mnemonic

CLASSIFICATION: PUBLIC

TECHNICAL REPORT

"OUT OF CONTROL" – A REVIEW OF DATA SHARING BY POPULAR MOBILE APPS

Norwegian Consumer Council

Place	Oslo
Date	14.01.2020
Version	1.0
Authors	Andreas Claesson and Tor E. Bjørstad

Report summary

Introduction

As part of an ongoing collaboration with the digital consumer rights team at the Norwegian Consumer Council (NCC), mnemonic researchers have carried out an in-depth investigation into how mobile applications share data with third parties for advertising purposes. The analysis has covered a selection of 10 popular mobile applications on the Android platform.

The purpose of the testing has been to increase our understanding of the mobile advertising ecosystem. In particular, we have aimed to identify some of the main actors collecting user data from our sample set of apps, understand the type and frequency of data flows, and examine the specific information that is being transmitted.

A key motivation for this project has been that data collection, sharing, and processing within the advertising industry on mobile platforms is poorly understood by the general public, policy-makers, and the tech community. One of our main goals has been to help clarify this topic.

All the apps have been analysed in mnemonic’s mobile testing lab, where we have set up infrastructure to monitor and capture communications from our test device. The project has been carried out between May and December 2019, with the majority of testing in July and August.

From our testing, we have collected a large amount of mobile traffic data, while working without any inside knowledge of the data collection ecosystems. The vast volumes, as well as the nature of black-box analysis, has made it hard to interpret the data and get a complete picture of the situation. This report documents data collection and sharing practices which appear highly problematic in terms of data privacy and consent. However, these findings are by no means exhaustive. We hope that this report may serve as the beginning of a debate on mobile advertising practices, rather than the final word.

Summary of findings

Some of the key findings in this report are:

1. All apps tested share user data with multiple third parties, and all but one share data beyond the device advertising ID. This includes information such as the IP address and GPS position of the user, personal attributes such as gender and age, and app activities such as GUI events. In many cases, this information can be used to infer attributes such as sexual orientation or religious belief.
2. The **Grindr** app shares detailed user data with a very large number of third parties, including IP address, GPS location, age, and gender. By using **MoPub** as a mediator, the data sharing is highly opaque as neither the third parties nor the information transmitted are not known in advance. We have also seen that **MoPub** can enrich the data that is shared with other parties dynamically.
3. The **Perfect365** app shares user data with a very large number of third parties, including attributes such as advertising ID, IP address, and GPS position. One could almost say that the app appears to be built to collect and share as much user data as possible.
4. The **MyDays** app shares the user’s GPS location with multiple parties, and the **OkCupid** app shares detailed personal questions and answers with **Braze**.

During testing, more than **88.000 web requests** made by the apps were logged and analysed, covering **216 unique domains** and at least **135 third parties** within the advertising space.

Figure 1 visualises the data flows observed for companies who receive data from multiple apps.

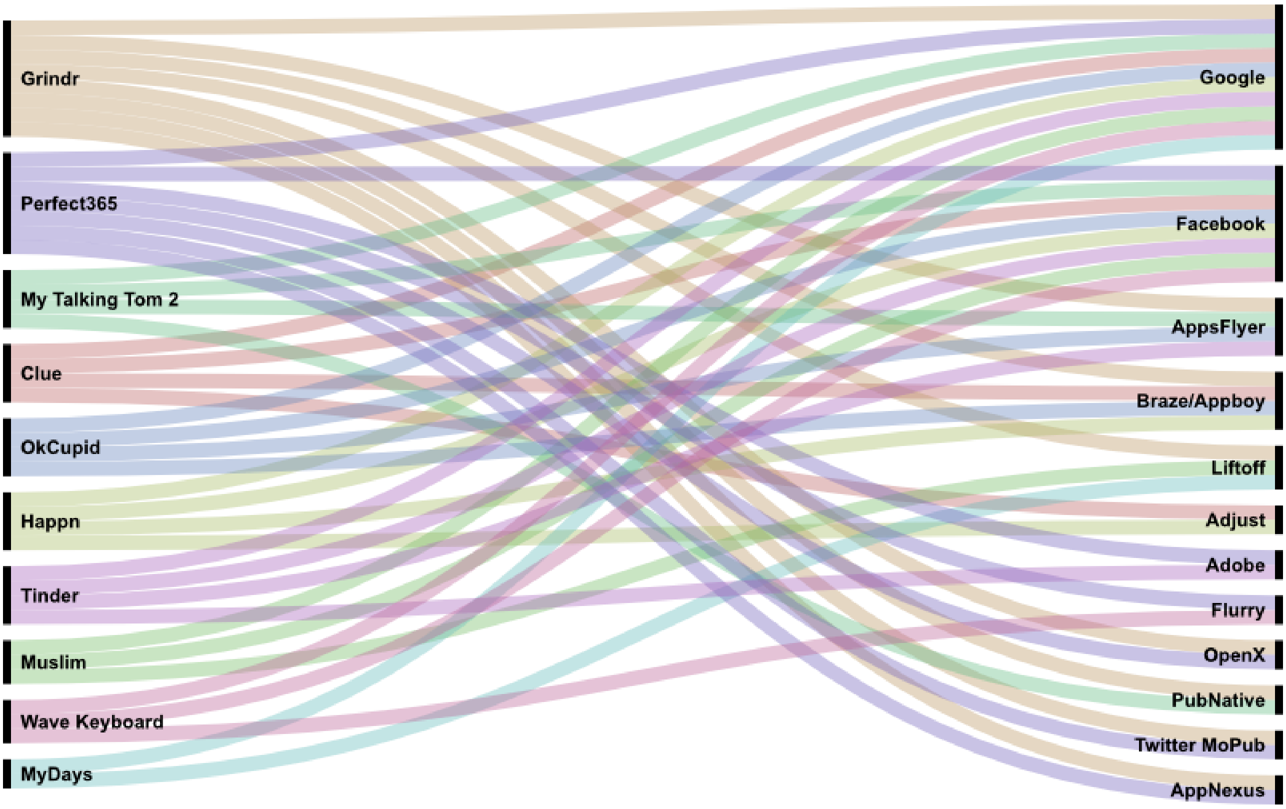


Figure 1. Advertising companies receiving data from multiple apps

About mnemonic

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Security Services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region’s top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally.

With intelligence-driven managed security services, 185+ security experts and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

This is the second major collaboration between the NCC and mnemonic, the first being the #WatchOut[1] investigation into the cybersecurity of smart watches for children in 2017.

[1] Published as https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/ and https://mnemonic.no/watchout on October 18th, 2017

Table of Contents

List of tables and figures

Tables

Figures

1 Introduction

1.1 Introduction to the report

mnemonic has carried out an in-depth investigation of 10 popular mobile apps, focusing on the type and amount of personal data that is being shared with third parties for advertising purposes. The purpose of the testing has been to gain knowledge about how the mobile advertising ecosystem works, in terms of data sharing and communication patterns, and document concrete examples of how user data is being collected and shared as part of app monetization.

All the testing carried out as part of this research has been done on Google's Android platform, with apps downloaded from the Google Play store. This was a practical decision made early on in the project, based on the fact that it would require significant additional effort to cover additional platforms such as iOS, and that the Android platform has by far the highest market share in the smartphone market globally[2]. Another factor is that Google plays a significant role in online advertising, although this has not been a primary focus of the research.

Our tests have covered 10 apps that are well-known and widely used, which were selected for analysis by the Norwegian Consumer Council. The apps cover a number of highly personal topics, such as dating, religion, and health. Chapter 1.2 provides a list of the specific apps and versions tested.

The results of our testing document that a significant degree of user data, including personal data, is being shared from the apps with third parties in the advertising or "adtech" industry. We expect that our results will be widely applicable to other people in Norway, using the same apps during the same time as the testing was carried out. We also expect that the findings are broadly generalizable within the EU / EEA. Privacy controls on the iOS platform are more stringent than on Android, but we expect that some of the findings would also apply there.

This report describes the results of the technical testing in further detail, providing evidence of our findings, as well as mnemonic's initial analysis and evaluation. Due to the sheer volume of data, as well as the presence of some personal data related to location in the datasets, the underlying raw data from our analysis is not included as part of the report.

For additional contextual information about the mobile advertising industry, and higher-level analysis of the findings, we refer to the Norwegian Consumer Council's technical report, *Out of Control – How consumers are exploited by the online advertising industry* [3], which is published as a companion to this work.

[2] Domestically in Norway, the respective market shares of Android and Apple's iOS are estimated to be roughly equal, although precise numbers are not known to us. Globally, Android is known to have the largest market share, estimated at about 75%.

[3] The NCC's full report and additional information about the project can be obtained at https://www.forbrukerradet.no/out-of-control/

1.2 Apps tested by mnemonic

mnemonic has tested 10 popular mobile apps on the Android platform. The apps are listed and categorised in Table 1.

App	Package name	Category
Grindr	com.grindrapp.android	Gay dating
Perfect365	com.arcsoft.perfect365	Virtual makeup
My Days	com.chris.mydays	Period tracker
OkCupid	com.okcupid.okcupid	Online dating
My Talking Tom 2	com.outfit7.mytalkingtom2	Children's app
Muslim: Qibla Finder	com.hundred.qibla	Muslim assistant
Tinder	com.tinder	Online dating
Clue	com.clue.android	Period tracker
Happn	com.ftw_and_co.happn	Online dating
Wave Keyboard	com.wave.keyboard	Keyboard themes

Table 1. List of apps tested by mnemonic

1.3 Test scope and boundaries

mnemonic has tested 10 mobile applications for Android that have been published by their developers on the Google Play store, and are distributed in the form of Android application packages (APKs). mnemonic has downloaded and installed the apps on our Android test device in the ordinary way, similarly to what a regular user would do.

Mobile apps commonly contain a variety of third-party software development kits (SDKs). The SDKs are self-contained pieces of code that the app developers have chosen to include as part of their app, and which may be used by the developers to provide added functionality. This is a common and legitimate pattern. For example, apps that need to support credit card payments normally embed an SDK from their payment service provider, in order to handle credit card information in a standardized and secure way.

mnemonic has observed a large number of SDKs from third parties associated mainly with online advertising, within the apps that we have tested. It is a reasonable assumption that these are primarily used to add advertising-related features to the apps. However, to conclusively determine how any given SDK is used by a specific app would require extensive in-depth analysis, and was considered out of scope for this project due to time constraints[4].

The apps communicate with back-end services using the HTTP protocol. Transport layer security (TLS, also referred to as HTTPS) is used to secure the data in transit over the Internet. mnemonic has applied various techniques, described further in Chapter 4, in order to monitor the transmissions from our test phone. Since such monitoring is generally what TLS is trying to prevent, this has mainly been feasible because we are in control of the test devices, and have intentionally weakened or bypassed some of the security mechanisms present to protect the users.

During testing, mnemonic has focused on documenting how the apps transmit data to third parties, identifying which third parties are receiving data from the apps, and analysing what information is present in the transmissions. In most situations, we are conclusively able to identify which app is responsible for any given message that has been observed by us. However, attributing the observable behaviour of the apps to specific SDKs within those apps, would require a significantly deeper analysis.

In our professional opinion, the distinction between app and SDK is in some sense less important, because the app's creators have ultimate responsibility for what their app does when they release it to the public. When an app is sending data to third parties, whether for advertising or other purposes, the root cause eventually boils down to choices made during development of the app. However, third parties that receive data are also responsible for how they collect and process such data.

It is worth pointing out that the presence of SDKs in an app does mean that the company who made a given app may only be *indirectly* involved in the act of sharing data, if the relevant functionality that collects and disseminates user data is implemented within third-party SDKs. For similar reasons, personal data being shared by an app may be sent directly to third parties, and will in many cases never touch the back-end systems of the company who made the app.

To give a concrete example, we have observed that the Grindr app communicates extensively with MoPub, who is one of their advertising partners, and also that the app contains MoPub's SDK. When our report thus states that the Grindr app sends specific information to MoPub, we mean that the Grindr app transmits this information directly from our test device to MoPub's servers. We do not conclude whether the data transmission is handled by parts of the app created by Grindr, entirely within MoPub's SDK, or somewhere in between. We also do not imply that any of the information is sent to or processed by Grindr's own back-end.

[4] See e.g. https://support.vungle.com/hc/en-us/articles/360002922871 for an example of vendor documentation on how to integrate an advertising SDK in an app. While we have not looked at the details at how SDKs such as Vungle's have been integrated in the app we tested, the documentation does reveal intriguing details, such as the fact that advertising ID is shared unless explicitly disabled, and that Vungle recommends that application publishers handle GDPR consent themselves

1.4 Structure of the report

The report consists of five main parts, following a top-down or pyramidal structure.

1. Chapter 1(the current chapter) describes the overall context and structure of the report
2. Chapter 2 provides aggregated information about the report findings
3. Chapter 3 provides detailed information about the technical findings
4. Chapter 4 describes the technical testing lab, setup, and methodology
5. Chapter 5 provides information about the project itself

Additional information is supplied in the appendices.

1.5 Acknowledgements

mnemonic would like to thank Gro Mette Moen, Ailo Krogh Ravna, and Finn Myrstad of the Norwegian Consumer Council for taking initiative to the project, coordinating activities across the project teams and participants, and for many fruitful discussions about the directions and implications of the work.

mnemonic would like to thank Wolfie Christl of Cracked Labs and Zach Edwards of Victory Medium for significant contributions to our understanding of the mobile advertising ecosystem, assistance with reviewing and interpreting parts of the data (particularly relating to real-time bidding and ad mediation), as well as useful discussions and feedback on the draft report.

Finally, mnemonic would like to thank domain experts from the privacy NGO noyb for useful discussions on the impact and interpretation of some of the findings.

2 Summary of findings

2.1 Scenarios and problem areas

In advance of the investigation, we have defined some specific scenarios that we wanted to understand better.

The privacy policy for a typical mobile app will often contain information about data sharing with advertising partners and service providers, but rarely contains much information about who those parties are, or precisely what data they get. An immediate observation is that it can be quite dynamic. While privacy policies are quite stable and have a low rate of change, the third parties receiving data may change more frequently, and even be chosen dynamically, without being known in advance. From a consumer perspective, it is challenging to find out who and how many of these parties are present. This makes it difficult to take control of one’s digital footprint. Wide distribution also increases the chances that something will leak.

- **Scenario**: Identify the third parties that receive data from our test device

Because of this, it is difficult for the user to fully understand the significance of such a privacy policy, and what personal data is actually being shared with whom. Also, information in the privacy policy will not be able to make the user fully aware of the consequences of personal data being shared with third-parties. It is not given that a user allowing an app to access the GPS on their device, will realize that the GPS data is potentially being collected 24/7, also when the app is not in use, and sent to third parties that you do not know about. Based on GPS location information alone, it is generally possible to identify individuals[5], based on their daily movement patterns over a few days.

- **Scenario**: Analyse the amount, frequency, and granularity of data collection

Turning the question on its head, it is even harder for the user to evaluate the implications of data collection when the same third parties receive data from multiple apps. This has been a common pattern during the test, and makes it possible to flesh out a user profile using pieces from multiple sources. We have even seen apps sharing a complete list of installed apps on the device, giving away a lot of information about the user’s interests. From a user perspective, the collection and correlation of data from multiple apps is quite opaque, and it is difficult to get a good picture of.

- **Scenario**: Illustrate third parties receive data from multiple apps

The effectiveness of privacy controls on Android is also an interesting topic. Using the Android advertising ID[6] provides advertising companies a unique device identifier for advertising and tracking, which can be used to correlate data from multiple sources. Privacy settings to control the advertising ID are buried deep within Android system settings. While it is possible to reset it

[5] For a recent example, see the New York Times’ investigation “*One Nation, Tracked*” from December 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
[6] Developer documentation for the Android advertising ID: http://www.androiddocs.com/google/play-services/id.html

manually to a new random value, it is not possible to remove or redact the advertising ID completely[7].

There is an option in the Android system settings to opt out of targeted advertising based on the advertising ID, but this mechanism appears to be largely trust-based, as it requires the app developers to actively check for and honour an opt-out, rather than supporting the opt-out natively in the platform. At the same time, end users have no way to evaluate whether a given app is respecting Android’s privacy controls, and may believe that the control is effective even if they are not.

- **Scenario**: Review the effectiveness of built-in privacy controls on targeted advertising and data collection

It is worth pointing out Google’s dual role within the Android ecosystem, as on one hand they are the company who controls the Android platform, the largest mobile platform in the market, and on the other hand they are one of the dominant online advertising companies.

2.2 Summary of findings per app

Table 2 gives a summary of the main findings in the test for each app. All apps transmit data such as the Android advertising ID to multiple advertising companies, but with the exception of Wave Keyboard, all the apps share significantly more data. Some of the apps, particularly Perfect365 and Grindr, share user data with a very large number of third parties.

App	**Description**
Grindr	Sends a lot of user data, including GPS location, IP address, gender, and age, to a large variety of third parties including **AdColony, AppNexus (Xandr)**, **Bucksense**, **MoPub, OpenX**, **PubNative**, and **Smaato**. Uses **MoPub** for ad mediation. Sends user information including “relationship type” to **Braze**. See chapter 3.2
Perfect365	The user’s GPS location is shared with several parties, particularly with **Fysical**, who receives it very frequently. In general, shares data with a lot of third parties. During the initial test in July / August, the app resisted attempts to force stop (this behaviour was changed in September 2019). GPS position is sent unencrypted to **Receptiv (Verve).** See chapter 3.3

[7] This is in contrast with Apple’s iOS platform, where opting out of targeted advertising sets the device advertising identifier to 00000000-0000-0000-0000-000000000000, according to developer documentation from Apple: https://developer.apple.com/documentation/adsupport/asidentifiermanager. This gives iOS users an opportunity to out out from targeted advertising and data collection based on unique device identifiers, although tracking and correlation may still be possible by other means. There are no obvious technical reasons why Android does not implement a similar feature.

My Days	Sends a lot of information, including a full list of installed apps, to **Placed**, as well as GPS position and IP address. Sends GPS position and wifi access points to **Placer.io**, and GPS position to **Neura**. See chapter 3.4
OkCupid	Sends answers to personal questions and GPS location to **Braze**. Sends detailed device information to **AppsFlyer**, including sensor readings. See chapter 3.5
My Talking Tom 2	Sends the user's IP address to **Mobfox**, **Rubicon Project** and **PubNative**. See chapter 3.6
Muslim: Qibla Finder	Sends the user's IP address to **Appodeal**. See chapter 3.7
Tinder	Sends the user's GPS position and information about age, gender, and target gender to **LeanPlum** and **AppsFlyer**. See chapter 3.8
Clue	Sends the user's birth year to **Amplitude**, **Braze** and **Apptimize**. See chapter 3.9
Happn	Sends country, gender and age segment of the user to **Google**. See chapter 3.10
Wave Keyboard	mnemonic did not observe user data sent to third parties, beyond the device's Android advertising ID. See chapter 3.11

Table 2. Summary of findings per app

2.3 Statistics, facts, and figures

2.3.1 General information

mnemonic tested ten different Android apps. In total across all tests, we observed the apps sending more than **88.000** HTTP requests, communicating with at least **216** unique third-party domains (*.example.com), owned by at least **135** different companies within the advertising space. As expected, there was some variation in the amount and type of data sharing. **Perfect365** was a particular standout among the apps, communicating with **at least 72** such companies.

All ten apps were observed interacting with Google and Facebook services to various extents. Not all of this traffic is explicitly advertising-related. Because the test was carried out on the Android platform, some degree of interaction with Google services is to be expected. Similarly, some of the Facebook traffic is likely to be related to platform services, such as federated authentication.

While investigating the scope and reach Google’s and Facebook’s advertising services was not the main focus of our investigation, we have tried to point out obvious advertising traffic where we see it. In some cases, it is fairly clear what is going on. Nine of the apps have been observed sending the Android advertising ID to *graph.facebook.com*, and eight of apps have been found communicating with subdomains of *g.doubleclick.net*. Traffic volumes vary, with MyDays being a particularly frequent user of Google DoubleClick.

Other situations are more unclear, particularly for Google, where device information and sometimes also the advertising ID is sent to other Google-owned services such as *app-measurement.com* (used by 8 apps) or *crashlytics.com* (appears to be used by all 10 apps). In two situations we even saw that the advertising ID was received in responses **from** Google, without being present in the corresponding request, clearly signifying that Google was able to identify the device.

2.3.2 Overall data sharing

Table 3 gives an overview of the number of third parties that we have associated with each of the apps, broken down into the following categories:

- Domains: the number of unique domains (e.g. *.example.com) we observed traffic to from the app
- Advertising: the number of identified companies related to advertising
- Ad ID: the number of parties receiving the Android advertising ID
- GPS: the number of parties receiving exact GPS location
- IP/MAC: the number of parties receiving IP and/or MAC address
- User data: the number of parties receiving personal information about the end user, such as age and gender

App	Domains	Advertising	Ad ID	GPS	IP/MAC	User data
Grindr	53	36	18	11	4	7
Perfect365	99	72	16	7	2	0
MyDays	14	6	5	3	1	0
OkCupid	16	9	3	1	0	2
MyTom	25	11	8	0	3	0
Muslim	16	7	5	0	1	0
Tinder	16	7	5	2	0	3
Clue	9	6	4	0	0	3

Happn	17	6	2	0	0	1
Wave	12	4	4	0	0	0

Table 3. Overview of data sharing for each app

These are just a few of the "interesting" parameters that are being tracked. Other examples of data include device model, information about the hardware and display, device configuration, battery levels, locale settings, carrier, nearby wireless networks, and so on. These have proved more difficult to turn into reliable statistics, due to variability in both presentation and granularity.

We stress that these figures are *minimum* numbers, in the sense that the testing protocol as well as the sheer data volumes means that we may have been unable to identify or miss certain transmissions. Methodological factors are discussed further in Chapter 4.

