CONTROL DEL USUARIO EN LA PERSONALIZACIÓN DE ANUNCIOS EN ANDROID

INTRODUCCIÓN

Esta nota técnica está orientada a que los usuarios conozcan qué son los identificadores de publicidad de sus dispositivos, para qué se utilizan y que opciones de control pueden ejercer sobre los mismos. En concreto se analiza el *Android Advertising ID (AAID)*[1] y se pone de manifiesto que la opción que ofrece Android al usuario para evitar la personalización de anuncios no evita que datos personales del usuario puedan ser comunicados a terceros. Desarrolladores, proveedores de contenido y todos los agentes implicados en el proceso deben comprobar la configuración del usuario en cuanto a no recibir publicidad personalizada y no ser perfilado, respetando esta elección y evitando cualquier tipo de tratamiento de datos personales del usuario en este sentido, incluida la mera recopilación o transmisión de los mismos.

IDENTIFICADOR PARA PUBLICIDAD EN ANDROID

En 2014, con el lanzamiento de KitKat, Android introdujo un identificador de publicidad conocido como AAID, en línea con el *Identifier for Advertisers* (IDFA) que Apple venía utilizando tiempo atrás. Este identificador también se conoce como *Google Advertising ID (GAID)*.

IDFA y AAID son identificadores únicos para publicidad, que en el caso de Android es proporcionado por los servicios de Google Play, y que el usuario puede cambiar en cualquier momento desde su dispositivo móvil. El uso de otros identificadores únicos del dispositivo como el IMEI, la dirección MAC o el número de serie del dispositivo, debía ser plenamente sustituido por el uso de identificadores como el AAID e IDFA. La política del programa para desarrolladores de Google Play[2] establece que, para cualquier fin publicitario, debe usarse el ID de publicidad en todas las actualizaciones y aplicaciones nuevas subidas a Google Play, y no otros identificadores de dispositivo, cualesquiera que sean.

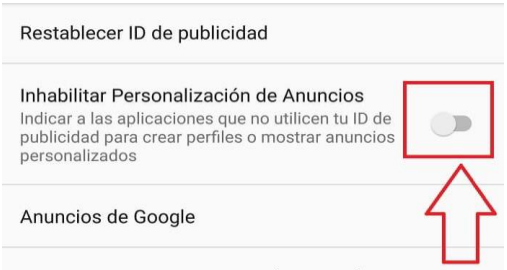

Figura 1

El objetivo alegado por Google para la introducción de *AAID* es proporcionar al usuario mejores controles sobre su privacidad, a la vez que dota a los desarrolladores de un sistema que les permite seguir obteniendo ingresos con sus aplicaciones. La mejora para los usuarios consiste básicamente en que pueden cambiar

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

[2] Política del Programa para Desarrolladores de Google Play

(restablecer según Google) el identificador, lo que permitiría desvincular el dispositivo de los datos recopilados anteriormente, y también pueden inhabilitar los anuncios personalizados en las aplicaciones de Google Play.

Para conocer el AAID, cambiarlo o inhabilitar los anuncios personalizados debe accederse a Ajustes->Google->Anuncios, como puede verse en la figura 1.

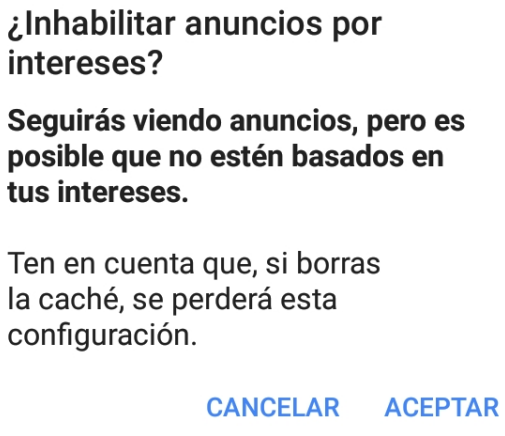

Figura 2

La realidad es que la posibilidad de restablecer el *AAID* es desconocida para la gran mayoría de usuarios, incluso su propia existencia y utilidad.

En cuanto a los efectos de inhabilitar los anuncios personalizados, se trata de una configuración que se transmite a las entidades que generan la publicidad, y depende de estas entidades respetar o no esta preferencia del usuario. Sin embargo, esto no evita que el *AAID* sea enviado por algunas aplicaciones y por tanto no impide que se pueda seguir construyendo un perfil basado en los intereses o gustos del usuario para, por ejemplo, utilizarlo en un futuro cuando la personalización de anuncios pueda volver a estar activa. Al inhabilitar la personalización de anuncios, el propio Google advierte de que, si el usuario borra la caché, la personalización de la publicidad volvería a estar activa, y además advierte de la ineficacia de la medida al indicar también que es posible que los anuncios no estén basados en los intereses del usuario, no asegurando este extremo en ningún caso. Ver Figura 2. Por ejemplo, tras reiniciar un dispositivo a valores de fábrica (Nexus 5, Android 6.0.1) la personalización de anuncios vuelve a estar habilitada por defecto. El usuario tiene realizar una acción para deshabilitarla a través del menú anteriormente expuesto, y no al revés, que es como debería suceder de acuerdo al principio de privacidad por defecto del RGPD.

