers.facebook.com/docs/app-ads/targeting/mobile-advertiser-ids/?locale=es_ES

[7] How Apps on Android Share Data with Facebook, Privacy International

Figure 5 shows a sending of the *AAID* while running an app with a sexual subject.[8]

The simple fact of opening this app leads to communicating the *AAID* to graph.facebook.com, indicating not only the app name, but other information, such as the location of the device 'Europe/Madrid', the model 'Nexus 5' and the language 'es_ES'. This sending occurs regardless of whether or not ad personalisation is disabled.

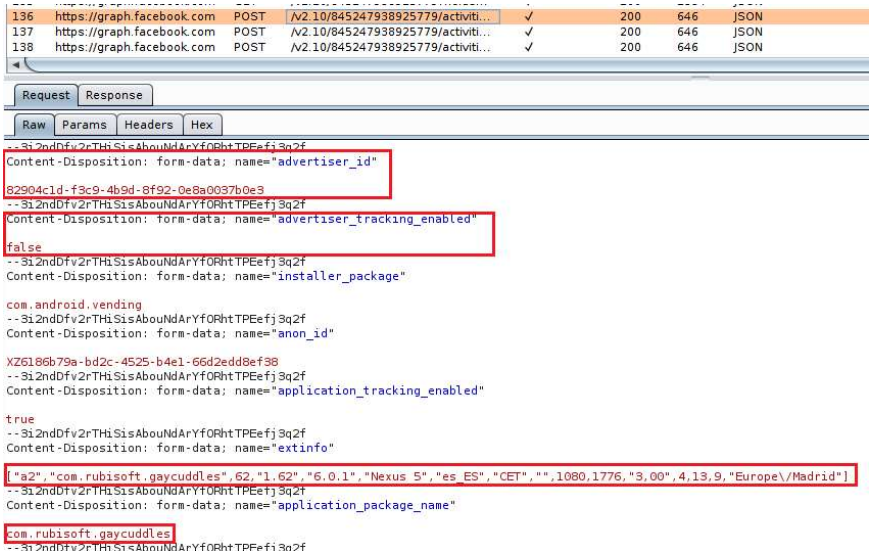

Figure 5

RECOMENDATIONS FOR APP DEVELOPERS

App developers should bear in mind that sending personal data to a third party is considered personal data processing, for which a legal basis is required and, as such, must also comply with all principles applicable to data processing established by the GDPR, including the data minimisation principle. Before including a third party SDK on an app, developers must assess the risks for user privacy that they could be introducing and thoroughly study the different privacy setting options that the SDK may offer, heeding default privacy principles and in their designs. In short, they must try to provide users with default settings that protect their privacy and real options that let them not be the object of tracking.

Those who make the implementation of these types of techniques available to SDK developers must also facilitate compliance with all GDPR principles, including the principles of privacy by design and by default.

In parallel, developers of operating systems for any types of device must provide users with real control over their personal data, in this case real control over their advertising ID, letting them not only change it, but also prevent apps and libraries from being able to access this ID if users do not give permission for their use with a specific purpose.

[8] https://play.google.com/store/apps/details?id=com.rubisoft.gaycuddles

RECOMENDATIONS FOR USERS

For users who want to avoid profiling, they must disable ad personalisation on their devices, despite the limitations on the effectiveness of this measure in many cases, also reset the AAID frequently and keep only those apps installed on the device that are useful and provide an adequate confidence level. A critical attitude must be kept, and only choose products from developers complying with their obligations as personal data controllers.