2.3.3 Use of third party SDKs

Using SDKs (software development kits) provides a way for app developers to integrate third party code in their apps. In the case of mobile advertising, SDKs are often provided in order to facilitate communication between the apps and the advertising vendors. We have decompiled the source code for all the apps, in order to figure out which SDKs were present in the various apps. The presence and usage of SDKs in code gives us a good indication of companies that the app would be expected to communicate with. Table 4 lists the third party SDKs that were observed, based on our identification of the associated companies.

App name	# SDKs	Company with integrated SDK
Perfect365	25	Amazon Advertisement, AppLovin, AppMonet, AreaMetrics, Chocolate (Vdopia), Facebook Ads, Flurry, Fysical, Google Ads, Google Crashlytics, Google Firebase, Integral Ad Science, Kin Ecosystem, Moat, MoPub, Ogury Presage, OneAudience, Receptiv (Verve), Sense360, SerServ, Tap Research, Tencent, Unacast, Unity3d, Vungle
My Talking Tom 2	25	AdColony, AppLovin, AppsFlyer, ChartBoost, Facebook Ads, Fyber, Google Ads, InMobi, Integral Ad Services, IQ Zone, IronSource, Mintegral, Moat, Mopub, myTarget, Nexage, Ogury Presage, Outfit 7 Ads / Bee7, Smaato, Soomla, Superawesome Ads, Tapjoy, Unity3d, Vungle
MyDays	21	AdColony, Adincube, Amazon Advertisement, AppLovin, ChartBoost, Google Crashlytics, Facebook Ads, Google Ads, Google Firebase, InMobi, Integral Ad Services, Moat, MoPub, Neura, OneAudience, Placed, Placer.io, AdBuddiz, Startapp, Unity3d, Vungle
Muslim: Qibla Finder	20	AdColony, Amazon Advertisement, AppLovin, AppMetrica, AppNext, Appodeal, Facebook Ads, Google Ads, Google Firebase, InMobi, Integral Ad Science,

		Ironsource, Moat, MoPub, Nexage, StartApp, TapJoy, Unity3d, Vungle, Yandex
Grindr	18	AdColony, AppsFlyer, Braze/Appboy, Google Crashlytics, Facebook, Fyber, Google Firebase, OpenX, Inner Active, AdColony, Millennial Media, Moat, MoPub, OpenX, SafeDK, Smaato, Tencent, Vungle
Wave Keyboard	14	AppLovin, Avocarrot (Glispa), Chartboost, Facebook Ads, Flurry, Fyber, Google Ads, Google Crashlytics, Google Firebase, OneAudience, OneSignal, PubNative, Unity3d, Vungle
OkCupid	10	AppsFlyer, Braze/Appboy, Embrace, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, Kochava, MoPub, MParticle
Tinder	7	AppsFlyer, Branch, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, LeanPlum
Happn	7	Adjust, Braze/Appboy, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, Mopub
Clue	6	Adjust, Amplitude, Apptimize, Braze/Appboy, Google Crashlytics, Google Firebase

Table 4. List of third-party SDKs integrated in the apps

It is important to note that not all parties identified with SDKs appeared to receive any data during our testing phase, and conversely, some parties received data without the use of a SDK (for example through mediation). The presence of a specific company’s SDK in an app only indicates a *potential* for interaction, and we have not attempted to reverse-engineer the usage of specific SDKs. We do not know the intents of the company including the SDK in their apps, nor the precise conditions necessary for it to be used.

To give an example, we found SDKs from myTarget and Yandex in the apps, but did not see traffic to these companies during testing. Since both of these companies mainly work with advertising within the Russian market, it is likely that we could have seen more traffic to these if we were testing from a location in Russia or Eastern Europe.

Figure 2 gives a graphical representation of third-party SDK usage, showing which SDKs were used by multiple apps. As we see, Google and Facebook are major players, although there is also significant diversity.

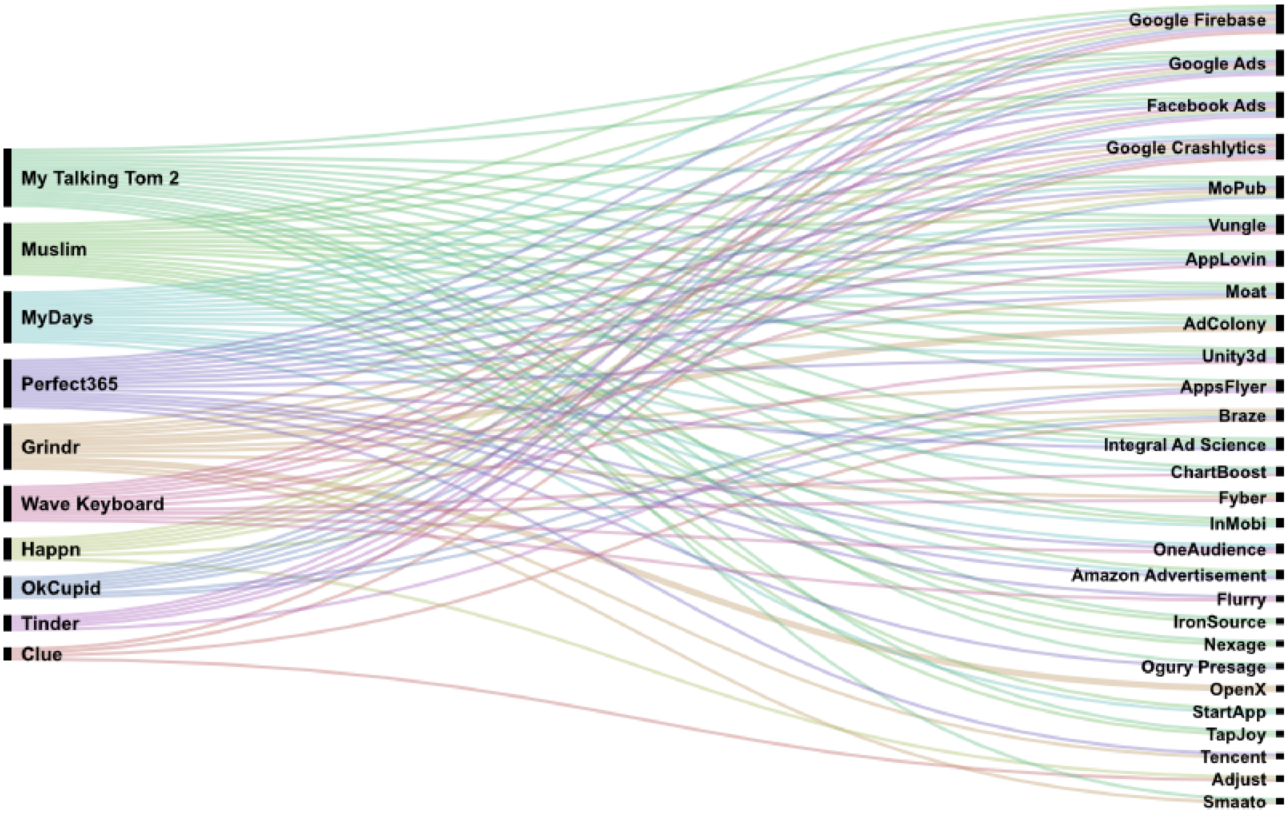


Figure 2. Illustration of SDKs that were used by multiple apps

2.3.4 Commonly observed domains

Table 5 shows the most frequently observed third party domains during testing, with each of these receiving more than 400 requests from our test device. Some of these are well known advertising companies like Google. Others are quite obscure, and required a bit of sleuthing in order to identify which company operates a particular domain.

Domain name	Company
ads.mopub.com	MoPub (Twitter)
sdk-android.ad.smaato.net	Smaato
googleads.g.doubleclick.net	Google
api.pubnative.net	PubNative
grindr2-d.openx.net	OpenX
ap.lijit.com	Sovrn (Lijit)
my.mobfox.com	MobFox
s.amazon-adsystem.com	Amazon

p.rfihub.com	Zeta Global
data.adsrvr.org	The Trade Desk
pixel-us-east.rubiconproject.com	Rubicon Project
pagead2.googlesyndication.com	Google
secure.adnxs.com	AppNexus (Xandr, AT&T)
impression-europe.liftoff.io	Liftoff
x.appbaqend.com	Appodeal
ic.tynt.com	Tynt (33across)
api.beaconsinspace.com	Fysical
contextual.media.net	Media.net
a.applovin.com	AppLovin
wapi.theneura.com	Neura

Table 5. Most frequently observed third parties, in terms of number of requests sent by the apps, as identified by mnemonic

Please note that the data in Table 5 is not a representative sample of third parties encountered during testing, because we spent more time testing some apps than others. This necessarily skewed the data towards the advertising companies present in those apps. Nevertheless, the table illustrates the heterogeneity of the ecosystem. While big players such as Twitter, Google and Amazon are certainly present, there are a lot of smaller fishes in the water. In Appendix B, we provide a full list of third-party companies within the advertising sector, that were identified as being present in our data.

3 Detailed findings and observations

3.1 Introduction

The chapter presents the detailed technical findings and mnemonic's initial analysis. We have organized the chapter based on the findings that have been made for each app.

Two different perspectives are relevant for the review:

1. App-centric perspective: To which parties does app X transmit data?
2. Actor-centric perspective: Which apps send data to the same party Y, and how do the actors act in concert regarding data collection?

In terms of understanding the advertising ecosystem, the second perspective is arguably just as useful as the first, allowing us to focus on the data elements that are collected and may be correlated across multiple sources. However, for the sake of readability, we have mainly stuck to the first perspective in this report.

A general observation from the project, is that the overall data volumes are very large, and that it quickly becomes difficult to analyze and present the data in an accessible way. mnemonic has in total collected a total of 88 155 data transmissions (number of requests), across 216 different third-party domains, generating on the order of 1 679 MB of raw log data.

It adds to the complexity that the "interesting" data may appear in several different places within the raw HTTP requests and responses, rather than in fixed locations, and that data may be encoded in various ways. Managing this dataset, understanding the interactions present, and analyzing the implications, has been a significant and time-consuming part of the project.

Our advice to future researchers is to stake out a data management plan early on, in order to handle this in a scalable way, preferably storing log data directly into an easily accessible format for dissemination and analysis within the team.

3.1.1 Data elements

During testing, we have looked for a wide variety of "interesting" data elements being transmitted. A quick summary of some of the most important types is as follows:

Data element	Description
Advertising ID	Google's Android advertising ID[9] provides a user-specific, unique, resettable ID to be used for advertising. During testing, our Advertising ID has been **`52d0d5c2-e923-4b1b-bd67-d3b225795edb`.** The advertising ID provides **linkability**, in the sense that it gives advertisers an easy way to connect the dots between multiple apps or multiple sources.

[9] http://www.androiddocs.com/google/play-services/id.html

IMEI	The International Mobile Equipment Identity (IMEI), also referred to device ID, is a unique device identifier. As opposed to previous research on mobile privacy, **we did not** observe the test device IMEI in data traffic. Since Android 10, access to the IMEI has required a specific permission, READ_PRIVILEGED_PHONE_STATE, as a privacy safeguard. This is a possible reason why we do not see it being tracked. On the other hand, we used an older version of Android, and were thus somewhat surprised not to see it.
IP address	The user's IP address can be used to determine approximate location, and in many cases identify an individual or small group of people. In some cases, it can also be used to track users across multiple devices, for example on a home network. During testing, the device IP address was fixed as **94.127.56.71**.
MAC address	The device's MAC address, which can be used to identify the device. Since Android 6.0[10], access to this parameter has been restricted by the operating system as a privacy safeguard. When an app tries to read the MAC address, a static value of 02:00:00:00:00:00 is given. As opposed to the IMEI, we did observe some instances of the MAC address being collected.
GPS location	The user's exact latitude and longitude. GPS location data can readily be used to identify people, as well as their activities and interests, based on daily habits (where they work, where they live, where they go about their day). It can also be used to infer relationships between people, based on whether they are at the same location, for how long, and how frequently. Because of this, it is very hard to properly anonymize a location dataset, and it may be used to infer information that could be considered highly personal, including political and religious views, as well as health. Throughout testing, the true GPS position of the test device was (**62.xxx N, 6.yyy E**). Please note that exact location data has been manually redacted or truncated throughout this report. These redactions are clearly marked.
Device information	Information about the device hardware, operating system version, screen resolution, language settings, battery status, et cetera. Device information collected ranges widely, from general information (which may be useful for compatibility or UX reasons) to detailed information about device settings, sensors, and hardware. Fine-grained device information may be used to "fingerprint" and identify a specific device. Parameters such as battery status can be valuable information for behavioural profiling, as people's behaviour may change, for example if they are stressed due to low battery levels.
Device configuration	Settings such as language, timezone, carrier, and cell information helps indicate the user's location, and possibly also other attributes.

[10] https://developer.android.com/about/versions/marshmallow/android-6.0-changes

Wifi networks	May be used to identify location, typically by comparing the list of accessible networks to precomputed databases of known networks and locations. Information such as street address and company names is also often present in SSID names, and may be used to infer additional detail. Some wireless network information has been manually redacted by mnemonic.
App name	Information about which app is making the request, typically including the app bundle id (e.g. `com.grindrapp.android`) and possibly version number. Given an app identifier, it is usually possible to attach more metadata, such as category or keywords. This is sometimes done explicitly as well.
Account information	User account ID or number for a particular app, or within a certain advertising ecosystem, potentially linkable with other data from that app or within the same ecosystem
User data	In some situations, we have seen specific user data from within the applications, such as age or gender, being transmitted

Table 6. List of typical data elements collected

In general, the combination of diverse data elements is more powerful than individual attributes. An advertising network that is able to combine geolocation with user data harvested across multiple apps, over time, will be in a good position to build a very precise profile of that user.

3.1.2 Interaction types

We have seen (at least) three different interaction types between the apps and third parties:

1. API integration: the apps call a defined service interface (API) on a third party domain, sending structured data. Data is typically sent either as HTTP GET parameters, or as a HTTP POST containing a JSON object
2. Complex flows: the apps call a ***sequence*** of third party endpoints, often involving multiple domains. The sequence is orchestrated either using HTTP 302 redirects or client-side scripting.
3. As part of resource fetch: we have also seen that user data, particularly the advertising ID, but sometimes also additional information, is sent as parameters when getting a resource such as a banner ad or video.
4. Tracking pixels: we have seen multiple requests to "tracking pixels"[11] in our network logs. Such requests sometimes transfer additional data as well.

This report mainly documents interactions either by showing the raw HTTP request, or a formatted presentation of the payload.

[11] Google's pixel *https://cm.g.doubleclick.net/pixel* is a well known, but hardly unique, example

3.2 Grindr

Grindr is a well-known social networking and dating app, focusing particularly on users in the gay, bisexual, transgender, and queer communities. The service is location based, allowing users to contact and locate other users nearby. According to Wikipedia, the app had more than 27 million users in 2017, and is available in 192 countries.

Our tests of Grindr primarily took place on July 8th, 15th, and 31st, as well as August 7th 2019. Additional verification and re-tests was done on September 23rd, November 8th and 13th, and finally with a newer Grindr version on December 25th and 31st 2019.

Notable prior research on Grindr includes analysis carried out by the Norwegian research institute SINTEF in the spring of 2018, in collaboration with Swedish Television (SVT). Their work[12] revealed that Grindr shared sensitive personal information from the app with multiple third parties. Notably, the app was found to be sharing the user's HIV status with two of Grindr's partners, Localytics and Apptimize. After a public outcry about these findings, changes were made both to the app and its privacy policy. It is worth noting that we did not see data transmissions from the Grindr app to Localytics nor Apptimize during our test.

When running the Grindr app in our test lab, the app would warn us about the connection being insecure, and closing. This is due to security measures within the app detecting our testing infrastructure, and interpreting it as dangerous. We were able to bypass this restriction during testing, but the workaround made us unable to catch any data being transmitted while the app was being started, leading to potential false negatives in the results. During our retest in November 2019, we managed to develop an alternate bypass mechanism to obtain more data.

The combination of precise and updated GPS location and information about (likely) the sexual orientation of the user that could be inferred from use of the Grindr app, seems particularly problematic in terms of misuse potential.

3.2.1 Grindr's use of MoPub for ad mediation

When analysing the traffic being sent from the Grindr app, we noticed that MoPub shows up very frequently. The MoPub SDK is integrated in the app, and MoPub is also specifically named in Grindr's privacy policy[13] as one of their main advertising parties. Our observation is that MoPub serves as advertising mediator, dynamically orchestrating traffic between Grindr and multiple third party advertising networks.

A direct implication of this, is that the type of third parties receiving data from the Grindr app, and the precise data elements that they receive, may to a large extent be controlled through MoPub, and may vary or change over time. During repeated testing, it appears that the main parties we encounter are "stably" present over time, but that new or different parties sometimes appear.

The mediation process we have observed consists of three main steps:

[12] https://github.com/SINTEF-9012/grindr-privacy-leaks

[13] https://www.grindr.com/privacy-policy/

1. The Grindr app sends an ad request to MoPub. Ad requests are sent frequently, typically several times per minute when using the app. In we show an example request from our logs. The request contains multiple data elements, including the user’s exact GPS position, Android advertising ID, app name, and finally the user’s gender and age.

```
POST /m/ad HTTP/1.1
accept-language: en-us
user-agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36
Content-Type: application/json; charset=UTF-8
Host: ads.mopub.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 600

{
  "ll":"REDACTED,REDACTED",
  "vv":"0",
  "nv":"5.4.1",
  "dn":"LGE,Nexus 5X,bullhead",
  "sc":"2.625",
  "consented_vendor_list_version":"0",
  "current_consent_status":"explicit_yes",
  "consented_privacy_policy_version":"0",
  "id":"agltb3B1Yi1pbmNyDQsSBFNpdGUYtebmEgw",
  "udid":"ifa:52d0d5c2-e923-4b1b-bd67-d3b225795edb",
  "bundle":"com.grindrapp.android",
  "llsdk":"1",
  "gdpr_applies":"1",
  "lla":"51",
  "mr":"1",
  "llf":"138693",
  "h":"1920",
  "force_gdpr_applies":"0",
  "dnt":"0",
  "android_perms_ext_storage":"0",
  "o":"p",
  "q":"app_version:5.12.1",
  "ct":"2",
  "av":"5.12.1",
  "v":"6",
  "w":"1080",
  "z":"+0200",
  "user_data_q":"m_gender:m,m_age:34"
}
```

Table 7. Initial request from the Grindr app to MoPub. The request body, formatted and trimmed for legibility, contains GPS position, device advertising ID, and user data (highlighted)

2. MoPub responds with a JSON object containing HTML content, which the Grindr app executes within a WebView. The data received from MoPub includes a specification of which endpoint to call next, and what data to send there. The specific response to the request shown in step 1 is given in Table 8. As we can see from the response, it instructs the app to request an ad from AppNexus (adnxs.com) containing the name of the app (“`appid=com.grindrapp.android`”), ip-address (“`ip=94.127.56.71`”), and advertising ID (“`idfa=52d0d5c2-e923-4b1b-bd67-d3b225795edb`”).

```
HTTP/1.1 200 OK
connection: close
Content-Length: 6006
content-security-policy: script-src 'self' *.mopub.com
mopub.com;connect-src 'self' *.mopub.com mopub.com;object-src 'none'
content-type: application/json; charset=utf-8
date: Mon, 08 Jul 2019 11:10:52 GMT
server: tsa_b
strict-transport-security: max-age=631138519
x-connection-hash: ee5a0af43191a623b55a068a0fca720d
x-response-time: 304
x-tsa-request-body-time: 1

{"ad-responses":[{"content":" <!DOCTYPE html> <html> <head>  <!-- Adgroup is
95a2ae2f559d4cbdbc77d106ef5b58f5 -->  <meta name=\"viewport\" content=\"widt
h=device-width, initial-scale=1.0, user-scalable=no\">  <style type='text/cs
s'> .mp_center { position: fixed; top: 50%; left: 50%; margin-left: -160px !
important; margin-top: -25px !important; } </style>  <script type=\"text/jav
ascript\"> function mopubFinishLoad(){ setTimeout(function() { window.locati
on = 'mopub://finishLoad'; }, 0); } </script>  <script type=\"text/javascrip
t\"> function webviewDidClose(){ if (typeof webviewDidCloseHelper == 'functi
on') { webviewDidCloseHelper(); } } function webviewDidAppear(){  if(typeof
trackImpressionHelper == 'function') { trackImpressionHelper(); }  if(typeof
webviewDidAppearHelper == 'function') { webviewDidAppearHelper(); } } window
.addEventListener(\"load\", function() { var links = document.getElementsByT
agName('a'); for(var i=0; i < links.length; i++) { links[i].setAttribute('ta
rget','_blank'); } }, false);  </script>  </head> <body style=\"margin:0;pad
ding:0;\"> <!-- BEGIN JS TAG - Android Banner 320x50 ($1.25) < - DO NOT MODI
FY -->\n<SCRIPT SRC=\"https://secure.adnxs.com/ttj?id=15627015&cb=1562584252
568\n&appid=com.grindrapp.android&ip=94.127.56.71&idfa=52d0d5c2-e923-4b1b-bd
67-d3b225795edb&psa=0\" TYPE=\"text/javascript\"></SCRIPT>\n<!-- END TAG -->
```

(remainder of response omitted for legibility)

Table 8. Response (excerpted) from MoPub to the request in Table 7, showing how MoPub instructs the app to request a resource from secure.adnxs.com (highlighted). Parameters sent to AppNexus includes the app bundle name, external IP address, and device advertising ID

3. After a few seconds, the Grindr app makes a second request, this time to the AppNexus endpoint specified by MoPub, and containing the parameters that were specified in the previous response. The corresponding request is shown in Table 9, and we can see that it matches the structure and format previously received from MoPub. While we have not determined it conclusively, it seems likely that this request is handled mainly or completely within MoPub’s SDK as part of the app

```
GET /ttj?id=15627015&cb=1562584252568&appid=com.grindrapp.android&ip=
94.127.56.71&idfa=52d0d5c2-e923-4b1b-bd67-d3b225795edb&psa=0 HTTP/1.1
Host: secure.adnxs.com
Connection: close
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36
Accept: */*
Referer: https://ads.mopub.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
X-Requested-With: com.grindrapp.android
```

Table 9. Request from the Grindr app to AppNexus, containing parameters previously specified by MoPub

In this specific example, although we did not send our IP address to MoPub in step 1, the response from MoPub received in step 2 contains our IP address together with the Advertising ID, which is subsequently sent to AppNexus in step 3.