Algunos estudios[3] han puesto de manifiesto cómo Facebook puede realizar seguimiento de los usuarios en Android, incluso a usuarios que no tengan cuenta en Facebook. En el estudio *How Apps on Android Share Data with Facebook,* de *Privacy International, s*e han analizado más de 30 aplicaciones, concluyendo que más del 61% de esas aplicaciones envían datos a Facebook en el momento en el que el usuario abre la aplicación. En otros estudios[4], se indica que hasta un 42% de aplicaciones gratuitas del Google Play Store podrían estar compartiendo datos con Facebook.

El funcionamiento de estos identificadores de publicidad es relativamente sencillo, durante el uso de una aplicación que utilice este tipo de tecnología, ante determinadas acciones del usuario se genera un mensaje que envía cierta información del evento junto con el identificador correspondiente a una determinada entidad, que así puede

[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

mantener un histórico de eventos relacionados con un dispositivo concreto. La información relativa al evento puede ser muy diferente dependiendo de cada aplicación concreta. Si se toma como ejemplo el caso de la aplicación AZ Screen Recorder[5], que utiliza los servicios de publicidad de Facebook, instalada en un dispositivo Android con la personalización de anuncios habilitada. Durante los momentos en los que la aplicación está en ejecución se producen comunicaciones con servidores de Facebook en los que se envía el *AAID* junto con otra información entre la que destaca el nombre de la aplicación. El *AAID* se envía mediante una petición POST a graph.facebook.com dentro del parámetro *IDFA*[6], y el nombre de la aplicación en el campo *BUNDLE*. Ver figura 3.

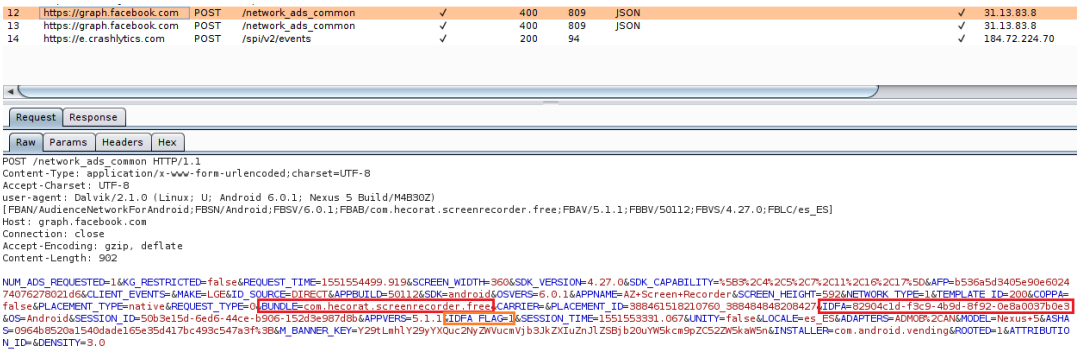

Figura 3

Si se ejecuta la misma aplicación, en el mismo dispositivo, pero esta vez con la personalización de anuncios deshabilitada, se produce una petición POST muy similar, como se aprecia en la figura 4.

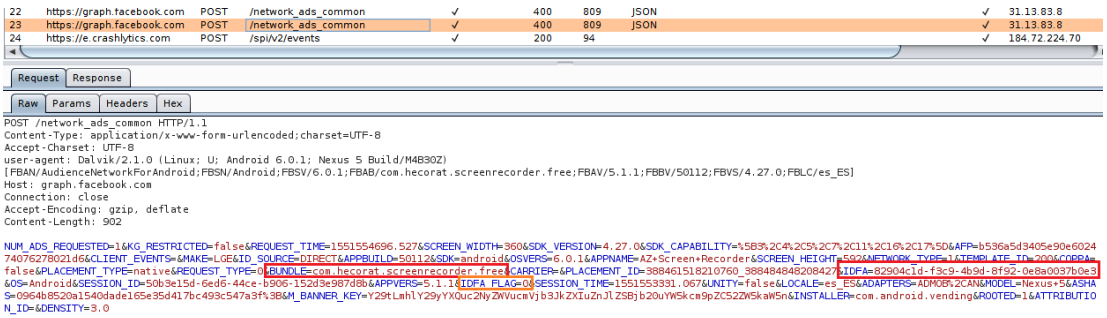

Figura 4

A pesar de la nueva configuración, se sigue enviando a graph.facebook.com el *AAID* y el nombre de la aplicación que se está ejecutando, la única diferencia se encuentra en el parámetro *IDFA_FLAG*, cuyo valor en este caso es 0, y sirve para indicar a la API de Facebook que el usuario no desea que el anuncio a mostrar en la aplicación esté basado en sus gustos o intereses.

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

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

Es decir, la acción de deshabilitar la publicidad basada en gustos e intereses del usuario para las aplicaciones únicamente indica, en este caso a Facebook, que no devuelva un anuncio personalizado, pero no evita que éste pueda seguir recopilando datos del usuario y asociándolos a un identificador de publicidad, como el nombre de la aplicación que ha generado la petición, por lo que puede continuar elaborando un perfil basado en las aplicaciones que se ejecutan. Como se ha indicado anteriormente, esta recopilación de datos se produce independientemente de que el usuario del dispositivo esté registrado en Facebook[7].

En la figura 5 se muestra en envío del *AAID* durante la ejecución de una aplicación de temática sexual[8].

El simple hecho de abrir esta aplicación produce la comunicación del *AAID* a graph.facebook.com, indicando no solo el nombre de la aplicación, sino otra información como por ejemplo la localización del dispositivo “Europe/Madrid”, el modelo “Nexus 5” y el idioma “es_ES”. Este envío se produce independientemente de que esté deshabilitada la personalización de anuncios.

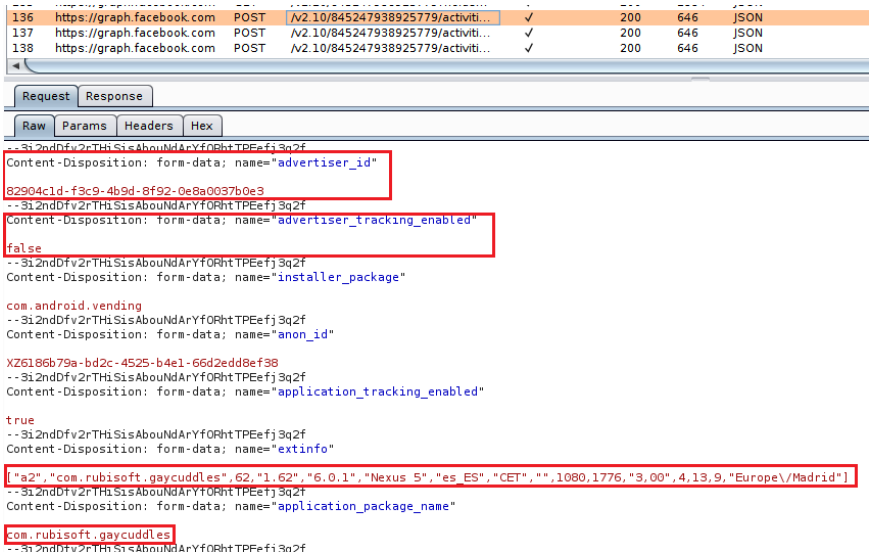

Figura 5

CONSEJOS PARA DESARROLLADORES

Los desarrolladores de aplicaciones deben tener en cuenta que el envío de datos personales a una tercera parte se considera un tratamiento de datos personales para el que es necesaria una base legal, y como tal, además deben cumplir con todos los principios aplicables a tratamientos de datos que el RGPD establece, entre ellos el principio de minimización de datos. Antes de incluir una SDK de tercera parte en una aplicación, los desarrolladores deben valorar los riesgos para la privacidad de los usuarios que se pueden introducir y estudiar meticulosamente las diferentes opciones

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

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

de configuración de privacidad que la SDK puede ofrecer, atendiendo a los principios de privacidad por defecto y desde el diseño. En definitiva, se trata de proporcionar al usuario una configuración por defecto que proteja su privacidad y opciones reales que le permitan no ser objeto de seguimiento.

Quienes ponen a disposición de desarrolladores los SDKs para la implementación de este tipo de técnicas deben facilitar el cumplimiento con todos los principios del RGPD, incluidos los principios de privacidad desde el diseño y por defecto.

Al mismo tiempo los desarrolladores de sistemas operativos para cualquier tipo de dispositivos deben proporcionar al usuario un control real sobre sus datos personales, en este caso concreto un control real sobre su identificador de publicidad, permitiendo no solo cambiarlo, sino también evitando que aplicaciones y librerías puedan acceder a ese identificador si el usuario no da permiso para su uso con una finalidad concreta.

CONSEJOS PARA USUARIOS

Aquellos usuarios que deseen evitar el perfilado tienen que deshabilitar la personalización de anuncios en el dispositivo tal como se indica en el texto, siendo consciente de la limitación de su eficacia, así como reiniciar el AAID frecuentemente y mantener instaladas en el dispositivo únicamente aquellas aplicaciones que realmente sean útiles y proporcionen un nivel de confianza adecuado.

El usuario ha de mantener una actitud crítica y seleccionar los productos de aquellos desarrolladores que cumplan con sus obligaciones como responsables de tratamiento de datos personales.