We have not been able to identify how MoPub receives and populates this IP address parameter. It could be data that they have previously associated with the device, it could be dynamically extracted from the network layer, or they might have received it through a back-end integration from an unknown party.

Figure 3 shows a schematic timeline indicating how data transmissions to third parties are mediated by MoPub, using two sets of interactions with AppNexus and Bucksense as examples.

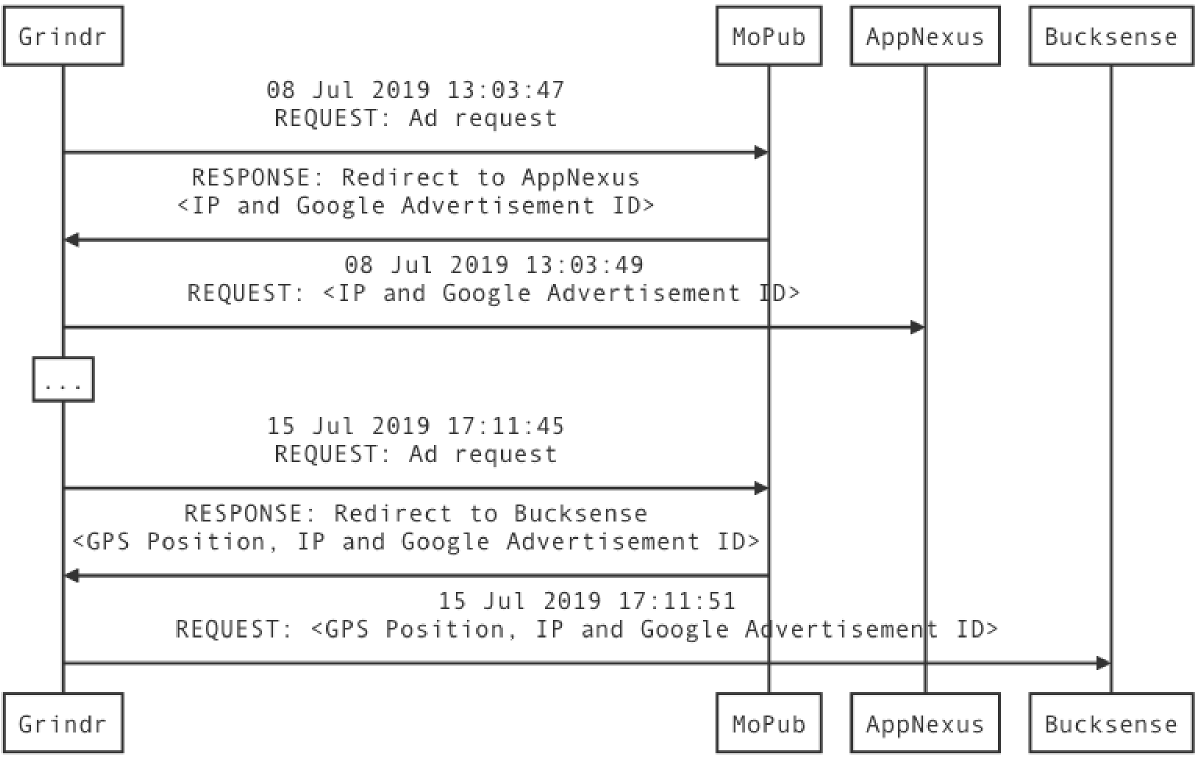

Grindr
MoPub
AppNexus
Bucksense
08 Jul 2019 13:03:47
REQUEST: Ad request
RESPONSE: Redirect to AppNexus
<IP and Google Advertisement ID>
08 Jul 2019 13:03:49
REQUEST: <IP and Google Advertisement ID>
...
15 Jul 2019 17:11:45
REQUEST: Ad request
RESPONSE: Redirect to Bucksense
<GPS Position, IP and Google Advertisement ID>
15 Jul 2019 17:11:51
REQUEST: <GPS Position, IP and Google Advertisement ID>
Grindr
MoPub
AppNexus
Bucksense

Figure 3. Sequence diagram showing data transmission between Grindr, MoPub, and third party advertising networks

During our testing, we saw ad traffic from Grindr to a variety of advertising networks being mediated via MoPub. The requests would contain different data and syntax, depending on which ad network was being used. We also identified metadata parameters indicating that MoPub was being used for mediation, e.g. by some requests containing a key/value parameter called `"mediation_network":"MoPub"`.

Whether a particular advertising networks is receiving data varies somewhat over time, due to the dynamic nature of mediation. When mnemonic did re-tests in September and November to confirm initial findings, several “new” third parties (Aarki, Adtelligent, Fyber, InMobi, Mars Video and Mobfox) were found in addition to the ones we had seen during initial testing. Table 10 gives an overview of all the parties where we observed traffic that was also associated with MoPub's mediation.

Third party	Host	Data elements
MoPub	ads.mopub.com	App name, advertising ID, GPS location, gender, age, device information
AppNexus (Xandr)	secure.adnxs.com	App name, advertising ID, IP address
OpenX[14]	grindr2-d.openx.net	App name, advertising ID, GPS location, gender, keywords
Bucksense	j.bksn.se retargeting.bkswin.com	App name, advertising ID, GPS location, IP address
Liftoff	adexp.liftoff.io	App name, advertising ID, location(inexact)[15], device configuration
PubNative[16]	api.pubnative.net	App name, advertising ID, GPS location,
Aarki	Multiple subdomains of *.aarki.net	App name, advertising ID, year of birth, gender
Adtelligent (Vertamedia)	*.vertamedia.com	App name, advertising ID, location (inexact), IP address
InMobi	js.w.inmobi.com	App name, advertising ID, GPS location
Fyber (Inner-Active)	wv.inner-active.mobi	App name, advertising ID, GPS location, gender, age
Mars Video	vpaid.mars.video	App name, advertising ID, IP address

[14] During testing, we observed two apparently distinct integration modes in the traffic from the Grindr app to OpenX. One of these can be conclusively linked to MoPub mediation, but we cannot rule out that there is another integration mechanism in play as well. As Grindr was found to contain OpenX's SDK, this could be a possible cause of the traffic that we observed.

[15] The location reported to LiftOff appears to be based on IP address or other metadata, rather than the GPS, as it shows an incorrect location in Oslo even though the device location was not near Oslo

[16] See https://developers.pubnative.net/docs/mopub-ad-tag-integration for the vendor's documentation on how PubNative supports integration with the MoPub SDK

Mobfox	my.mobfox.com	App name, advertising ID, GPS location

Table 10. Overview of third-party companies receiving data from the Grindr app that appear to be part of MoPub's mediation network

In the traffic to OpenX, we made two additional observations that are worth highlighting: it transmits additional keywords related to the app, and data indicating that user data is being transmitted as part of a real-time bidding process. Table 11 shows sample request parameters sent to OpenX from the July 8th testing.

```
ai=de4c8e07-eb43-4e4c-8d1c-cdf748b63f7f&
o=709976558&callback=OX_709976558&
auid=538352635&
lat=62.redacted&
lon=6.redacted&
lt=1&
app.name=Grindr - Gay chat, meet & date&
sp=js&
app.bundle=com.grindrapp.android&
url=https://play.google.com/store/apps/details?id=com.grindrapp.andro
id&
did.adid=52d0d5c2-e923-4b1b-bd67-d3b225795edb&
did.adid.enabled=true&
dims=0x0&
adxy=0,0&
openrtb={
    "app":{
        "domain":"www.grindr.com",
        "privacypolicy":1,
        "paid":0,
        "keywords":"Social Network, Gay, Bi, Bi-curious, Chat,
Dating, Nearby",
        "publisher":{"name":"Grindr, LLC","domain":"grindr.com"},
        "storeurl":"https://play.google.com/store/apps/details?id=co
m.grindrapp.android"},
    "user":{"gender":"m"}}&
res=412x732x24&
plg=pm&
ch=UTF-8&
tz=-120&
ws=0x0&
ifr=0&
tws=0x0&
vmt=1&
sd=215&
mt=1&
nl=134,103,86,360,444&
ul=180,140,126,389,479
```

Table 11. Request parameters sent from the Grindr app to OpenX, as part of a MoPub mediation flow

The above parameters were sent to the grindr2-d.openx.net/ma/1.0/acj endpoint, signifying a mobile ad request to OpenX's asynchronous chain JSON endpoint. Additional information about the OpenRTB protocol[17] and request parameter structure[18] is available, although mnemonic has not investigated these areas in further depth.

While OpenX appears to support an *optional* consent parameter based on the IAB consent string format, this was not observed during the test.

3.2.2 Direct interactions between Grindr and other third parties

In addition to the third party traffic that is orchestrated by MoPub, we also found multiple other third-party integrations that we did not link to MoPub. The observed interactions are summarized in Table 12.

Third party	Host	Data elements
Smaato	sdk-android.ad.smaato.net	App name, advertising ID, GPS location, some device information and configuration, gender, age
AdColony[19]	Multiple subdomains of *.adcolony.com	App name, advertising ID, GPS location, device information including permissions, device configuration, gender, Grindr user ID
AppsFlyer	t.appsflyer.com	App name, advertising ID, Grindr user ID, Braze user ID, device information, device configuration (including mobile operator)
Braze	gaspra.iad-03.braze.com	App name, GPS location, Grindr user ID, Braze user ID, app usage (GUI events), relationship type
Crashlytics[20]	e.crashlytics.com	Grindr user ID, possibly other data
Facebook	graph.facebook.com	App name, advertising ID
SafeDK	api.safedk.com	App name, device information
Google	app-measurement.com	App name, advertising ID

[17] Official OpenRTB documentation at https://www.iab.com/guidelines/real-time-bidding-rtb-project/

[18] OpenX provides developer documentation on their request API, information about OpenRTB is available at: https://docs.openx.com/Content/developers/ad_request_api/openrtb_parameters.html and https://docs.openx.com/Content/developers/ad_request_api/openrtb_fields_passed_by_publishers.html

[19] It is unclear to us whether all AdColony traffic is part of MoPub mediation, as the traffic follows a different pattern than the one described in Chapter 3.2.1. Our main evidence for an association is an explicit key/value pair which is present in some of the requests to AdColony: `"mediation_network": "mopub"`. This suggests a link between the two, even if the mechanism of interaction is different

[20] Crashlytics is included for the sake of completeness, as personal data is sometimes captured and transmitted (either by design or inadvertently) as part of technical diagnostics

Vungle	api.vungle.com	App name, advertising ID, GPS location, device information, device configuration

Table 12. Third parties receiving data directly from the Grindr app

A few additional parties were seen to receive the advertising ID and app name a small number of times, particularly during the retest sessions in September and November. These include **PubMatic**, **Cedato**, and **Improve Digital**. Because of the rarity of these interactions, it has been difficult to confirm or reproduce these findings.

There are significant differences in the relative traffics volumes observed, with Smaato collecting an order of magnitude more requests than any of the others, and Vungle appearing only intermittently in our data.

It is also worth highlighting the parties receiving data related to the individual user:

- Advertising ID was sent to all third parties mentioned, **except** Braze, Crashlytics, and SafeDK
- IP address was sent as an explicit parameter to **AppNexus (Xandr)**, **Bucksense**, **Mars Video**, and **Adtelligent**
- GPS location was sent to **OpenX**, **Bucksense, AdColony**, **PubNative, MobFox**, **InMobi**, **Fyber (Inner Active), MoPub**, **Smaato**, **Braze**, and **Vungle**
- User data such as gender or age was shared with **OpenX**, **AdColony**, **Aarki**, **MoPub**, **Fyber (Inner Active)**, and **Smaato**

Furthermore, we saw that information about what type of relationship the user is looking for (dates, friends, relationship, etc.) was sent to **Braze**, as well as information about page views and GUI activity within the app.

3.2.3 A note on gender in Grindr

During our tests, we saw multiple parties that appeared to be receiving the user’s gender in application data broadcast by the Grindr app: **OpenX**, **AdColony**, **Aarki**, **Fyber (Inner Active)**, **Smaato**, and **MoPub**. However, when we tried to change the gender setting within the app, the changes did not appear to reflect in the value that is being sent to these companies.

This is as opposed to the age / date of birth parameter, which is also shared with multiple parties, and does change based on what we set in the user’s profile settings.

The observed behaviour may be a bug (or feature) in the particular version of the Grindr app, a bug in the advertising networks’ code, or a legacy feature that has been discontinued. Based on what we see in the traffic, it **appears to us** like the intent has been to capture and transmit the user’s gender, even though it does not work properly. However, we are not able to conclude on this. From a demographic perspective, we believe that a majority of Grindr’s users are likely to be male, although this is a coarse generalisation.

3.2.4 Traffic from Grindr to Smaato, and use of the IAB consent string

After MoPub, Smaato received the largest amount of traffic from Grindr. For example, during two short tests on July 8th, Smaato received 92 requests from the app in less than ½ hour of testing with the app. Table 13 shows the parameters sent in a typical request to Smaato.

```
gender=m&
modifyRM=true&
apiver=600&
format=display&
adspace=130573042&
gdpr_consent=BOjXn4OOjXn4ODHABBktBy-
AAAAU4AAABAAAAAAAQAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAA&
gps=62.redacted%2C6.redacted&
secure=true&
mraidver=2&
gdpr=1&
extensions=moat&
coppa=0&
googleadid=52d0d5c2-e923-4b1b-bd67-d3b225795edb&
googlednt=0&
client=sdkandroid_9-1-2&
connection=wifi&pub=1100000436&
lang=en-US&
dimension=MEDRECT&
bundle=com.grindrapp.android&
age=34&
mediationversion=2&
devicemodel=Nexus+5X
```

Table 13. Typical request parameters sent from the Grindr app to Smaato

The gdpr_consent parameter requires additional interpretation. Interactive Advertising Bureau (IAB) has defined a so-called consent framework[21] for GDPR, and it is this framework that is used to represent and encode the parameter. It is worth pointing out that we have not seen the consent framework used anywhere else during our tests.

The consent string that we see being sent to Smaato, is a binary representation that has been base64-encoded for transmission. We can decode the contents and review the consent parameters that are being sent to Smaato, this is shown in Table 14.

```
{
  "cookieVersion": 1,
  "created": "2019-07-08T09:27:55.000Z",
  "lastUpdated": "2019-07-08T09:27:55.000Z",
  "cmpId": 199,
  "cmpVersion": 1,
  "consentScreen": 1,
  "consentLanguage": "en",
  "vendorListVersion": 114,
```

[21] See https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/Consent%20string%20and%20vendor%20list%20formats%20v1.1%20Final.md

```
  "purposeIdBitString": "111110000000000000000000",
  "maxVendorId": 334,
  "isRange": false,
  "vendorIdBitString":
"00000000000000000000000010000000000000000000000000000000000000000000
100000000000010000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000100000000000000000000000"
}
```

Table 14. Example of IAB consent string sent from the Grindr app to Smaato

The `purposeId` bitfield consists of five 1s, which correspond to the following purposes:

1. Information storage and access
2. Personalisation
3. Ad selection, delivery, reporting
4. Content selection, delivery, reporting
5. Measurement

The `vendorIdBitString` contains the admissible vendors according to the vendor list[22], in version 1 of the framework. Based on the positions of the 1s in the bitmap, we identify vendor 25, 69, 82, and 311 from the list. These are, respectively, **Oath (EMEA), OpenX**, **Smaato, Inc.**, and **Mobfox US LLC**. We have not looked any further into possible collaboration between these parties.

```
{"id":25,"name":"Oath (EMEA)
Limited","purposeIds":[1,2],"legIntPurposeIds":[3,5],"featureIds":[1,2,3],"p
olicyUrl":"https://policies.oath.com/ie/en/oath/privacy/index.html"}

{"id":69,"name":"OpenX","purposeIds":[1,2,3],"legIntPurposeIds":[],"featureI
ds":[1,2,3],"policyUrl":"https://www.openx.com/legal/privacy-policy/"}

{"id":82,"name":"Smaato,
Inc.","purposeIds":[1,2,3,4,5],"legIntPurposeIds":[],"featureIds":[3],"polic
yUrl":"https://www.smaato.com/privacy/"}

{"id":311,"name":"Mobfox US
LLC","purposeIds":[1,2,3,4,5],"legIntPurposeIds":[],"featureIds":[3],"policy
Url":"https://www.mobfox.com/privacy-policy/"}
```

Table 15. Excerpt of Consensu’s vendor list used in the consent string

3.2.5 Traffic from Grindr to Braze

The Grindr app sends data to Braze every few minutes when the app is in use. A variety of data is being shared using an endpoint at gaspra.iad-03.braze.com/api/v3/data.

[22] Refer to the vendor list published at https://vendorlist.consensu.org/vendorlist.json

Some of the messages sent from Grindr to Braze are of particular interest, because they show GUI activity and the type of relationship the user is looking for, which is not shared anywhere else. A few examples are given below, highlighting some of the interesting parameters observed.

```
{"app_version":"5.12.1","device_id":"cd3f91a9-a12e-48fd-888b-db8aca73
7d46","time":1562584826,"api_key":"3fe66e8b-3937-48d8-8f84-a622d8a777
f7","sdk_version":"3.2.1","events":[{"name":"cc","data":{"ids":["5c81
776ca12f740d64c1c5d0"]},"time":1.562584807426E9,"user_id":"233335973"
,"session_id":"be0dbbab-ab9e-4c0b-9440-29670f3bc3dd"},{"name":"ce","d
ata":{"n":"clicked_newsfeed_card","p":{"message_id":"welcome_message_
english"}},"time":1.562584807426E9,"user_id":"233335973","session_id"
:"be0dbbab-ab9e-4c0b-9440-29670f3bc3dd"},{"name":"si","data":{"trigge
r_ids":["NWM3ZDk4M2JhMTJmNzQzNTEzNjljZmVlXyRfY2MmbXMmbXY9NWM3ZDk4M2Nh
MTJmNzQzNTEzNjljZmY0JnBpPWNtcCZ1aWQ="]},"time":1.562584807551E9,"user
_id":"233335973","session_id":"be0dbbab-ab9e-4c0b-9440-29670f3bc3dd"}
,{"name":"i","data":{"n":"feed_displayed"},"time":1.5625848046E9,"use
r_id":"233335973","session_id":"be0dbbab-ab9e-4c0b-9440-29670f3bc3dd"
}]}
```

```
{"app_version":"5.12.2","device_id":"cd3f91a9-a12e-48fd-888b-db8aca73
7d46","time":1564571350,"api_key":"3fe66e8b-3937-48d8-8f84-a622d8a777
f7","sdk_version":"3.2.1","events":[{"name":"lr","data":{"latitude":6
2.redacted,"longitude":6.redacted,"altitude":0,"ll_accuracy":19.58699
9893188477},"time":1.564571290658E9,"user_id":"233335973","session_id
":"d40ce93d-034b-4151-94f6-9fbf561eeeb2"}]}
```

```
{"app_version":"5.12.2","device_id":"cd3f91a9-a12e-48fd-888b-db8aca73
7d46","time":1569222454,"api_key":"3fe66e8b-3937-48d8-8f84-a622d8a777
f7","sdk_version":"3.2.1","events":[{"name":"ce","data":{"n":"edit_pr
ofile_viewed"},"time":1.569222352402E9,"user_id":"233335973","session
_id":"74bab6b1-99c4-4471-8522-457ca0390280"},{"name":"set","data":{"k
ey":"looking_for","value":["3","4","6"]},"time":1.569222370549E9,"use
r_id":"233335973","session_id":"74bab6b1-99c4-4471-8522-457ca0390280"
}]}
```

Table 16. Examples of data sent from the Grindr app to Braze: app activity, GPS location, and type of relationship

The “`looking_for`” parameter in Braze data corresponds to the categories chosen by the user in the app:

2. Chat
3. Dates
4. Friends
5. Networking
6. Relationship
7. Right now

It is also worth noting that Braze uses its own device identifier (`device_id`) rather than the advertising ID. This identifier, **cd3f91a9-a12e-48fd-888b-db8aca737d46**, is also observed in traffic to **AppsFlyer** as `brazeCustomerId`.

3.3 Perfect365

Perfect365 is an app that can be used for virtual makeup on live pictures and saved images. It is widely associated with selfie-taking celebrities such as Kim Kardashian[23]. The app has a login function allowing you to create your own account, including information such as name and age.

The majority of testing was carried out on July 4th and 5th, July 9th, July 15th and August 7th, with additional verification on September 18th 2019.

3.3.1 General observations

When we started testing the app in July, we noticed that the app requested a wide range of permissions on the device. Most notably, it requests the GPS position as well as other location data such as wireless access point (wifi) information. This is worrying since the app does not seem to use the location for any app-specific use cases. The app also requested other interesting permissions, such as preventing the phone from going to sleep.

Perfect365 communicates with a **lot** of third parties, and is also quite persistent at collecting data. To give an example, the following 16 third parties were observed receiving the device's Android advertising ID (amongst other data), which is a good indication of advertising activity.

- Amazon: *.amazon-adsystem.com
- Chocolate (Vdopia): serve.vdopia.com
- Facebook: graph.facebook.com
- Fluxloop: uc-eu2.pinch.no
- Fyber: *.fyber.com
- Fysical: api.beaconsinspace.com
- Google: www.googleadservices.com
- InMobi (AerServ): ads.aerserv.com
- Inner-Active (acquired by Fyber): wv.inner-active.mobi
- Ogury Presage: *.presage.io
- Safegraph: api.safegraph.com
- Receptiv (Verve): mobile.mediabrix.com
- Unacast (?)[24]: improbability-dot-uc-h2g2.appspot.com
- Unity3d / Unity Ads: *.unityads.unity3d.com
- Vungle: api.vungle.com
- srv.dc-1.net (we have not determined which company owns this domain)

The device's advertising ID is also sent to Perfect365 directly, although it is unclear to us what the purpose of this is.

During testing in July and August, we noticed that it was not possible to "force stop" the app to prevent it from sending location information in the background. The app was constantly sending

[23] See e.g. https://www.seventeen.com/celebrity/news/a28985/this-is-why-kendall-kylie-jenners-selfies-always-look-so-flawless/

[24] We believe this host belongs to Unacast, but haven't been able to conclusively determine who owns this GCP subdomain. See Chapter 3.3.5 for additional info.

location information to third parties, several times per hour, regardless if the app was in active use or not.

Around the middle of September, the Perfect365 app was briefly removed from Google Play store. When the app returned in an updated version on or around September 18th, this behaviour was not observed again during a brief re-test.

When analysing data being transmitted from Perfect365 to third-parties, we also observed communications with a wide variety of hosts owned by consumer data aggregators or data brokers, including **Oracle** (bluekai.com), **Lotame** (crwdcntrl.net), **Dotomi/Publicis** (dotomi.com), **Adobe** (everesttech.net), **Nielsen** (exelator.com), **Quantcast** (quantserve.com), **Comscore** (scorecardresearch.com) and **33Across** (tynt.com). It was difficult to fully understand the purpose of these transmissions, since they generally either had an empty request body or contained parameters that we were not able to decode and interpret.

3.3.2 Location sharing from the Perfect365 app to third parties

The following third parties were observed receiving location data from the Perfect365 app.

- GPS location:
  - **Fysical** received the device’s GPS location in hundreds of requests to their api.beaconsinspace.com host, often several times per minute
  - The following parties have received GPS location data from the Perfect365 app, albeit less often: **Amazon**, **InMobi**, **Vungle**, **Receptiv (Verve)**, **Fyber (Inner Active)**, **Safegraph**
- The device’s IP address was sent to **srv.dc-1.net**, and (sporadically) to **GumGum** and **StackAdapt**

The transmissions to **Fysical** are interesting because of their high frequency. A typical example of a request sent on August 7th is given in Table 17 and Table 18.

```
POST /v1/batch HTTP/1.1
Authorization: Basic
MkY0NTY0RDI1OUVBNDM2QUE3NkRERjk4NTY1Q0RFMjk1NzdFRjFEMjk2MzI4Nzg5NTk5N
DU2OmNvbS5hcmNzb2Z0LnBlcmZlY3QzNjU=
bisData:
Content-Type: application/x-www-form-urlencoded
Accept: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: api.beaconsinspace.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 1685


(base64-encoded payload omitted; decoded version shown in Table 18)
```

Table 17. Request sent from the Perfect365 app to Fysical (beaconsinspace)

Decoding the base64-encoded payload, we see the following data:

```
country=en_US&
gpsBearing=0.0&
gpsLongitude=6.redacted&
userIdType=AUUID&
tz=Europe%2FOslo&
detect=gps&
language=en_US&
gpsAltitude=97.0&
appStateDetection=background&
manufacturer=LGE&
batteryState=charging&
userId2=52d0d5c2-e923-4b1b-bd67-d3b225795edb&
isBluetoothEnabled=0&
model=Nexus+5X&
brand=google&
gpsLatitude=62.redacted&
batteryLevel=0.77&
os=ANDROID+8.1.0&
creationTimeInEpochMillis=1565170511556&
userAgent=Dalvik%2F2.1.0+%28Linux%3B+U%3B+Android+8.1.0%3B+Nexus+5X+B
uild%2FOPM7.181205.001%29&
gpsSpeed=0.0&
eventType=gps&
userId=2cd17a45-b2a9-436c-a547-2a1b3cb961e9&
sdkVersion=2.1.4&
device=bullhead&
gpsHorizontalAccuracy=5.0&
userIdType2=ADID
```

Table 18. Decoded payload sent from the Perfect365 app to Fysical / beaconsinspace

The data transmission to **SafeGraph** also stood out, because it in addition to GPS data contained information about WiFi access points (SSID and BSSID), which can be used to triangulate location even in places with poor GPS reception, and inside buildings.

3.3.3 Vungle and the unknown GDPR consent

Data transmission to **Vungle** also stood out in the logs. We observed messages containing user location data, which also stated that the GDPR consent status was unknown. A request from Perfect365 to Vungle on July 4th is given as example.

```
POST /api/v5/ads HTTP/1.1
Vungle-Version: 5.2.0
User-Agent: VungleDroid/6.3.17
Content-Type: application/json
Content-Length: 1377
Host: api.vungle.com
Connection: close
Accept-Encoding: gzip, deflate

{"device":{"make":"LGE","model":"Nexus
5X","osv":"8.1.0","carrier":"","os":"android","w":1080,"h":1794,"ext"
:{"vungle":{"android":{"gaid":"52d0d5c2-e923-4b1b-bd67-
d3b225795edb","battery_level":1.0,"battery_state":"BATTERY_PLUGGED_US
B","battery_saver_enabled":0,"connection_type":"WIFI","connection_typ
e_detail":"WIFI","data_saver_status":"NOT_APPLICABLE","network_metere
d":0,"locale":"en_US","language":"en","time_zone":"Europe/Oslo","volu
me_level":0.53333336,"sound_enabled":1,"storage_bytes_available":6710
8864,"is_tv":false,"os_api_level":27,"is_sideload_enabled":false,"sd_
card_available":1,"os_name":"google/bullhead/bullhead:8.1.0/OPM7.1812
05.001/5080180:user/release-keys","vduid":"","location":{"accuracy":"
15.0","latitude":"62.redacted","longitude":"6.redacted","speed":"1.95
56328","timestamp":1562233761520}}}},"ua":"Mozilla/5.0 (Linux; Androi
d 8.1.0; Nexus 5X Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTM
L, like Gecko) Version/4.0 Chrome/74.0.3729.157 Mobile Safari/537.36"
,"ifa":"52d0d5c2-e923-4b1b-bd67-d3b225795edb","lmt":0,"is_google_play
_services_available":true},"app":{"id":"5bf39c09402b4d7c357c7de2","bu
ndle":"com.arcsoft.perfect365","ver":"7.83.3"},"user":{"gdpr":{"conse
nt_status":"unknown","consent_source":"no_interaction","consent_times
tamp":0,"consent_message_version":"0.0"}},"request":{"placements":["D
EFAULT-4977016"],"header_bidding":false}}
```

Table 19. Example request from the Perfect365 app to Vungle, containing location and missing GDPR consent

3.3.4 Unencrypted traffic from Perfect365 to third parties

Several parties received unencrypted HTTP traffic from Perfect365, rather than traffic encrypted with HTTPS. This is worrisome, since it implies that anyone with network layer access (e.g. somebody on the same open wireless network) would be able to access the contents. Unencrypted web traffic is generally considered a security risk.

We have seen roughly 35 advertising-related requests to **Sovrn / Lijit** (http://ap.lijit.com/beacon) and a similar amount to **Amazon**, http://s.amazon-adsystem.com/x/, but these appear to be beacons that do not transmit any data.

More worrying are 20 requests sent unencrypted to **Receptiv / Verve** (mediabrix.com), which does contain user data in form of the app name, device information, advertising ID, and GPS location. None of the traffic observed towards the mediabrix.com domain uses HTTPS for security. Table 20 shows a typical request from August 7th.

```
POST /v2/manifest/YSoHQpdPrL HTTP/1.1
Accept: application/json; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36
Content-Length: 479
Content-Type: text/plain; charset=ISO-8859-1
Host: mobile.mediabrix.com
Connection: close

{"session":"EAB1A938-131F-0800-36E7-25C152E89800","version":"1.8.2","
sdk":"1.8.2.002","application_id":"YSoHQpdPrL","device_info":{"packag
e_name":"com.arcsoft.perfect365","system_API":"27","system_name":"And
roid","system_version":"8.1.0","model":"Nexus 5X","UID":"52d0d5c2-e92
3-4b1b-bd67-d3b225795edb","trk":1,"screen_size":"normal","screen_DPI"
:"420","carrier":"Telenor","connection_type":"WiFi","language":"en","
manufacturer":"LGE","latitude":62.redacted,"longitude":6.redacted}}
```

Table 20. User data sent unencrypted from the Perfect365 app to Receptiv / Verve (mediabrix.com)

3.3.5 Perfect365 interaction with FluxLoop (Pinch) and Unacast

The Perfect365 app is observed to send requests to Pinch, which is the name of FluxLoop’s (https://fluxloop.com/) location service. We observe POST requests to the following URL endpoint:

- https://uc-eu2.pinch.no/api/v1/config

The parameters to this request contain information including the mobile app, and the phone model. The request returns multiple endpoints as part of the configuration, including:

- "eventsEndpoint":"https://improbability-dot-uc-h2g2.appspot.com/unacastsdk",
- "deviceInfoEndpoint":"https://proxingest.azurewebsites.net/api/v1/deviceinfo",
- "liveEventEndpoint":"https://pureingestlive.azurewebsites.net/api/v1/event",

We subsequently observe traffic going from the phone to the eventsEndpoint, which is located in Google App Engine at improbability-dot-uc-h2g2.appspot.com. The messages contain information about the current Wifi network, device, battery level, and location. We did not observe any information to the proxingest / pureingestlive endpoints. Table 21 shows a message on August 7th (formatted to increase legibility) containing information about network connection, device, events, location, and state.

```
POST /unacastsdk HTTP/1.1
Content-Type: application/json
Accept: application/json
app_id: com.arcsoft.perfect365
client_id: f5887d33-c7bd-4fb7-b334-abf0fa02ae04
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: improbability-dot-uc-h2g2.appspot.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 9394

{"events":[{"connection":{"bssid":"xx:xx:xx:xx:xx:xx","cellType":"LTE
","level":-62,"mcc":"242","mnc":"01","ssid":"redacted","timestamp":"2
019-08-07T11:06:19+02:00","type":"WIFI"},"device":{"activity":true,"a
did":"52d0d5c2-e923-4b1b-bd67-d3b225795edb","adidLimited":false,"appI
d":"com.arcsoft.perfect365","appVersion":"7.85.5","bluetoothEnabled":
false,"configUrl":"https:\/\/uc-eu2.pinch.no\/api\/v1\/config","local
e":"en_US","location":"always","locationServicesEnabled":true,"manufa
cturer":"LGE","mcc":"242","mnc":"01","model":"Nexus 5X","os":"android
","osSdkVersion":"27","osVersion":"8.1.0","playServicesEnabled":true,
"playServicesVersion":"12451000","publisherId":"none","sdkVersion":"1
.2.24","timestamp":"2019-08-07T11:06:19+02:00","trackingEnabled":true
},"event":{"altitude":79,"bearing":0,"hacc":34,"lat":62.redacted,"lon
":6.redacted,"provider":"SNAPSHOT","speed":0,"timestamp":"2019-08-07T
11:06:19+02: 00","updated":"2019-08-07T11:06:20+02:00","type":"LOCATI
ON"},"location":{"altitude":79,"bearing":0,"hacc":34,"lat":62.redacte
d,"lon":6.redacted,"provider":"SNAPSHOT","speed":0,"timestamp":"2019-
08-07T11:06:1 9+02:00","updated":"2019-08-07T11:06:20+02:00","type":"
LOCATION"},"state":{"activity":"Still","battery":0.84,"bluetoothEnabl
ed":false,"charging":false,"foreground":false,"powersave":false,"time
stamp":"2019-0 8-07T11:06:13+02:00"}},
```

[… remainder of payload omitted for brevity …]

Table 21. Data sent from the Perfect365 app to what we think is Unacast

We conjecture, but are not able to conclusively prove, that the traffic is being broadcast based on the configuration supplied by FluxLoop and flowing into Unacast’s ecosystem. This is based in part on the endpoint names – “Prox” (proximity) and “Pure” are two of Unacast’s main services[25], and the name “unacastsdk” is also indicative.

[25] See https://www.unacast.com/post/welcome-to-unacast-prox-network and https://www.unacast.com/solutions/data-feeds

3.4 MyDays

MyDays is a period tracker and fertility app that potentially handles a great deal of personal information such as information related to fertility, sexual activity and similar. It requests permissions to detailed location data (i.e. GPS) without any obvious use case for the app itself.

The MyDays app was tested mainly on July 12th, 15th and 16th, July 30th and 31st, and August 7th.

3.4.1 General observations

The MyDays app transmits data to a number of different advertising companies. We observed the following 5 parties receiving the advertising ID from the app:

- AppLovin (*.applovin.com)
- Liftoff (adexp.liftoff.io)
- Google (app-measurement.com)
- Ogury Presage (pad-v3.presage.io)
- Placed (panelist.placed.com)

An interesting observation is that the app sends a large number of requests to Google (nearly 4000 requests to googleads.g.doubleclick.net observed in total). While the requests to Doubleclick do **not** contain the advertising ID, the responses from Google **do** contain it – demonstrating that Google is readily able to identify the device based on the other user information they receive.

As with Grindr, Liftoff receives latitude and longitude pointing to a location in Oslo. We think that this may be inferred from either the external IP address or other metadata, as this location is not particularly close to the actual location of the device during testing.

3.4.2 Data transmission from MyDays to Placed

During the technical testing we observed that **Placed** receives quite a lot of data from the MyDays app. During a few days of testing, Placed received GPS coordinates more than 250 times. The app also attempts to send the device MAC address[26], and other identifiers.

```
POST /api/v2/sync HTTP/1.1
Authorization: redacted
User-Agent: placed-agent-android/5.0.1.4/56d4ef8ce9ef/295_2.9.5
Accept: application/json, image/gif
Content-Type: application/json
Content-Length: 1231
Host: panelist.placed.com
Connection: close
Accept-Encoding: gzip, deflate
```

[26] The MAC address is set to a fake value, 02:00:00:00:00:00 by the Android operating system, as noted in Chapter 3.1.1 this would not have happened on older Android versions

```
{
  "deviceIdentifier":"c5e2dd23e25a358f",
  "batchKey":"d97deb78-bf56-448d-a7ea-49a58c7de5b3",
  "device":{
    "identifierType":"android_id",
    "identifier":"c5e2dd23e25a358f",
    "make":"LGE",
    "model":"Nexus 5X",
    "carrier":"Telenor",
    "osName":"Android",
    "osVersion":"8.1.0",
    "alternateIdentifier":[
      {"name":"android_id","value":"c5e2dd23e25a358f"},
      {"name":"mac_address","value":"02:00:00:00:00:00"},
      {"name":"advertising_id","value":"52d0d5c2-e923-4b1b-bd67-
d3b225795edb"},
      {"name":"random_id","value":"da1e860b-de91-4111-84e5-
a33d4c252925"}],
    "traits":[
      {"name":"app_bundle_id","value":"com.chris.mydays"},
      {"name":"app_version","value":"295_2.9.5"},
      {"name":"sdk_version","value":"5.0.1.4"},
      {"name":"android_min_sdk_version","value":"19"},
      {"name":"android_target_sdk_version","value":"26"}
    ]},
  "batteryModel":"android:BOBCAT",
  "location":[
    {"provider":"fused","source":"passive-fused",
    "latitude":62.redacted,"longitude":6.redacted,
    "accuracy":16.463,"altitude":0,"time":1562942690652},
    {"provider":"wifi","source":"passive-lm",
    "latitude":62.redacted, "longitude":6.redacted,
    "accuracy":20.463,"altitude":0,"time":1562942690653},
    {"provider":"fused","source":"passive-fused",
    "latitude":62.redacted,"longitude":6.redacted,
    "accuracy":16.463, "altitude":0,"time":1562942697103}
]}
```

Table 22. Excerpts of data sent from the MyDays app to Placed on July 16th

In another rather surprising finding, we observed MyDays sending the whole list of installed apps (about 150 packages) to Placed’s sync API (panellist.placed.com/api/v2/sync). An excerpt of this message is shown in Table 23, as the full list is prohibitively long.

```
"event":[{
"appKey":"56d4ef8ce9ef",
"eventRole":"SYSTEM_EVENT",
"eventType":"packages",
"attribute":[
  {"name":"com.android.hotwordenrollment.xgoogle", "value":"8.1.0"},
  {"name":"com.android.printspooler", "value":"8.1.0"},
  {"name":"com.verizon.omadm", "value":"6.0-PDK2275151"},
  {"name":"com.android.defcontainer", "value":"8.1.0"},
  {"name":"com.android.sdm.plugins.dcmo", "value":"8.1.0"},
[…]
  {"name":"com.chris.mydays","value":"2.9.5"},
[…]
  {"name":"com.google.android.inputmethod.latin",
"value":"8.3.6.250752527-release-arm64-v8a"},
  {"name":"com.google.android.music","value":"8.20.8059-1.N"},
  {"name":"com.android.htmlviewer","value":"8.1.0"},
  {"name":"com.google.android.configupdater","value":"8.1.0"},
  {"name":"com.google.android.calendar","value":"6.0.39-252984007-
release"}],
"time":1563272213557}]}
```

Table 23. Excerpts from list of installed packages, sent from the MyDays app to Placed

This seems rather problematic from a data privacy perspective, as it would allow Placed to build a *very* detailed profile of the user’s interests (based on their app selecetion), as well as identify other apps that might report additional data.

Finally, requests to Placed are sent with an Authorization header. This is a base64-encoded token which sometimes contains the device IP address as an explicit parameter, as shown in Table 24 which shows an encoded and decoded header.

```
Authorization: PFRESH
eyJ1dWlkIjoiNGQ5YTZlYTY5MGQ4NDJhZjg4NTQyY2NlNzBiYzI4YzQiLCJ0b2tlbiI6e
yJwbGFjZWRSZXNvdXJjZU5hbWUiOiJ1c2VyOjE0OTg2NzM2NjsiLCJub25jZSI6ImJuc2
8xcDJzNGMzdHJhYWxkaGxjY2VpZjE4IiwiZXhwaXJlc0F0Ijo5MjIzMzcyMDM2ODU0Nzc
1ODA3LCJjcmVhdGVkQXQiOjE1NjMyNzIyMDYsInZlcnNpb24iOiIxIiwic2lnbmF0dXJl
IjoiYk4vYXk0dUk4cUtKOXYyLzQ5bnhqQTZRUGlvSTAvRHVDcTUvU25CRzVJMFx1MDAzZ
CJ9LCJob3N0IjoiOTQuMTI3LjU2LjcxIn0=
```

```
{
    "uuid":"4d9a6ea690d842af88542cce70bc28c4",
    "token":{
        "placedResourceName":
        "user:149867366;",
        "nonce":"bnso1p2s4c3traaldhlcceif18",
        "expiresAt":9223372036854775807,
        "createdAt":1563272206,
        "version":"1",
        "signature":
            "bN/ay4uI8qKJ9v2/49nxjA6QPioI0/DuCq5/SnBG5I0\u003d"
    },
    "host":"94.127.56.71"
}
```

Table 24. Authorization token sent from MyDays to Placed, before and after base64 decoding

3.4.3 Location data sharing from MyDays to Neura and Placer

The MyDays app also communicated a lot with **Neura**, to endpoints located at wapi.theneura.com and inputapi.theneura.com. The former endpoint appears to be mainly concerned with behavioural events, such as “userGotUp”. In the requests to the latter, we observe information such as GPS coordinates, MAC-address (once again masked by Android), a nearby Wi-Fi networks, and battery information. Similarly to Placed, Neura employs their own unique tracking ID instead of using the built-in advertising ID. In total we observed about 500 requests to Neura.

```
POST /api/channels HTTP/1.1
Timezone: Europe/Oslo
X-Volley-Retry: 0
X-Mobile-Data-Connected: false
X-Device-Brand: google
X-Device-Model: Nexus 5X
X-Neura-Operating-System: android
X-Neura-Request-Id: 9f7c06f11b544bf0a6854bac48023f86
X-Neura-Timestamp: 1562942698256
X-Neura-SyncSource: AppGoesToTheForeground
x-neura-data-format-version: 1
Authorization: Bearer redacted
X-Neura-Sdk-Version: 5.5.0
X-Neura-Location-Permission: enabled
Content-Encoding: gzip
X-Wifi-Connected: true
X-Wifi-Signal-Strength: -41
X-App-Version: 2.9.5
Connection: close
X-Os-Version: 27
X-Neura-Chunk-Number: 1
X-Device-Manufacturer: LGE
X-Retry: 0
X-Android-Api-Level: 27
X-Neura-Google-Play-Installed: 1
X-Neura-Device-Id: Android_c5e2dd23e25a358f
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: inputapi.theneura.com
Accept-Encoding: gzip, deflate
Content-Length: 424


{"channel":
{"routers":[
  {"mac":"04:92:26:86:92:38",
  "name":"testnetwork","signal_strength":-41,
  "application":"MyDays","connected":true,
  "timestamp":1562942695,"timezone":"Europe\/Oslo",
  "ip":"192.168.150.1","source":"onChange",
  "syncSource":"AppGoesToTheForeground"}],
"geolocations":[
  {"lon":-1,"lat":-1,"alt":-1,"battery":1,
  "horisontal_accuracy":-1,"provider":"N\/A","application":"MyDays",
  "elapsed_realtime_nanos":0,"bearing":359,"speed":-1,
  "timestamp":1562920537,"timezone":"Europe\/Oslo",
  "utc_offset":-2,"source":"otherApps",
  "syncSource":"AppGoesToTheForeground"},
  {"lon":-1,"lat":-1,"alt":-1,"battery":1,
  "horisontal_accuracy":-1,"provider":"N\/A","application":"MyDays",
  "elapsed_realtime_nanos":0,"bearing":359,"speed":-1,
  "timestamp":1562920537,"timezone":"Europe\/Oslo",
  "utc_offset":-2,"source":"onDemand",
  "syncSource":"AppGoesToTheForeground"},
  {"lon":6.redacted,"lat":62.redacted,"alt":-1,"battery":1,
  "horisontal_accuracy":16.46299934387207,
  "provider":"fused","application":"MyDays",
  "elapsed_realtime_nanos":22152863000000,"bearing":359,
  "speed":-1,"timestamp":1562942690,"timezone":"Europe\/Oslo",
  "utc_offset":-2,"source":"onDemand",
  "syncSource":"AppGoesToTheForeground"},
  {"lon":6.redacted,"lat":62.redacted,"alt":-1,"battery":1,
  "horisontal_accuracy":16.46299934387207,
  "provider":"fused","application":"MyDays",
  "elapsed_realtime_nanos":22152863000000,"bearing":359,
  "speed":-1,"timestamp":1562942690,"timezone":"Europe\/Oslo",
  "utc_offset":-2,"source":"otherApps",
  "syncSource":"AppGoesToTheForeground"}
]}}
```

Table 25. Request from the MyDays app to Neura on July 12th. In a separate transmission, neighbouring wifi networks were also listed in detail

Finally, mnemonic observed that **Placer** was receiving detailed GPS location data, WiFi access point data, cell tower data, and Bluetooth properties from the MyDays app. Together, these data points can be used to pinpoint location, even inside a building, down to a specific floor. **Placer** was not observed to receive the Android advertising ID, but appears to use its own identifiers. Table 26 shows an excerpt of the data that is transmitted.

```
P-APPINFO: com.chris.mydays/2.9.5
Host: api.placer.io

{
  "sdk_version": "PlacerSDK 2.7.11.1",
  "data": [
    {
      "type": "location",
      "time": "2019-07-16T11:53:35.953+0200",
      "serial": 0,
      "session_serial": 0,
      "value": {
        "provider": "fused",
        "time": "2019-07-16T11:53:35.482+0200",
        "accuracy": 15.956999778747559,
        "loc": {
          "long": 6.redacted,
          "lat": 62.redacted
        },
        "workspace": {
          "debug_info": "mLocationCount=1, OrigTime=1563270814786"
        },
        "cell_tower": {
          "mcc": "242",
          "mnc": "01",
          "cid": redacted,
          "lac": redacted
        }
      }
    },
[…]
    {
      "type": "wifi_info",
      "time": "2019-07-16T11:53:35.869+0200",
      "serial": 0,
      "session_serial": 0,
      "value": {
        "WifiState": "On",
        "wifi_active_network": {
          "SSID": "\"testnetwork\"",
          "BSSID": "36:16:XX:XX:XX:XX",
          "RSSI": -52
        },
        "wifi_networks_scan": [

(full list of neighbouring wifi networks redacted by mnemonic for privacy reasons)

        ],
        "wifi_networks_scan_original_count": 13,
        "wifi_networks_scan_original_ts": 1563270815869,

(remainder of transmission redacted)
```

Table 26. Excerpts from request sent from the MyDays app to Placer on July 16th

3.5

3.5 OkCupid

OkCupid is a dating app owned by Match Group. When first opening an OkCupid account, the user is asked to answer a series of questions about themselves, in order to create a profile. These can be innocuous questions about what movies the user likes, but also includes very intimate questions about sexual desires, drug and alcohol use, political views, and more.

OkCupid was tested mainly on July 8th and 9th, July 15th, and August 7th.

3.5.1 General observations

The OkCupid app transmits data to a number of different advertising companies. We observed the following parties receiving the advertising ID from the app, together with other information:

- AppsFlyer (t.appsflyer.com)
- Facebook (graph.facebook.com) -
- Kochava (control.kochava.com)

We did not observe location information such as IP address transmitted to either of these parties, but they do collect detailed information about the device. In particular, AppsFlyer collects data from device sensors including magnetometer, gyroscope and accelerometer. The purpose of this collection is not clear to us.

Some user data sent to Google DoubleClick as custom parameters, including gender and age.

The OkCupid app asks for permission to use location data, but since this is needed for the basic functionality of the app, this behaviour is not very suspicious in itself.

Table 27, 28, and 29 shows sample requests from the OkCupid app to **AppsFlyer**, **Facebook**, and **Kochava**, indicating the level of detail present in the transmissions.

```
POST /api/v4/androidevent?buildnumber=4.8.7&app_id=com.okcupid.okcupid HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Length: 1825
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X Build/OPM7.181205.001)
Host: t.appsflyer.com
Connection: close


{"country":"US","af_timestamp":"1563206657892","appsflyerKey":"XkJdrCAFbLCxnQ4SH7xon6","af_events_api":"1","isFirstCall":"false","registeredUninstall":false,"operator":"Telenor","network":"WIFI","timepassedsincelastlaunch":"525778","af_v2":"0a7db8d6122d0e3da932b0a80de3519a05b9572d","uid":"1562251834189-3710564754916840950","isGaidWithGps":"true","lang_code":"en","installDate":"2019-07-04_145034+0000","app_version_code":"1213","firstLaunchDate":"2019-07-09_140119+0000","model":"Nexus 5X","lang":"English","brand":"google","installAttribution":"{\"af_status\":\"Organic\",\"af_message\":\"organic install\",\"is_first_launch\":\"false\"}","deviceType":"user","product":"bullhead","deviceData":{"sensors":[{"sT":2,"sVS":[-25.9375,-125.375,-177.6875],"sN":"B
MM150 magnetometer","sV":"Bosch","sVE":[-27.8125,-126.125,-177.75]},{
"sT":4,"sVS":[-0.0013545793,-8.7138417E-4,0.010109018]," sN":"BMI160
gyroscope","sV":"Bosch","sVE":[0.001841214,0.0023244093,-0.00586995]}
,{"sT":1,"sVS":[0.60354495,0.9244776,10.063872],"sN":"BMI160 accelero
meter","sV":"Bosch","sVE":[0.6562354,0.9053174,10.130933]}],"cpu_abi"
:"arm64-v8a","build_display_id":"OPM7.181205.001","btch":"no","arch":
"","btl":"100.0","cpu_abi2":""},"installer_package":"com.android.vend
ing","date2":"2019-07-04_145034+0000","counter":"2","date1":"2019-07-
04_145034+0000","extraReferrers":"{\"utm_source= google-play& utm_med
ium=organic\":\"[1563206657356]\"}","advertiserId ":"52d0d5c2-e923-4b
1b-bd67-d3b225795edb","advertiserIdEnabled":"true","referrer":"utm_so
urce=google-play&utm_medium=organic","af_v":"ab97027b85c8864993ac1001
64408ea3fc1c3058","carrier":"Telenor","af_preinstalled":"false","iaec
ounter":"0","tokenRefreshConfigured":false,"sdk":"27","appUserId":"79
06987202621823856","app_version_name":"30.3.2","device":"bullhead","p
latformextension":"android_native"}
```

Table 27. Data transmitted from the OkCupid app to AppsFlyer

```
POST /v3.3/484681304938818/activities HTTP/1.1
Accept-Encoding: gzip, deflate
User-Agent: FBAndroidSDK.5.0.2
Accept-Language: en_US
Content-Type: application/x-www-form-urlencoded
Host: graph.facebook.com
Connection: close
Content-Length: 1287


format=json&sdk=android&custom_events=%5B%7B%22_eventName%22%3A%22fb_
mobile_deactivate_app%22%2C%22_eventName_md5%22%3A%2292255b491a4e25b5
d809edcf3665affe%22%2C%22_logTime%22%3A%221562682304%22%2C%22_ui%22%3
A%22MainActivity%22%2C%22_session_id%22%3A%223bcb040f-ac03-4ee6-a307-
9918a945b6fe%22%2C%22_valueToSum%22%3A2036.728%2C%22fb_mobile_time_be
tween_sessions%22%3A%22session_quanta_9%22%2C%22fb_mobile_launch_sour
ce%22%3A%22Unclassified%22%2C%22fb_mobile_app_interruptions%22%3A%220
%22%7D%2C%7B%22_eventName%22%3A%22fb_mobile_activate_app%22%2C%22_eve
ntName_md5%22%3A%22cb7f3b6cd294afce05ece615d43ea7b9%22%2C%22_logTime%
22%3A1563206657%2C%22_ui%22%3A%22MainActivity%22%2C%22_session_id%22%
3A%223bcb040f-ac03-4ee6-a307-9918a945b6fe%22%2C%22fb_mobile_launch_so
urce%22%3A%22Unclassified%22%7D%5D&event=CUSTOM_APP_EVENTS&advertiser
_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb&advertiser_tracking_enabled=
true&installer_package=com.android.vending&anon_id=XZ671e13ae-0adc-4e
b1-90ab-b808df4a88da&application_tracking_enabled=true&extinfo=%5B%22
a2%22%2C%22com.okcupid.okcupid%22%2C1213%2C%2230.3.2%22%2C%228.1.0%22
%2C%22Nexus+5X%22%2C%22en_US%22%2C%22GMT%2B02%3A00%22%2C%22Telenor%22
%2C1080%2C1794%2C%222.62%22%2C6%2C11%2C6%2C%22Europe%5C%2FOslo%22%5D&
application_package_name=com.okcupid.okcupid&
```

Table 28. Data transmitted from the OkCupid app to Facebook

```
POST /track/kvTracker.php HTTP/1.1
Content-Length: 734
Content-Type: application/xml
Host: control.kochava.com
```

```
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)


[{"kochava_app_id":"kookcupid----android554154662c06a","kochava_devic
e_id":"KAedc2d8efc26e4426aefdedad101bf053","action":"initial","last_p
ost_time":0,"currency":"USD","sdk_version":"Android20150511","data":{
"usertime":"1562594548","uptime":"5","updelta":"0","adid":"52d0d5c2-e
923-4b1b-bd67-d3b225795edb","device":"Nexus 5X-google","disp_h":1794,
"disp_w":1080,"package_name":"com.okcupid.okcupid","app_version":"OkC
upid 1213","app_short_string":"30.3.2","android_id":"12f13f16b160bb1f
","os_version":"Android 8.1.0","app_limit_tracking":false,"device_lim
it_tracking":false,"odin":"1ccd99a656ca306671a3781fb57d3868e8728af5",
"fb_attribution_id":"","conversion_type":"gplay","conversion_data":"u
tm_medium:organic&utm_source:google-play"}}]
```

Table 29. Data transmitted from the OkCupid app to Kochava

Traffic to AppsFlyer and Facebook was quite frequent when the app was in use, every few minutes or so. With Kochava, we only observed a handful of requests, and all the requests but one used Kochava’s own device id, rather than the advertising ID. Since the advertising ID is transmitted once, this information is of course still linkable by Kochava on the backend.

In addition to the above, we observed traffic to the following interesting third parties:

- Doubleclick / Google
  - In-app advertising, receives device info
- Sift (siftscience.com)
  - Receives device info, possibly attempting to detect device modification or rooting
- Embrace.io (data.emb-api.com)
  - Appears to receive information about GUI events, used for debugging, but could potentially lead to data privacy concerns
- Crashlytics (reports.crashlytics.com)
  - Used to report crash diagnostics
- mParticle (jssdkdns.mparticle.com)
  - Gets the mParticle javascript SDK, although we did not observe further traffic
- Braze / Appboy (sdk.iad-01.braze.com, dev.appboy.com)
  - Discussed in next section

Finally, it is worth noting that we observed a large number of requests to the Google Maps API, apparently transmitting the user’s GPS coordinates in order to receive a static map. However, these requests all failed with a 403 Forbidden, due to a missing API key.

3.5.2 Data transmissions from OkCupid to Braze

Braze, previously known as AppBoy, is a company that develops software for customer relationship management and mobile marketing automation. During our testing, we discovered that Braze received a lot of application data from the OkCupid app, including the personal questions and answers, as well as information about the user’s ethnicity. Braze also received the user’s GPS location in some cases.

We note that the Braze device ID used with OkCupid is not the same as in Grindr.

Table 30 and Table 31 show excerpts of requests made by the OkCupid app to Braze, with sensitive contents highlighted. Due to the size of the requests, we only provide relevant context.

```
{
  "app_version": "30.3.2",
  "device_id": "12027c9f-2fe6-40a7-a548-1ecebe7eb435",
  "time": 1563206812,
  "api_key": "a7fa62f4-0365-49e1-bd21-5bdbbfda2458",
  "sdk_version": "2.2.4",
  "attributes": [{
      "custom": {
          "religion": "christian",
          "education level": "high school"
      },
      "user_id": "7906987202621823856"
    }
  ],
  "events": [
    {
      "name": "set",
      "data": {
        "key": "desired relationship",
        "value": ["new friends"]
      },
      "time": 1.563206762399E9,
      "user_id": "7906987202621823856",
      "session_id": "5ff87b97-2d19-490e-84a7-8ab62f6225bd"
    },
    {
      "name": "lr",
      "data": {
        "latitude": redacted,
        "longitude": redacted,
        "altitude": 0,
        "ll_accuracy": 20.084999084472656
      },
      "time": 1.563206755939E9,
      "user_id": "7906987202621823856",
      "session_id": "5ff87b97-2d19-490e-84a7-8ab62f6225bd"
    },
[…]
    {
      "name": "set",
      "data": {
        "key": "ethnicity",
        "value": [
          "null"
        ]
      },
      "time": 1.563206762404E9,
      "user_id": "7906987202621823856",
      "session_id": "5ff87b97-2d19-490e-84a7-8ab62f6225bd"
    }
  ]
}
```

```
{
    "app_version":"30.3.3",
    "device_id":"12027c9f-2fe6-40a7-a548-1ecebe7eb435",
    "time":1565186761,
    "api_key":"a7fa62f4-0365-49e1-bd21-5bdbbfda2458",
    "sdk_version":"2.2.4",
    "events":[
    {
        "name":"ce",
[...]
        "time":1.565186719733E9,
        "user_id":"7906987202621823856",
        "session_id":"1e6fedb7-1e73-46b5-bacf-9e2da078e5e0"},
        {
            "name":"set","data":{
                "key":"ethnicity",
                 "value":["white"]},
            "time":1.565186748207E9,"user_id":"7906987202621823856",
            "session_id":"1e6fedb7-1e73-46b5-bacf-9e2da078e5e0"},
```

Table 30. Examples of user data and geolocation sent to Braze

```
{
  "name":"ce",
  "data":{
    "n":"answered question",
    "p":{
      "reanswer":"false",
      "debug_platform":"android",
      "importance":"somewhat",
      "question text":"what is your preferred cuddling position?",
      "drilldown filter name":"null",
      "source":"self profile",
      "drilldown filter id":"null",
      "question id":"464470",
      "answered publicly":"true",
      "user responses":"big spoon",
      "skipped":"false"
    }
  },
  "time":1.565187207344E9,
  "user_id":"7906987202621823856",
  "session_id":"1e6fedb7-1e73-46b5-bacf-9e2da078e5e0"
},
```

```
{
  "name": "ce",
  "data": {
    "n": "answered question",
    "p": {
      "reanswer": "false",
      "debug_platform": "android",
       "importance": "medium",
       "question text": "have you used psychedelic drugs (lsd,
mescaline, peyote, etc.) or would you like to?",
       "drilldown filter name": "null",
       "source": "self profile",
       "drilldown filter id": "null",
       "question id": "15414",
       "answered publicly": "true",
       "user responses": "yes, i have used psychedelic drugs",
       "skipped": "false"
     }
   },
   "time": 1.565189217162E9,
   "user_id": "7906987202621823856",
   "session_id": "1e6fedb7-1e73-46b5-bacf-9e2da078e5e0"
 },
```

Table 31. Examples of user answers to sensitive questions in the OkCupid app, sent to Braze

The questions in OkCupid cover a wide range of subjects, including politics, sex, economics and health. Further examples of questions observed during testing include:

- Do you have student debt?
- Do you prefer hardcore or softcore when it comes to your porn?
- Are you jewish?
- How does the idea of being slapped hard in the face during sex make you feel?
- Is it easy for you to achieve orgasm?
- Do you enjoy exercise?
- Generally, do you enjoy being drunk?
- Is climate change real?
- Is the US educational system designed to benefit the rich?
- Would you ever date someone that is hiv positive?

3.6 My Talking Tom 2

My Talking Tom 2 is a children’s app / game developed by Outfit7, a company which also happens to run an advertising network[28]. The app does not ask for any suspicious permissions upon install.

My Talking Tom 2 was tested mainly on July 4th, July 12th, and July 16th.

3.6.1 General observations

In our tests, My Talking Tom 2 is observed sending the device advertising ID to 8 different parties (including Outfit7 themselves):

- AppsFlyer (events.appsflyer.com)
- AppLovin (rt.applovin.com)
- Facebook (graph.facebook.com)
- IQzone (pssvc.iqzone.com)
- ironSource (SuperSonic) (*.supersonicads.com)
- Mobfox (my.mobfox.com)
- Outfit7 (*.bee7.com, *.outfit7.com)
- Rubicon Project (exapi-eu.rubiconproject.com)

We observe that data sent to Facebook includes sensor data from the device accelerometer and gyroscope.

The app transmits its external IP address to 3 different parties: **Mobfox**, **Rubicon Project**, and **PubNative**. These interactions were reasonably sparse, with 2 requests to PubNative, 4 to Mobfox, and 15 to Rubicon Project observed.

```
GET /api/v3/native?apptoken=89a7be08b18747aab4f839e2a6818f6a&zoneid=1
&gid=&bundleid=com.outfit7.mytalkingtom2&os=android&al=m&mf=points,re
venuemodel,campaignid,creativeid,contentinfo&osver=8.1.0&devicemodel=
Nexus%2B5X&dnt=0&srvi=1&ua=Mozilla%2F5.0+%28Linux%3B+Android+8.1.0%3B
+Nexus+5X+Build%2FOPM7.181205.001%3B+wv%29+AppleWebKit%2F537.36+%28KH
TML%2C+like+Gecko%29+Version%2F4.0+Chrome%2F75.0.3770.101+Mobile+Safa
ri%2F537.36&ip=94.127.56.71&coppa=1 HTTP/1.1
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: api.pubnative.net
Accept-Encoding: gzip, deflate
```

```
GET /request.php?rt=api&r_type=native&n_ver=1.1&n_layout=content_wall
&n_adunit=promoted_listings&n_context=product&n_plcmttype=atomic&i=94
.127.56.71&u=Mozilla%2F5.0+%28Linux%3B+Android+8.1.0%3B+Nexus+5X+Buil
d%2FOPM7.181205.001%3B+wv%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Ge
cko%29+Version%2F4.0+Chrome%2F75.0.3770.101+Mobile+Safari%2F537.36&m=
live&s=eba59acacb61893537ce963d48d067a2&adspace_strict=1&adspace_widt
```

[28] See https://outfit7.com/advertising/ for details

```
h=320&adspace_height=480&o_andadvid=52d0d5c2-e923-4b1b-bd67-d3b225795
edb&sub_bundle_id=com.outfit7.mytalkingtom2&sub_storeurl=http%3A%2F%2
Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dcom.outfit7.mytalkin
gtom2&imp_instl=1&dev_dnt=0&dev_lmt=0&n_img_icon_req=1&n_img_icon_siz
e=80&n_img_large_req=1&n_img_large_w=1200&n_img_large_h=627&n_title_r
eq=1&n_title_len=25&n_desc_req=0&n_desc_len=90 HTTP/1.1
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: my.mobfox.com
Accept-Encoding: gzip, deflate
```

```
POST /a/api/exchange.json HTTP/1.1
Authorization: Basic redacted
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36
Connection: close
Content-Type: application/json
Host: exapi-eu.rubiconproject.com
Accept-Encoding: gzip, deflate
Content-Length: 2215

 […]
      "bundle":"com.outfit7.mytalkingtom2",
[…]
  "device":{
      "ua":"Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36",
      "language": "en",
      "dnt":0,
      "lmt":0,
      "ip":"94.127.56.71",
      "make":"google",
      "model":"Nexus 5X",
      "carrier":"Telenor",
      "connectiontype": 2,
      "dpidsha1":"91e0c1fc031d6778bdd1e81d1ca56abf19f70f8b",
      "ifa":"52d0d5c2-e923-4b1b-bd67-d3b225795edb",
      "os": "android",
      "osv":"5.0"
  },
  "user":{
      "ext": {

      }
  },
  "regs": {
    "coppa":1
    ,"ext":{"gdpr":1}
  }
}
```

Table 32. Requests from My Talking Tom app to PubNative, Mobfox, and Rubicon Project

It is worth noting that communications with **Rubicon Project** goes over unencrypted HTTP rather than HTTPS, which means that all the data is visible in cleartext for a network attacker who is eavesdropping on traffic.

3.6.2 My Talking Tom 2’s use of IQzone for ad mediation

In a similar way as the traffic flow between Grindr and MoPub (described in Chapter 3.2.1), My Talking Tom 2 seems to use IQzone as a mediation layer. We have observed the following three-step process:

1. The My Talking Tom 2 app sends a request to IQzone (postitial.com belongs to IQzone):

```
GET /imd/schemas/contextual_mobfox_native_schema_android_cv2118plus_2
0190328_0900.json HTTP/1.1
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: cdn-cf.postitial.com
Accept-Encoding: gzip, deflate
Cookie: __cfduid=db015705b9021d48d6c34241bf01345d21563269308
```

Table 33. Initial request sent from the My Talking Tom 2 app to IQzone

2. IQzone responds with information about what ad the mobile app should fetch. Note that this response contains placeholders for sensitive information, like **`${DEVICE_IP_ADDRESS}`** instead of the actual IP address of the device.

```
HTTP/1.1 200 OK
Date: Tue, 16 Jul 2019 09:29:59 GMT
Content-Type: application/json
Connection: close
x-amz-id-2:
NzY2ri/bn88ntEOAABLqEQEv5DovDu9yJKHj/z8WIt20+dcgkJ8LeV3m6dgOdjwJrlePA
7Q6EjM=
x-amz-request-id: E2145004961B8B41
Last-Modified: Wed, 10 Apr 2019 23:32:18 GMT
ETag: W/"0e4f0ce67b7ba510f18576a78783997e"
CF-Cache-Status: HIT
Age: 3080
Expires: Wed, 15 Jul 2020 09:29:59 GMT
Cache-Control: public, max-age=31536000
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 4f72f470ff90cae0-ARN
Content-Length: 7528

{

  "3" : {
    "render-engine" : 4,
    "request-engine" : 1,
    "request" : {
      "url" :
"http://my.mobfox.com/request.php?rt=api&r_type=native&n_ver=${NATIVE
_VER}&n_layout=${NATIVE_LAYOUT}&n_adunit=${NATIVE_ADUNIT}&n_context=$
{NATIVE_CONTEXT}&n_plcmttype=${NATIVE_PLCMTYPE}&i=${DEVICE_IP_ADDRESS
}&u=${ENCODED_USER_AGENT}&m=${LIVE_OR_TEST}&s=${I_HASH}&adspace_stric
t=1&adspace_width=${AD_SPACE_WIDTH}&adspace_height=${AD_SPACE_HEIGHT}
${ANDROID_ID_SHA1_GENERATED}&o_andadvid=${GENERATED_ADID}&sub_bundle_
id=${PACKAGE_NAME}&sub_storeurl=http%3A%2F%2Fplay.google.com%2Fstore%
2Fapps%2Fdetails%3Fid%3D${PACKAGE_NAME}&imp_instl=1&dev_dnt=${DO_NOT_
TRACK}&dev_lmt=${DO_NOT_TRACK}${GENERATED_GPS_LOCS}${GENERATED_GENDER
}${GENERATED_YOB}&n_img_icon_req=${IMG_ICON_REQ}&n_img_icon_size=${IM
G_ICON_SIZE}&n_img_large_req=${IMG_LARGE_REQ}&n_img_large_w=${IMG_LAR
GE_W}&n_img_large_h=${IMG_LARGE_H}&n_title_req=${TITLE_REQ}&n_title_l
en=${TITLE_LEN}&n_desc_req=${DESC_REQ}&n_desc_len=${DESC_LEN}",
```

Table 34. Response from IQzone to the My Talking Tom 2 app, showing which fields to populate in the subsequent request

3. The My Talking Tom 2 app sends the request from the **IQzone** response to **Mobfox**. Note that the placeholder fields are now populated, and the IP address and Advertising ID is shared with the third party.

```
GET /request.php?rt=api&r_type=native&n_ver=1.1&n_layout=content_wall
&n_adunit=promoted_listings&n_context=product&n_plcmttype=atomic&i=94
.127.56.71&u=Mozilla%2F5.0+%28Linux%3B+Android+8.1.0%3B+Nexus+5X+Buil
d%2FOPM7.181205.001%3B+wv%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Ge
cko%29+Version%2F4.0+Chrome%2F75.0.3770.101+Mobile+Safari%2F537.36&m=
live&s=eba59acacb61893537ce963d48d067a2&adspace_strict=1&adspace_widt
h=320&adspace_height=480&o_andadvid=52d0d5c2-e923-4b1b-bd67-d3b225795
edb&sub_bundle_id=com.outfit7.mytalkingtom2&sub_storeurl=http%3A%2F%2
Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dcom.outfit7.mytalkin
gtom2&imp_instl=1&dev_dnt=0&dev_lmt=0&n_img_icon_req=1&n_img_icon_siz
e=80&n_img_large_req=1&n_img_large_w=1200&n_img_large_h=627&n_title_r
eq=1&n_title_len=25&n_desc_req=0&n_desc_len=90 HTTP/1.1
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: my.mobfox.com
Accept-Encoding: gzip, deflate
```

Table 35. Request sent from the My Talking Tom 2 app to MobFox, containing IP address and advertising ID

As opposed to the Grindr, the response from IQzone does not contain any sensitive information, but only placeholders. This would imply that the fields are populated in the My Talking Tom 2 app itself before being sent to the third party, and that IQzone does not necessarily know these values. We discuss how the My Talking Tom 2 app gets access to the IP address in Chapter 3.13.1.

A schematic view of the process with timestamps can be seen in the figure below.

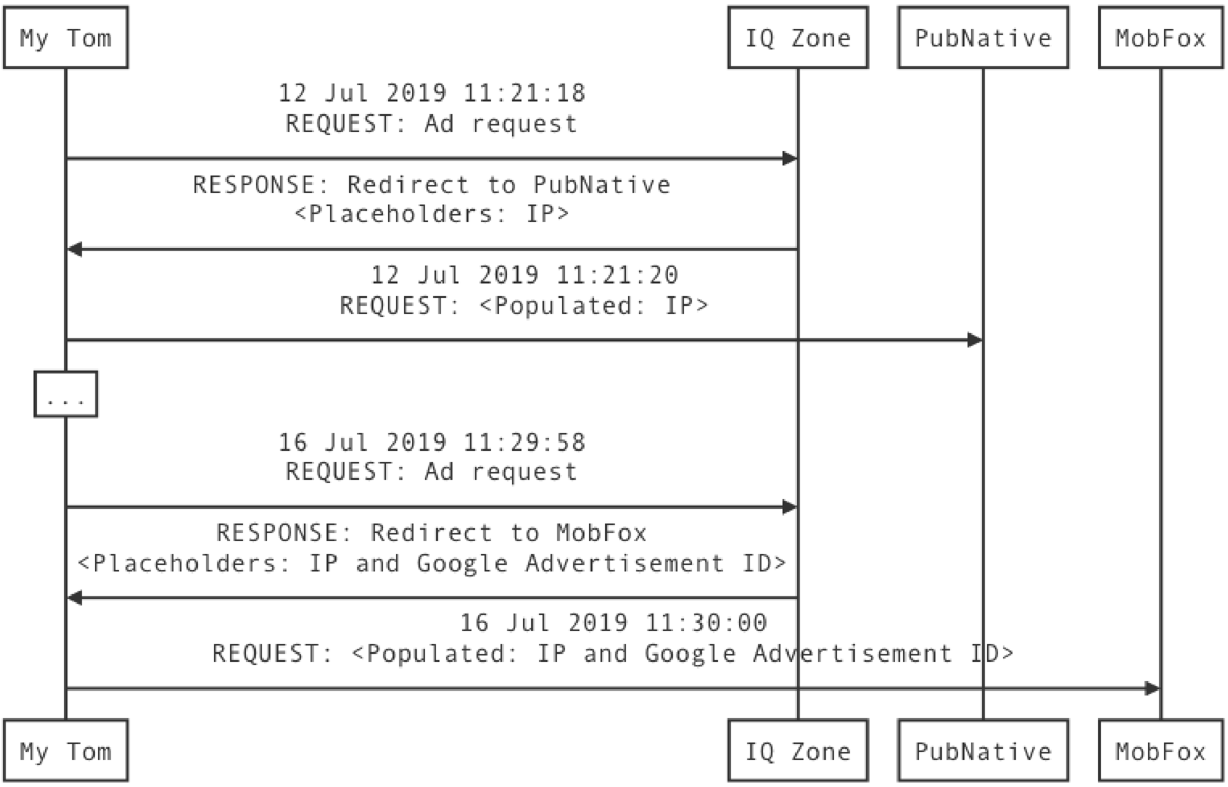


Figure 4: Sequence diagram showing the information flow between the My Talking Tom 2 app and various third-party companies, using IQzone as mediator

3.7 Muslim: Qibla finder

The “*Muslim - Qibla Finder, Prayer Times, Quran, Azan*” app is a tool which can be used to receive useful information and reminders related to religious observance, such as prayer times, and the qibla (direction of prayer) at the user’s current location. The app requests user permission to access location data, which is needed in order to determine the qibla.

When starting the Muslim app in our test lab, the app warned us about the connection being insecure, and closing shortly after, similarly to Grindr. To bypass this, we had to start the app with a “normal” (i.e. non-proxy) connection, and switch to our test setup when the app was running. Because of this it was not possible to observe absolutely all traffic during start-up of the app. Despite this, we observed a significant amount of advertising-related traffic.

The combination of precise and updated GPS location and information about the (probable) religious beliefs of the user, inferred from use of this app, seems particularly problematic in terms of misuse potential.

The Muslim app was tested mainly on July 5th, 11th, and 16th.

3.7.1 General observations

The Muslim app shares the Android advertising ID with the following parties:

- AppLovin (a.applovin.com)
- Appodeal (ach.appodeal.com, *.appbaqend.com)
- Facebook (graph.facebook.com)
- Google (app-measurement.com)
- Liftoff (adexp.liftoff.io)

The app also sends advertising requests to **Google** / Doubleclick, and uses **Bugsnag** for error reporting and analysis. Crash reports also appear to be sent to *ach.appodeal.com*.

Data is sent to **Appodeal** quite frequently while using the app, and includes the user’s external IP address. We notice that it also identifies the device as rooted.

```
POST /request/banner?ad_space_id=60&ip=94.127.56.71&dm_ver=2.4.10&bid
floor=0.35&osv=8.1.0&os=android&h=1794&w=1080&devicetype=4&connection
type=0&make=LGE&model=&utcoffset=120&country=NOR&geo_type=2&language=
en&ver=4.1.24&external_app_id=80549&publisher_id=1&native_ad_type=Aut
o&coppa=1&lmt=0&hwv=&e_ci_id=14915&ifa=52d0d5c2-e923-4b1b-bd67-d3b225
795edb&gdpr=1&ua=Dalvik%2F2.1.0%20(Linux%3B%20U%3B %20Android%208.1.0
%3B%20Nexus%205X%20Build%2FOPM7.181205.001)&carrier=&marketplaces=ope
n%2Cpb&consent=1&device_ext=%7B%22battery%22%3A100%2C%22rooted%22%3At
rue%7D&app_ext=%7B%22session_id%22%3A16%2C%22session_uptime%22%3A5134
%2C%22app_uptime%22%3A6842%2C%22sdk%22%3A%222.4.10%22%2C%22imp_count%
22%3A2%2C%22imp%22%3A%7B%22interstitial%22%3A2%7D%2C%22timp%22%3A%7B%
22banner%22%3A32%2C%22interstitial%22%3A7%7D%7D&ppi=420&pxratio=2.625
&impid=14e3a683-b826-4387-8980-6e1a3f6219f5&metadata_headers=1
HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
```

```
Host: x.appbaqend.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 342

[{"displaymanager":"mraid","displaymanager_ver":"2.0","appodeal":{"id
":"YlpiMmR3bnlhK3hhdXlEY0MzckJUTTBpMHpkMENMV0gwMW1ybG41V1YwdUpUSGtEd1
BnODh0eEJjVytzcVpPcHFFMDZKSytaNDFXYjd4T2F0Nk1sdXpObzM1M1ZBcWZOMTJjeWx
WWWVGd3NKK3VHSGFYdVFYR0xBOGlqVkloeEctLXZMdk5Gc0J2cU04UHFpTXo3S3JpTVE9
PQ%3D%3D--9f7b8e878a8a092ca509b89ccb6790451f53a657","ecpm":0.35}}]
```

Table 36. Example request from the Muslim app to Appodeal, containing the public IP address

While the above request does not identify the Muslim app as the originator, responses from Appodeal contain references such as `\"source_app_id\":\"com.hundred.qibla\"` which makes the situation clear.

The requests to **AppLovin** were quite few, and only contained device information along with the advertising ID.

Requests to **Liftoff** contain the user’s latitude and longitude, but the GPS location stated is somewhat inexact. As the name of the city and ZIP-code is also transmitted, we suspect that the location may be based on a place-name lookup rather than using the GPS sensor. It is unclear where the city and zip parameters come from.

```
POST /adexp_metrics HTTP/1.1
Host: adexp.liftoff.io
Connection: close
Content-Length: 1482
Origin: null
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36
Content-Type: text/plain
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-Requested-With: com.hundred.qibla


{"adexp_logging_frequency":0.075,"is_rewarded":false,"dest_app_platfo
rm":"android","dest_app_id":1334,"ad_group_id":92845,"app_id_external
":"ca7a212aa1","supports_native_browser":false,"spend_type":"ua","bid
_request_at":"2019-07-05T13:03:54Z","is_ua_or_abr":true,"ec2_region":
"eu-central-1","enable_html_return":false,"city":"redacted","creative
e_id":71657,"width":320,"force_custom_close":false,"source_app_name":
"Muslim: Prayer Times, Qibla, Quran, Dhikr","longitude":redacted,"is_
reengagement":false,"template_config_id":5571,"size":"320x50","channe
l_id":39,"no_custom_close":false,"source_app_genre":"Lifestyle","conn
ection_type":"wifi","supports_mraid":true,"source_app_id":"com.hundre
d.qibla","device_family":"Mobile","dest_app_russian_age_rating":16,"l
anguage":"en","zip":" redacted","region_code":null,"bid_request_id":"
b064919e-2f21-43b4-8c7e-c5ae42a6f233","device_id_type":"google-aid","
device_id_sha1":"64cd8607138ce00b371a61f16e179dfb074f536e","is_inters
titial":false,"latitude":62.redacted,"template_md5":"madlib-a028eeb4c
a56be2af0eb","exchange":"appodeal","is_skippable":null,"device_id":"5
2d0d5c2-e923-4b1b-bd67-d3b225795edb","vast_companion_types":null,"cou
ntry":"NOR"," ab_tests":["mopub-browser-experiment","applovin-mraid-
android-control","mraid-fallback-experiment","applovin-nv-end-card-ex
periment","orie ntation-test-experiment"],"platform":"android","heigh
t":50,"mraid":true,"madlib":true,"ad_language":"en-US","metrics":[{"m
etric-name":"image_load_time","metric-value":0}]}
```

Table 37. Request from the Muslim app to Liftoff containing inexact location information

This is not entirely dissimilar to the requests to Liftoff observed for Grindr and My Days, which also report an inexact location, although a different inexact location (presumed to be based on the IP address, rather than the city and zip code).

3.8 Tinder

Tinder is a popular dating app owned by the same company as OkCupid, Match Group. It allows users to view profile pictures from nearby users, and swipe to connect.

The app asks for permission to use location data. This is reasonable, since it is needed for the basic functionality of the app.

Tinder was mainly tested on July 8th, 11th, 12th, and 15th, with a re-test on September 20th.

3.8.1 General observations

We observed the Tinder app sending the advertising ID to the following parties:

- AppsFlyer (events.appsflyer.com)
- Branch (api.branch.io)
- Facebook (graph.facebook.com)
- Salesforce Audience Studio (Krux) (beacon.krxd.net)
- Tinder (etl.tindersparks.com)

Tinder sends age and gender as custom parameters to Google DoubleClick (*pubads.g.doubleclick.net*). Similarly to MyDays, Tinder **receives** the advertising ID in the responses from DoubleClick, even though the ad ID is not part of the requests. This demonstrates that Google perfectly well knows which device it is. We also observe traffic to Crashlytics for crash reporting / debugging.

There is significant traffic to *etl.tindersparks.com*, which appears to be Tinder’s own analytics service. It receives event data from the app roughly every minute, including GPS location, device information, carrier information, and user data such as age, gender, and gender filter.

3.8.2 User data transmission from Tinder to LeanPlum and AppsFlyer

During the technical tests, we observed **LeanPlum** and **AppsFlyer** receiving data from the app about the user’s GPS location, age and gender, as well as user attributes such as the “gender filter”. The gender filter describes which potential romantic partners the user is looking for, and is therefore a good indication of the user’s likely sexual orientation. These observations were made during the initial test in July, and subsequently confirmed during retest in September.

Table 38 and Table 39 shows two example transmissions in detail. The message bodies have been formatted and excerpted to increase legibility.

```
POST /api/v4/androidevent?buildnumber=4.9.0&app_id=com.tinder
HTTP/1.1
Content-Length: 3077
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: events.appsflyer.com
Connection: close
Accept-Encoding: gzip, deflate
```

```
{
  "country":"US",
  "af_timestamp":"1562921114662",
  "appsflyerKey":"XkJdrCAFbLCxnQ4SH7xon6",
  "af_events_api":"1",
  "isFirstCall":"false",
  "registeredUninstall":false,
  "operator":"Telenor",
  "network":"WIFI",
  "af_v2":"fe0109ff1445ffe259b2f1d1b0e06bd4da6605aa",
  "uid":"1562596650148-8175594770857825549",
  "eventValue":"{
    \"birthday\":\"491961600\",
    \"spotifyConnected\":false,
    \"appVersion\":\"10.18.0 (android)\",
    \"gender\":0,
    \"advertisingId\":\"52d0d5c2-e923-4b1b-bd67-d3b225795edb\",
    \"registered\":true,
    \"lon\":6.redacted,
    \"targetGender\":1,
    \"language\":\"en\",
    \"userSessionId\":\"2b142878-61e6-4ed0-b211-22a19080bdc6\",
    \"authId\":\"eBscmK5NhnA\",
    \"appBuild\":3390,
    \"platform\":2,
    \"uid\":\"5d28488d047f051600ff677a\",
    \"instanceId\":\"eBscmK5NhnA\",
    \"osVersion\":\"Android 8.1.0\",
    \"androidDeviceId\":\"1ca32d01353e564f\",
    \"pushEnabled\":true,
    \"model\":\"Nexus 5X\",
    \"appSessionId\":\"00e0bc8c-bb48-4c9a-9080-d0dfa7514e6e\",
    \"tinderPlus\":false,
    \"lat\":62.redacted,
    \"appSessionTimeElapsed\":163.45,
    \"anthemConnected\":false,
    \"manu\":\"LGE\",
    \"dataProvider\":\"wifi\",
    \"age\":\"33\",
    \"userSessionTimeElapsed\":11.705,
    \"ts\":1562921114434,
    \"Resume\":false}",
[…]
```

Table 38. Excerpt of data sent from the Tinder app to AppsFlyer (formatted for legibility)

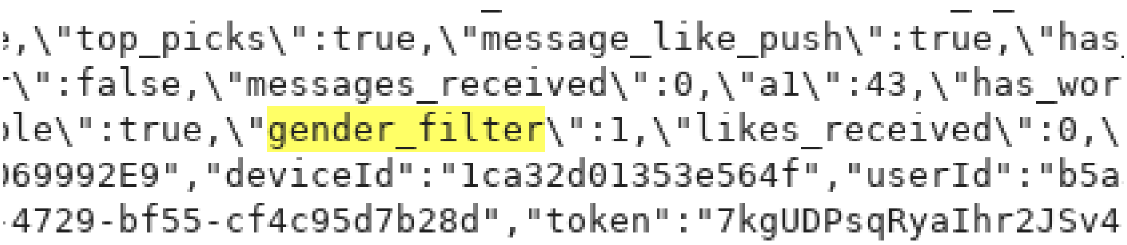
```
POST /api HTTP/1.1
User-Agent: Tinder/10.18.0/app_laEitk47uoJnyWx7Jn9Su85T6rcjovOYm3FfGY
CIgRk/android/4.2.1.0/Android OS/8.1.0/s
Content-Type: application/x-www-form-urlencoded
Host: api.leanplum.com
Connection: close
Accept-Encoding: gzip, deflate
Cookie: GOOGAPPUID=x
Content-Length: 9424
```

```
ata={
  "data":[
[...]
  {
    "newUserId":"b5a39abcfd56db24354b4c4e525248c14d0eeedb",
    "devMode":"false",
    "userAttributes":"{
      \"gender\":0,
      \"distance_filter\":50,
      \"f1\":false,
      \"likes_remaining\":0,
      \"squads_discoverable\":false,
      \"f2\":1,
      \"settings_push\":true,
      \"messages_push\":true,
      \"has_snapchat\":false,
      \"b1\":1,
      \"superlike_push\":true,
      \"b2\":\"2019-07-12T10:45:01.969+02:00\",
      \"uid\":\"5d28488d047f051600ff677a\",
      \"tinder_u_status\":0,
      \"smart_photos_connect\":false,
      \"is_select\":false,
      \"new_matches_push\":true,
      \"w1\":false,
      \"w3\":false,
      \"message_like_push\":true,
      \"has_bitmoji\":false,
      \"anthem_connect\":false,
      \"has_bio\":false,
      \"has_custom_gender\":false,
      \"a1\":43,
      \"has_work\":false,
      \"has_education\":false,
      \"a2\":23,
      \"spotify_connect\":false,
      \"signup_source\":\"sms\",
      \"discoverable\":true,
      \"gender_filter\":1,
      \"age\":33
    }",
[...]
```

Table 39. Excerpt of data sent from the Tinder app to LeanPlum (formatted for legibility)

While the example in Table 39 does not contain GPS coordinates, we did see GPS coordinates transmitted to LeanPlum – once on July 12th, once on July 15th, and 9 times in a 5-minute interval on September 20th.

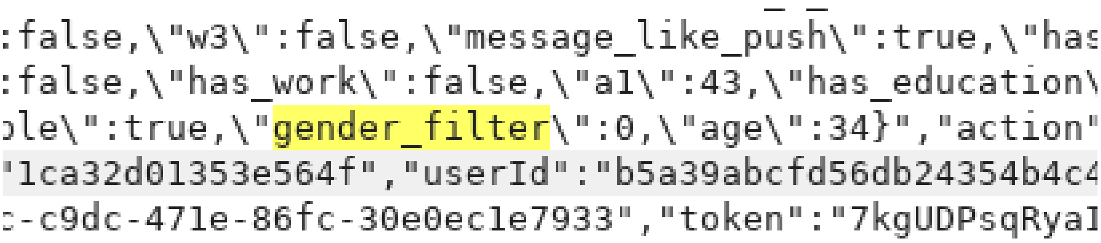
The `gender` and `gender_filter` parameters are encoded as integers, where zero (0) means “men”, one (1) means “women”, and minus one (-1) means “both”. The setting “**Show me**” in the Tinder app is reflected in the data that is being sent, as verified with transmissions to LeanPlum.



```
:,\"top_picks\":true,\"message_like_push\":true,\"has
-\":false,\"messages_received\":0,\"a1\":43,\"has_wor
ole\":true,\"gender_filter\":1,\"likes_received\":0,\
)69992E9","deviceId":"1ca32d01353e564f","userId":"b5a
-4729-bf55-cf4c95d7b28d","token":"7kgUDPsqRyaIhr2JSv4
```

Figure 5. Transmission from the Tinder app to LeanPlum when looking for women

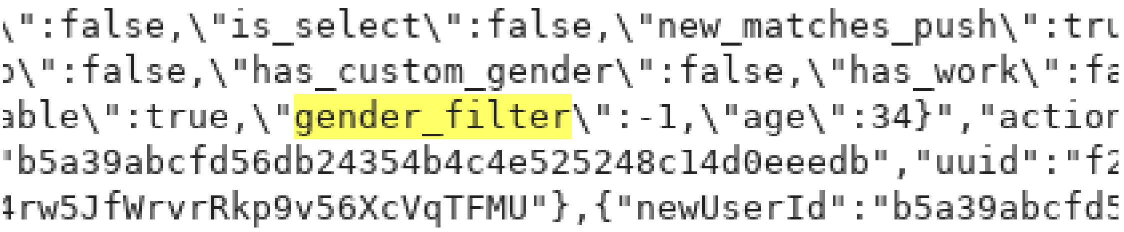
- Show me: Men



```
:false,\"w3\":false,\"message_like_push\":true,\"has
:false,\"has_work\":false,\"a1\":43,\"has_education\
ole\":true,\"gender_filter\":0,\"age\":34}","action"
"1ca32d01353e564f","userId":"b5a39abcfd56db24354b4c4
:-c9dc-471e-86fc-30e0ec1e7933","token":"7kgUDPsqRyaI
```

Figure 6. Transmission from the Tinder app to LeanPlum when looking for men

- Show me: Both



```
\":false,\"is_select\":false,\"new_matches_push\":tru
)\":false,\"has_custom_gender\":false,\"has_work\":fa
able\":true,\"gender_filter\":-1,\"age\":34}","actior
"b5a39abcfd56db24354b4c4e525248c14d0eeedb","uuid":"f2
4rw5JfWrvrRkp9v56XcVqTFMU"},{"newUserId":"b5a39abcfd5
```

*Figure 7. Transmission from the Tinder app to LeanPlum when looking for women **and** men*

Leanplum also appears to receive quite detailed information about app activity. For example, we see many transmissions where the event “Ad.View” is referenced.

3.9 Clue

Clue is a period tracker and fertility app where users can input a data related to fertility, health and lifestyle. It did not request any suspicious permissions.

Clue was mainly tested on July 4th, 5th, 11th, and 16th.

3.9.1 General observations

We observed the following third parties receiving the Android advertising ID.

- Adjust (app.adjust.com)
- Amplitude (api.amplitude.com)
- Facebook (graph.facebook.com)
- Google (app-measurement.com)

Other third parties receiving data include **Apptimize** and **Braze**. We also see **Crashlytics** used for crash reporting and analysis, though this appears to be innocuous.

The “Birth Year” and hence the age of the user is sent to both **Amplitude**, **Braze**, and **Apptimize**, and all the actors receive a significant amount of device information.

Requests to **Amplitude** contain events from within the GUI, we observed the following events being transmitted as parameters. The type and sequence of events might be used to infer how the app is being used.

```
"event_type":"Analysis Align Left",
"event_type":"Analysis Align Right",
"event_type":"Analysis Select Measurement",
"event_type":"Close Magic Box",
"event_type":"Device Info",
"event_type":"Exit Data Entry",
"event_type":"$identify",
"event_type":"Magic Box Card Shown",
"event_type":"Open Analysis",
"event_type":"Open Calendar",
"event_type":"Open Cycle View",
"event_type":"Open Data Entry",
"event_type":"Open Login/Signup",
"event_type":"Open Magic Box",
"event_type":"Open More Menu",
"event_type":"Open Tracking Options",
"event_type":"Select Menu Category",
"event_type":"Select Onboarding Method",
"event_type":"Select Onboarding Type",
"event_type":"session_end",
"event_type":"session_start",
"event_type":"Show Welcome Screen",
"event_type":"Stat Box Shown",
"event_type":"Tried To Get User Details",
```

Table 40. Event types transmitted from the Clue app to Amplitude

3.10 Happn

Happn is a location-based social network and dating app developed by the French FTW & Co. The app requests permission to use location data, which is expected since this is a central part of its functionality.

Happn was mainly tested on July 4th, 8th, 11th, and 16th.

3.10.1 General observations

We observed Happn sharing the user's advertising ID with two parties, as well as Happn itself:

- Adjust (app.adjust.com)
- Facebook (graph.facebook.com)

In addition to this, the app sent data to **Google** (DoubleClick) and **Braze** (AppBoy).

We did not observe the user's location or IP address being shared with third parties. The only unusual data sharing was found in some of the messages to DoubleClick, where user information is conveyed through custom parameters, similarly to what we found for OkCupid and Tinder. This is shown in Table 41.

```
GET /gampad/ads?[… selected request parameters shown below …] HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/75.0.3770.101 Mobile Safari/537.36 (Mobile; afma-
sdk-a-v17785019.17785019.0)
x-afma-drt-cookie: redacted
x-afma-drt-v2-cookie: redacted
Host: pubads.g.doubleclick.net
Connection: close
Accept-Encoding: gzip, deflate
```

Request parameters include:

```
url=595.android.com.ftw_and_co.happn.adsenseformobileapps.com

iu=%2F21677312273%2FNORWAY%2FANDROID%2FMALE%2FTIMELINE19

cust_params=excl_cat%26has_pending_likes%3Dfalse%26language%3Den%26ti
meline_version%3D3%26modulo%3D17%26android_app_version%3D24.7.0%26has
h%3D7759251861660347455%26is_buyer%3Dfalse%26days_since_register%3D0%
26age_segment%3DSEGMENT_25_34
```

By URL decoding the `iu` and `cust_params` parameters, we get:

```
iu=/21677312273/NORWAY/ANDROID/MALE/TIMELINE19

cust_params=excl_cat&has_pending_likes=false&language=en&timeline_ver
sion=3&modulo=17&android_app_version=24.7.0&hash=7759251861660347455&
is_buyer=false&days_since_register=0&age_segment=SEGMENT_25_34&
```

Table 41. Data transmission from the Happn app to Google Doubleclick

3.11 Wave Keyboard

This app acts as a system extension, replacing the default keyboard with other customised versions. It did not ask for any suspicious permissions, and we did not observe personal data being sent to third parties, apart from the advertising ID.

Wave was mainly tested on July 8th and 9th.

The following parties received the device advertising ID from Wave:

- Crashlytics (settings.crashlytics.com)
- Facebook (graph.facebook.com)
- Flurry (data.flurry.com)
- Onesignal (onesignal.com)

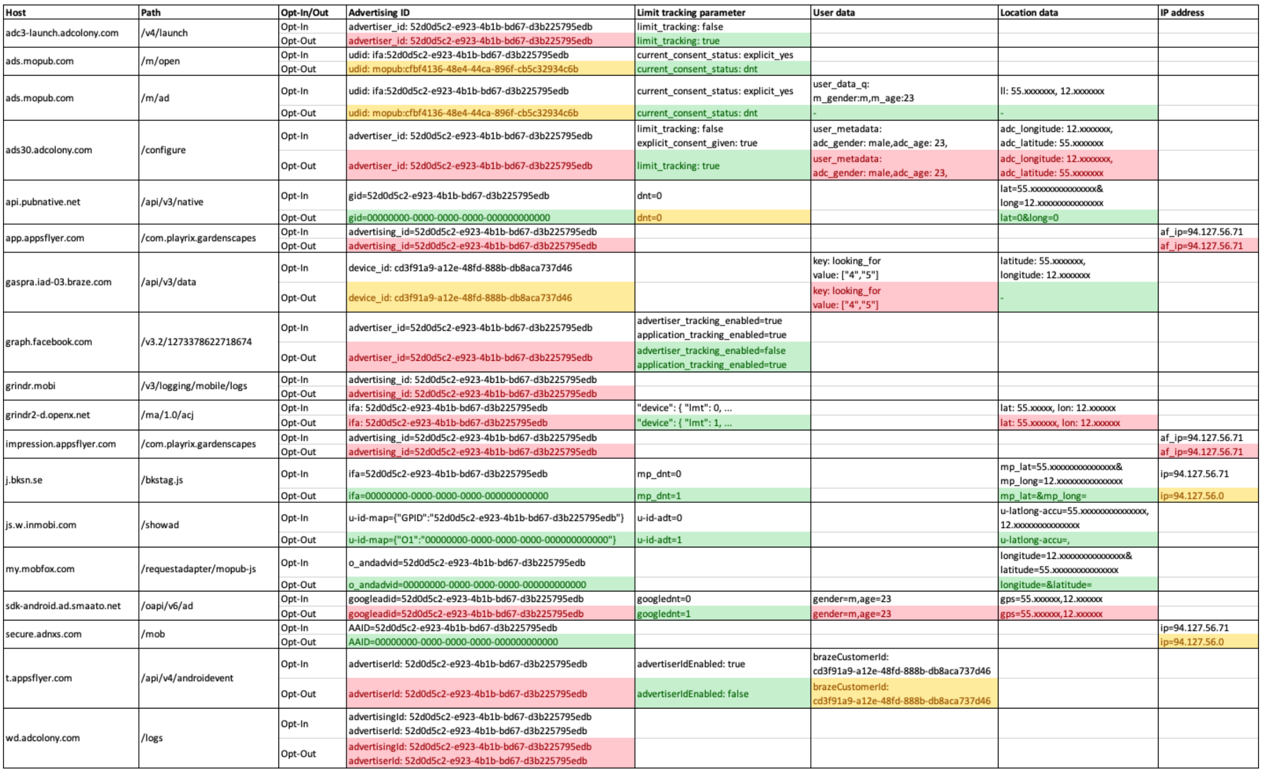
We also saw the usual advertising traffic to **Google** (DoubleClick).

3.12 The effect of opting out of ad tracking

The Android operating system offers a setting that can be used to opt out of ad tracking. This setting is there to protect users from being identified through the Android advertising ID. It’s not obvious how to find the setting, but on most phone models it’s a toggle button called “Opt out of Ads Personalization”, which can be found in *Settings / Google / Ads*.

In order for this opt-out to be effective, it has to be honored by the apps and in the SDKs. All the apps contain at least **some** reference to the setting in the decompiled code, but it is not obvious how it is used. Because of this, we did a brief test of the Grindr app with “opt out” both enabled and disabled, and compared the results.

In many of the observed data transmissions, the “opt out” setting had a limited effect on how user data such as the advertising ID, GPS position and IP address was treated. In Figure 9, we see a graphical representation of this.



Host	Path	Opt-In/Out	Advertising ID	Limit tracking parameter	User data	Location data	IP address
adc3-launch.adcolony.com	/v4/launch	Opt-In	advertiser_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	limit_tracking: false			
		Opt-Out	🟥 advertiser_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 limit_tracking: true			
ads.mopub.com	/m/open	Opt-In	udid: ifa:52d0d5c2-e923-4b1b-bd67-d3b225795edb	current_consent_status: explicit_yes			
		Opt-Out	🟨 udid: mopub:cfbf4136-48e4-44ca-896f-cb5c32934c6b	🟩 current_consent_status: dnt			
ads.mopub.com	/m/ad	Opt-In	udid: ifa:52d0d5c2-e923-4b1b-bd67-d3b225795edb	current_consent_status: explicit_yes	user_data_q: m_gender:m,m_age:23	ll: 55.xxxxxxx, 12.xxxxxxx	
		Opt-Out	🟨 udid: mopub:cfbf4136-48e4-44ca-896f-cb5c32934c6b	🟩 current_consent_status: dnt	🟩 -	🟩 -	
ads30.adcolony.com	/configure	Opt-In	advertiser_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	limit_tracking: false explicit_consent_given: true	user_metadata: adc_gender: male,adc_age: 23,	adc_longitude: 12.xxxxxxx, adc_latitude: 55.xxxxxxx	
		Opt-Out	🟥 advertiser_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 limit_tracking: true	🟥 user_metadata: adc_gender: male,adc_age: 23,	🟥 adc_longitude: 12.xxxxxxx, adc_latitude: 55.xxxxxxx	
api.pubnative.net	/api/v3/native	Opt-In	gid=52d0d5c2-e923-4b1b-bd67-d3b225795edb	dnt=0		lat=55.xxxxxxxxxxxxxxx& long=12.xxxxxxxxxxxxxxx	
		Opt-Out	🟩 gid=00000000-0000-0000-0000-000000000000	🟨 dnt=0		🟩 lat=0&long=0	
app.appsflyer.com	/com.playrix.gardenscapes	Opt-In	advertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb				af_ip=94.127.56.71
		Opt-Out	🟥 advertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb				🟥 af_ip=94.127.56.71
gaspra.iad-03.braze.com	/api/v3/data	Opt-In	device_id: cd3f91a9-a12e-48fd-888b-db8aca737d46		key: looking_for value: ["4","5"]	latitude: 55.xxxxxxx, longitude: 12.xxxxxxx	
		Opt-Out	🟨 device_id: cd3f91a9-a12e-48fd-888b-db8aca737d46		🟥 key: looking_for value: ["4","5"]	🟩 -	
graph.facebook.com	/v3.2/1273378622718674	Opt-In	advertiser_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb	advertiser_tracking_enabled=true application_tracking_enabled=true			
		Opt-Out	🟥 advertiser_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 advertiser_tracking_enabled=false application_tracking_enabled=true			
grindr.mobi	/v3/logging/mobile/logs	Opt-In	advertising_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb				
		Opt-Out	🟥 advertising_id: 52d0d5c2-e923-4b1b-bd67-d3b225795edb				
grindr2-d.openx.net	/ma/1.0/acj	Opt-In	ifa: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	"device": { "lmt": 0, ...		lat: 55.xxxxx, lon: 12.xxxxxx	
		Opt-Out	🟥 ifa: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 "device": { "lmt": 1, ...		🟥 lat: 55.xxxxxx, lon: 12.xxxxxx	
impression.appsflyer.com	/com.playrix.gardenscapes	Opt-In	advertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb				af_ip=94.127.56.71
		Opt-Out	🟥 advertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb				🟥 af_ip=94.127.56.71
j.bksn.se	/bkstag.js	Opt-In	ifa=52d0d5c2-e923-4b1b-bd67-d3b225795edb	mp_dnt=0		mp_lat=55.xxxxxxxxxxxxxxx& mp_long=12.xxxxxxxxxxxxxxx	ip=94.127.56.71
		Opt-Out	🟩 ifa=00000000-0000-0000-0000-000000000000	🟩 mp_dnt=1		🟩 mp_lat=&mp_long=	🟨 ip=94.127.56.0
js.w.inmobi.com	/showad	Opt-In	u-id-map={"GPID":"52d0d5c2-e923-4b1b-bd67-d3b225795edb"}	u-id-adt=0		u-latlong-accu=55.xxxxxxxxxxxxxxx, 12.xxxxxxxxxxxxxxx	
		Opt-Out	🟩 u-id-map={"O1":"00000000-0000-0000-0000-000000000000"}	🟩 u-id-adt=1		🟩 u-latlong-accu=,	
my.mobfox.com	/requestadapter/mopub-js	Opt-In	o_andadvid=52d0d5c2-e923-4b1b-bd67-d3b225795edb			longitude=12.xxxxxxxxxxxxxxx& latitude=55.xxxxxxxxxxxxxxx	
		Opt-Out	🟩 o_andadvid=00000000-0000-0000-0000-000000000000			🟩 longitude=&latitude=	
sdk-android.ad.smaato.net	/oapi/v6/ad	Opt-In	googleadid=52d0d5c2-e923-4b1b-bd67-d3b225795edb	googledntt=0	gender=m,age=23	gps=55.xxxxxx,12.xxxxxx	
		Opt-Out	🟥 googleadid=52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 googledntt=1	🟥 gender=m,age=23	🟥 gps=55.xxxxxx,12.xxxxxx	
secure.adnxs.com	/mob	Opt-In	AAID=52d0d5c2-e923-4b1b-bd67-d3b225795edb				ip=94.127.56.71
		Opt-Out	🟩 AAID=00000000-0000-0000-0000-000000000000				🟨 ip=94.127.56.0
t.appsflyer.com	/api/v4/androidevent	Opt-In	advertiserId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	advertiserIdEnabled: true	brazeCustomerId: cd3f91a9-a12e-48fd-888b-db8aca737d46		
		Opt-Out	🟥 advertiserId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb	🟩 advertiserIdEnabled: false	🟨 brazeCustomerId: cd3f91a9-a12e-48fd-888b-db8aca737d46		
wd.adcolony.com	/logs	Opt-In	advertisingId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb advertiserId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb				
		Opt-Out	🟥 advertisingId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb advertiserId: 52d0d5c2-e923-4b1b-bd67-d3b225795edb				

Figure 8. A summary of how opting out of ads personalization affects data transmission from Grindr. Green means that there is an observable difference, yellow means a partial difference, and red means that there is no change.

In most cases there is a parameter in the payload that correctly identifies the setting (such as `limit_tracking: true` or `false`), but we could observe the advertising ID quite often being transmitted anyway, even in the same request as the limit tracking parameter itself.

In some cases, we observed gender, age, GPS position and/or IP address being sent regardless of opt-out status. A specific example is given in Table 42, where AdColony is receiving a significant amount of data despite such an opt-out.

Opt out of Ads Personalization: **Disabled**

```
POST /configure HTTP/1.1
Accept-Charset: UTF-8
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36
Content-Type: application/json
Content-Length: 2731
Host: ads30.adcolony.com
Connection: close
Accept-Encoding: gzip, deflate

{"advertiser_id":"52d0d5c2-e923-4b1b-bd67-
d3b225795edb","carrier":"","custom_id":"","limit_tracking":false,"ln"
:"en","locale":"US", ...

"explicit_consent_given":true,"consent_response":true,"user_metadata"
:{"adc_gender":"male","adc_age":23,"adc_longitude":REDACTED,"adc_lati
tude":REDACTED,

... }
```

Opt out of Ads Personalization: **Enabled**

```
POST /configure HTTP/1.1
Accept-Charset: UTF-8
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36
Content-Type: application/json
Content-Length: 3084
Host: ads30.adcolony.com
Connection: close
Accept-Encoding: gzip, deflate

{"advertiser_id":"52d0d5c2-e923-4b1b-bd67-
d3b225795edb","carrier":"","custom_id":"256729490","limit_tracking":t
rue,"ln":"en","locale":"US", ...

"user_metadata":{"adc_gender":"male","adc_age":23,"adc_longitude":RED
ACTED,"adc_latitude":REDACTED,

...}
```

Table 42. Comparison of data sent from the Grindr app to AdColony, with and without opt-out from personalisation

In another example, AppsFlyer was receiving the IP address with the advertising ID in the same request, regardless of the opt out setting. This is shown in Table 43.

Opt out of Ads Personalization: **Disabled**

```
GET /com.playrix.gardenscapes?clickid=d3b67cb8d8da775b6342acd7dcb5808
99db0e039&redirect=false&c=GS_GP_WW_CPI_wl_v2_Low2&af_ua=Mozilla%2F5.
0+%28Linux%3B+Android+8.1.0%3B+Nexus+5X+Build%2FOPM7.181205.001%3B+wv
```

```
%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Version%2F4.0+Chro
me%2F78.0.3904.96+Mobile+Safari%2F537.36&af_click_lookback=30d&sha1_a
ndroid_id=&af_keywords=Grindr+LLC&af_ad=%28market%291920x1080_gs_vide
o400_pf_en_30s_12mb_options_gp_storeview&af_siteid=5201043537198df103
720afec1789c57593bcc58&pid=adcolony_int&app_id=com.playrix.gardenscap
es&advertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb&af_c_id=137548
&af_lang=en&af_sub3=vz9b79680498804b028f&af_sub1=com.grindrapp.androi
d&af_adset_id=137548&af_sub4=5a67c6431950bb953267065ec4ca940ede777aac
&af_ip=94.127.56.71&af_adset=GS_GP_WW_CPI_wl_v2_Low2&af_ad_id=214702&
af_sub_siteid=com.grindrapp.android&af_ref=d3b67cb8d8da775b6342acd7dc
b580899db0e039 HTTP/1.1
Accept-Charset: UTF-8
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36
Host: app.appsflyer.com
Connection: close
Accept-Encoding: gzip, deflate
```

Opt out of Ads Personalization: **Enabled**

```
GET /com.playrix.homescapes?clickid=3a487d1e3b0eb6bf4df79d7dffa501998
7fcc188&redirect=false&c=HS_GP_WW_CPI_wl_v2_Low2&af_ua=Mozilla%2F5.0+
%28Linux%3B+Android+8.1.0%3B+Nexus+5X+Build%2FOPM7.181205.001%3B+wv%2
9+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Version%2F4.0+Chrome
%2F78.0.3904.96+Mobile+Safari%2F537.36&af_click_lookback=30d&sha1_and
roid_id=&af_keywords=Grindr+LLC&af_ad=%28market%291080x1920_hs_video3
70_nb_en_30s_48mb_options_gp_storeview&af_siteid=5201043537198df10372
0afec1789c57593bcc58&pid=adcolony_int&app_id=com.playrix.homescapes&a
dvertising_id=52d0d5c2-e923-4b1b-bd67-d3b225795edb&af_c_id=137536&af_
lang=en&af_sub3=vz9b79680498804b028f&af_sub1=com.grindrapp.android&af
_adset_id=137536&af_sub4=5a67c6431950bb953267065ec4ca940ede777aac&af_
ip=94.127.56.71&af_adset=HS_GP_WW_CPI_wl_v2_Low2&af_ad_id=212740&af_s
ub_siteid=com.grindrapp.android&af_ref=3a487d1e3b0eb6bf4df79d7dffa501
9987fcc188 HTTP/1.1
Accept-Charset: UTF-8
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36
Host: app.appsflyer.com
Connection: close
Accept-Encoding: gzip, deflate
```

Table 43.Comparison of data sent from the Grindr app to AppsFlyer, with and without opt-out from personalisation

Our test results show that pushing the responsibility for handling the ads personalisation opt-out to the developers implementing the apps and SDKs does not work well in practice. It is a trust-based system which appears to have few verification or enforcement mechanisms built in, and might give users a false sense of security. In our opinion, joint transmission of IP and advertising ID from a user who has opted out of personalised ads is quite problematic.

3.13 Other noteworthy observations

3.13.1 Observations regarding public IP address

Quite a few of the apps share the IP address with various advertising companies. The IP address is an especially interesting piece of information since it can potentially be used as a persistent identifier. However, a device does not necessarily know its externally visible public IP, since it is likely to be sitting behind network address translation (NAT) on a private IP as defined in RFC1918.

As seen with Grindr (Chapter 3.2), the public IP address is received in the response from MoPub. There are several ways MoPub can get the IP address, it's for example present in the IP packet header. But in My Talking Tom 2 (Chapter 3.6), the response from IQzone contains placeholders and not the actual IP address. The fields are then populated by the app itself before being sent to any third parties.

One way for the app to figure out its IP address could be to ask an external server to return the public IP address. There are several such services (e.g. https://www.whatsmyip.org/) and we found traffic to one of these when testing two of the apps, My Talking Tom 2 and MyDays. A request is sent to http://checkip.amazonaws.com/ which simply returns the externally visible IP address of the device. This value can then be sent to other third-party companies.

Request:

```
GET / HTTP/1.1
Connection: close
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: checkip.amazonaws.com
Accept-Encoding: gzip, deflate
```

Response:

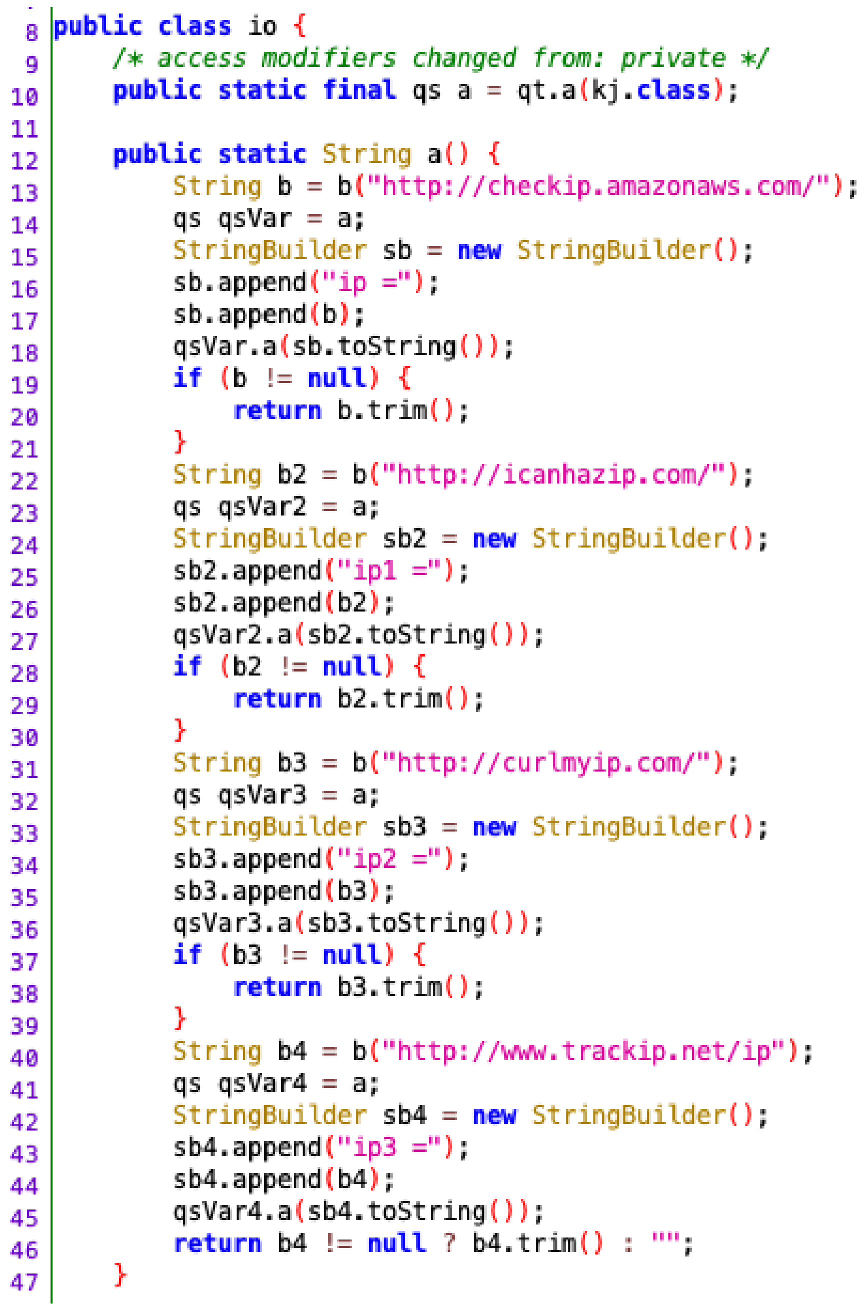
```
HTTP/1.1 200 OK
Date: Tue, 16 Jul 2019 09:32:42 GMT
Server: lighttpd/1.4.41
Content-Length: 13
Connection: Close

94.127.56.71
```

Table 44. Request from app to find its public IP address through a public service

As the app does not identify itself in the request, we cannot with certainty determine how and where this is done by the apps, by only inspecting the traffic.

When inspecting the decompiled source code for the My Talking Tom 2 app, we find references to the IP-check endpoint in the IQzone SDK. This suggests that IQzone is in fact using this method to figure out the public IP of the device.



```
public class io {
    /* access modifiers changed from: private */
    public static final qs a = qt.a(kj.class);

    public static String a() {
        String b = b("http://checkip.amazonaws.com/");
        qs qsVar = a;
        StringBuilder sb = new StringBuilder();
        sb.append("ip =");
        sb.append(b);
        qsVar.a(sb.toString());
        if (b != null) {
            return b.trim();
        }
        String b2 = b("http://icanhazip.com/");
        qs qsVar2 = a;
        StringBuilder sb2 = new StringBuilder();
        sb2.append("ip1 =");
        sb2.append(b2);
        qsVar2.a(sb2.toString());
        if (b2 != null) {
            return b2.trim();
        }
        String b3 = b("http://curlmyip.com/");
        qs qsVar3 = a;
        StringBuilder sb3 = new StringBuilder();
        sb3.append("ip2 =");
        sb3.append(b3);
        qsVar3.a(sb3.toString());
        if (b3 != null) {
            return b3.trim();
        }
        String b4 = b("http://www.trackip.net/ip");
        qs qsVar4 = a;
        StringBuilder sb4 = new StringBuilder();
        sb4.append("ip3 =");
        sb4.append(b4);
        qsVar4.a(sb4.toString());
        return b4 != null ? b4.trim() : "";
    }
```

Figure 9. Decompiled source code excerpt of the IQzone SDK, which is built into the My Talking Tom 2 app

The code shows that there are several backup URLs included, should the first one fail:

- checkip.amazonaws.com
- icanhazip.com
- curlmyip.com
- www.trackip.net/ip

3.13.2 Unattributed traffic to Tutela

During testing, we have observed about 60 requests to hail-reporting.tutelatechnologies.com. We have not been able to conclusively associate with a specific app, as the messages do not indicate which app sends the data, nor have we identified the Tutela SDK in any of the apps.

Transmissions to Tutela are primarily associated with the tests of MyDays and OKCupid, and a hypothesis is that one or both of these apps are the source of the traffic.

According to their own marketing material[30], "*Tutela collects and analyzes anonymous mobile network coverage and experience statistics from millions of mobile devices to deliver actionable insights to telecoms and other mobile companies.*"

A typical example of traffic, from August 7th, is shown in Table 45.

```
POST /v2/wifi HTTP/1.1
Content-Type: application/json
Accept: application/json
x-api-key: redacted
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build/OPM7.181205.001)
Host: hail-reporting.tutelatechnologies.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 438

{"timestamp":1565170461732,
"deploymentKey":"redacted",
"sdkVersion":"5.2.37",
"location":{"latitude":62. redacted,"longitude":6.redacted,
"horizontalAccuracy":10,"verticalAccuracy":-32768,"altitude":96},
"userAgent":"Dalvik\/2.1.0 (Linux; U; Android 8.1.0; Nexus 5X
Build\/OPM7.181205.001)",
"id":{"tutela":"71A479330889A835"},
"bssid":"02:69:d8:5c:7c:ac",
"ssid":"testnetwork"}
```

Table 45. Traffic from unknown mobile app to Tutela Technologies

We see that Tutela receives information about the GPS location of the user, as well as the connected wifi network's SSID and BSSID.

3.13.3 Unattributed traffic to AreaMetrics

During testing, we have observed around 70 requests to api.areametrics.com, for which we have not been able to identify the app or apps behind. The AreaMetrics SDK was also found in Perfect365, which makes it a likely suspect, but our log data appears inconclusive.

[30] Source: https://www.tutela.com/

All requests observed contain the same `vendor_id=d9f0a4c8-bf68-385b-a8ff-a37e041df86f` parameters, which may indicate that the same app/vendor caused all requests. We have not been able to identify which vendor this is based on the ID.

```
GET /v3/user_init?pub_id=844ca42ce005ad86647673e7a9320e9fa19b65a1acaf
d7d8ee6d615ea3994e80&snippet_ver=1.5&ad_id=52d0d5c2-e923-4b1b-bd67-d3
b225795edb&os_ver=8.1.0&os=android&vendor_id=d9f0a4c8-bf68-385b-a8ff-
a37e041df86f&loc_permission=authorized&model=LGE%20Nexus%205X&locale=
US HTTP/1.1
Host: api.areametrics.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.0
```

Table 46. Traffic from unknown mobile app to AreaMetrics

The user agent okhttp/3.12.0 corresponds to the popular okhttp client[31], which appears to be present in most or all the apps. Thus this does not help us identify the app either.

3.13.4 Correlating traffic from multiple sources – AppsFlyer example

Many of the parties we have observed during testing receive information from multiple apps. It is interesting to look at how this information can be combined.

AppsFlyer’s SDK is used by both Grindr, OkCupid, My Talking Tom 2, and Tinder, and provides a good example of how data may be combined from multiple apps. Table 47 compares 4 requests sent to AppsFlyer from different apps.

Parameter	Grindr	OkCupid	MTT2	Tinder
app_id	com.grindrapp.android	com.okcupid.okcupid	com.outfit7.mytalkingtom2	com.tinder
af_timestamp	Aug 07 2019 9:43am (UTC)	July 15 2019 4:04pm (UTC)	July 04 2019 2:21pm (UTC)	July 12 2019 8:45am (UTC)
appsflyerKey	pP6nnscAupjjqd43siuNfV	XkJdrCAFbLCxnQ4SH7xon6	56VQKaum5gTk8JGG75PKWm	XkJdrCAFbLCxnQ4SH7xon6
lang_code	en	en	en	en
operator / carrier	Telenor	Telenor		Telenor
model / brand	Nexus 5X google	Nexus 5X google	Nexus 5X google	Nexus 5X google
advertiserId	52d0d5c2-e923-4b1b-bd67-d3b225795edb	52d0d5c2-e923-4b1b-bd67-d3b225795edb	52d0d5c2-e923-4b1b-bd67-d3b225795edb	52d0d5c2-e923-4b1b-

[31] https://github.com/square/okhttp

				bd67-d3b225795edb
appUserId	233335973	7906987202621823856		b5a39abcfd56db24354b4c4e525248c14d0eeedb
app_version_name	5.12.2	30.3.2	1.4.2.514	10.18.0
deviceData	Information about CPU, display including dimensions, and battery level	Information about CPU, display, battery level, **and** sensor data from magnetometer, gyroscope, and accelerometer	Information about CPU, display, and battery level	Information about CPU and display including dimensions

Table 47. Comparison of transmissions to AppsFlyer from multiple apps, selected parameters

In addition to the above, there are several custom data fields being sent by some of the parties. These are yet more interesting, because they allow AppsFlyer to build a more complete profile of the user.

- Tinder transmits events, containing a selection of user data: Birthday, gender, targetGender, latitude / longitude, age, and more, as described in Chapter 3.8. This would allow very precise enrichment of data from the other sources.
- Grindr transmits the Braze customer ID from the app as part of `customData`: `\”brazeCustomerId\”:\”cd3f91a9-a12e-48fd-888b-db8aca737d46\”`. Although the Braze ID seems to be app specific, this could allow AppsFlyer to correlate additional data received via Braze.
- MTT2 transmitted the `customData` parameter: `\”san_gate\”:\”false\”`, though we do not know what this is for.
- OkCupid transmits detailed information about the device’s sensors, and we are not sure how this could be used
- The appUserId parameters could allow AppsFlyer to identify partial data coming from the same apps through other sources

We also notice that the `appsflyerKey` for OkCupid and Tinder are the same, possibly because both apps are part of Match Group.

The fact that a given user is using apps X, Y, and Z is in itself interesting. That someone uses both Grindr, Tinder, and OkCupid, combined with their respective usage patterns (and changes in usage patterns over time), together with the other application data that is being transmitted, gives a pretty good indication of relationship status, sexual preferences, as well as dating activity.

4 Test environment and methodology

4.1 Summary

The purpose of this section is to describe mnemonic's experimental setup and test methodology in additional detail, and discuss and clarify the advantages as well as limitations of our setup.

The mobile apps we are trying to monitor are black-box installations where we do not have access to original source code or documentation, nor the cooperation of the app creators. At the same time, we want to gain insight into aspects such as:

- Which back-end services and third parties do the apps communicate with
- How much, how often, and in what order, do they communicate
- Which data elements are being transmitted, and to whom

Our main approach to data collection has been traffic analysis. Data transmitted from the mobile applications has been routed through our lab environment, and captured for analysis. Because most traffic is encrypted, we have installed a trusted root certificate on the test devices, and used an explicit proxy to decrypt the TLS connections.

A secondary approach has been static analysis and decompilation of the Android application packages (APKs), in order to gain additional insight into how the apps work.

One fundamental limitation should be stated up front: our experimental setup is only able to analyze direct transmissions from the mobile apps to back-end service endpoints. Any secondary relaying or data sharing between the various third parties, potentially also including additional parties, will not be visible to us.

4.2 Test device description

The test device used for all tests was a rooted[32] Android device with the following specification:

- Phone model: Google (LG) Nexus 5X
- Hardware serial number: 00bda51b37d0aaee
- Operating system: Android 8.1.0
- Android advertising ID: `52d0d5c2-e923-4b1b-bd67-d3b225795edb`
- Opt out of personalized ads: OFF

[32] https://en.wikipedia.org/wiki/Rooting_(Android)

4.3 Test environment description

Apps have been installed on an Android test device, owned by mnemonic. The device is connected to a dedicated wireless network[33], which routes all data traffic through mnemonic's test infrastructure. Because of this, we are able to monitor the traffic sent by the phone. No other devices but the dedicated testing device was connected to the wireless network during testing, to be certain that the traffic was in fact generated by the specific device. Internet access is provided through mnemonic's ISP, with all traffic having external IP within the 94.127.56.64/26 subnet.

Our test devices are rooted, and has a custom root certificate installed. Because the certificate is trusted on the device, we are able to send the traffic through an intercepting HTTP proxy[34], such as Burp Suite, in order to decrypt TLS and capture the traffic in a readable format. The fact that the devices are "compromised" in this sense, is the mechanism that allows us to bypass the TLS encryption.

Two of the apps, *Grindr* and *Muslim: Qibla Finder*, attempt to check whether they are being run in a compromised environment, and initially refused to start when connected to our test infrastructure. This required additional workarounds on our side in order to intentionally bypass these safeguards. For the benefit of future researchers, we note that we had most success using dynamic instrumentation tools such as Frida[35].

In parallel with the traffic analysis, frameworks such as Exodus Privacy[36] and MobSF[37] have been used for static analysis. We have also disassembled code using jadx and smali/baksmali[38], amongst other things to verify whether specific third party SDKs are present in the application packages on the device.

4.4 Test protocol

All apps were installed and tested on the same test device, and tested using synthetic personal data and dummy user accounts. We did not manually update the apps during the test period.

Naively, running all the apps on the same device might lead to issues where it could be difficult to tell apart network requests made by different apps. In practice, this was not generally an issue, as almost all HTTP requests made by the apps explicitly identify the app that sent them. For example, an Android WebView will automatically set the custom X-Requested-With HTTP header on any requests made from the WebView. The header contains the package name of the app, unless this is explicitly disabled in code. Furthermore, many of the integrations we observed

[33] mnemonic also has the possibility to use a dedicated APN to capture mobile data traffic as well, but this capability was not used as part of the assessment
[34] It would be possible to use similar techniques to intercept or decrypt other application protocols
[35] https://www.frida.re/
[36] https://exodus-privacy.eu.org/en/
[37] https://github.com/MobSF/Mobile-Security-Framework-MobSF
[38] https://github.com/JesusFreke/smali

would actually send the package name and version as a parameter in JSON data. Examples of this are shown in Table 48.

Generic http header set by Android:

```
X-Requested-With: com.grindrapp.android
```

Custom http headers set by a particular advertising framework:

```
P-APPINFO: com.chris.mydays/2.9.5
app_id: com.arcsoft.perfect365
```

Application data parameters:

```
{"name":"app_bundle_id","value":"com.chris.mydays"},
"bundle": "com.grindrapp.android","ver": "5.12.2"
```

Table 48. Examples of app identifiers observed in traffic

In a few cases, the app causing a given network transmission was not conclusively identified. In particular, Tutela is an example of this, as described in Chapter 3.13.2.

It is also worth noting that merely having multiple apps installed may generate a significant amount of baseline traffic, if the apps have many third-party trackers installed. This is the case even when the apps are not running in the foreground. In order to limit the traffic, we only tested one app at a time, and all apps not currently being tested were "force stopped" to prevent them from sending data in the background.

During testing, we discovered that the Perfect365 app could not be force stopped, as it kept running in the background at all times, continuing to transmit data. This observation was not done for any other apps, which made it a bit more noticeable. After the Perfect365 app was updated on Google Play on or near September 18th, this behaviour ceased, according to a re-test we carried out after the update.

Most of the apps require users to accept the terms of service when the apps are run for the first time. While a user could refuse to accept the terms of service in general, not accepting the terms lead to not being able to use the app at all. In general, the apps did not have individual "opt out" settings to control the possibility of which data is shared with third parties.

The Android operating system provides a system-wide setting to "opt out" from ad personalization in general, although this switch can be somewhat hard to find. The general setting, as described in the Android developer documentation[39], requires the app developer to explicitly read this setting and take action accordingly in their code. As such, opting out in the settings will not have any effect on which data is being shared by an app, unless the app developer explicitly has implemented code to honor this setting.

Sampling conducted on a few of the apps indicate that the effect of the "opt out" setting is limited in practice, and that it in many cases is not honored. The Grindr app was tested with this setting both enabled and disabled to give a concrete example of how much effect opting out has on data sharing. This is described in Chapter 3.12. Apart from this experiment, testing was generally conducted without a system-level opt-out from personalization.

[39] https://developer.android.com/training/articles/user-data-ids

4.5 Known limitations of technical setup

The experimental setup is quite conservative, in the sense that it does not produce false positives. When we see a request being sent through our proxy, we know that it is real traffic, and we can identify which app it was sent by. On the other hand, the experimental setup has limitations which could lead to false negatives, in the sense of potential data transmission and interactions with third parties that we are not able to observe.

1. As stated previously: any back-end retransmission or sharing of data would not be possible to observe directly[40], since we do not control the back-end infrastructure, nor have any insight into it
2. The experiments have been carried out from a limited number of physical locations, a limited number of test devices, and from a single country (Norway)
3. If an app sends certain messages rarely, or under very specific conditions, we may not be able to trigger or observe transmissions during our test
4. Other security protocols than TLS (such as SSH and IPSEC) would need a dedicated approach in order to carry out man-in-the-middle attacks and gain access to traffic
5. Apps that implements explicit hardening techniques to protect its users from surveillance or prevent reverse-engineering, could cause problems with our current data collection approach, although different observation techniques could be feasible to depending on the types of countermeasures
6. Speculatively, if backend infrastructure is actively trying to detect clients behaving oddly or attempting to reverse engineer the system (such as our research), the systems might change their advertising behaviour adaptively as a result

On the balance, we feel that the setup we chose gives a good trade-off between technical simplicity, and reducing false negatives.

An additional data source which was not used to a significant extent during the experiment, would be to look at DNS queries as well as HTTP, as DNS traffic is generally not encrypted (although DNS over HTTPS is undergoing trials). This is suggested as a possible future improvement to the testing protocol. On the other hand, the ongoing move towards DNS over HTTPS actually makes analysis easier, since it means that the DNS traffic is visible without adding additional data sources.

Our analysis approach also tends towards false negatives, as the sheer amount of data makes it very time-consuming to analyse all interactions in detail. Because of that, we would not be surprised if additional deep analysis of the data would lead to additional findings.

4.6 Personal data

All testing was carried out using synthetic personal data, working from company-owned devices, and connecting to the Internet through mnemonic’s ISP. However, during testing, we realized

[40] It would be feasible to submit unique identifiers to each of the back-ends and try to discover any sharing of these through indirect means, but that would be a separate and quite different experiment.

that location information such as GPS coordinates and information about the neighbouring wireless networks (wifi as well as cellular networks) was collected by some of the apps.

As this information might be used to identify one of the researchers, all such information has been redacted from the data published in this report.

4.7 Generality of results

Because the test setup has been designed to avoid false positives, we believe that our test results are **representative** for the type and amount of data collection and sharing other Norwegian users of these apps would have been subject to, within the time period of the test (mainly July – August 2019, but also including the retests as described). If anything, due the flaws in our detective capabilities leading to potential false negatives, our findings give a lower bound of sorts for the amount of personal data that is being collected and distributed by the apps.

However, due to the dynamic nature of Internet advertising, somebody trying to re-do the experiment are likely to see different **detailed** results, due to factors such as:

- Changes and updates to the various apps between testing, publication, and re-test
- Changes and updates to the Android operating system
- Differences in geographical location, possibly also related to local privacy regulations
- Differences within the ad ecosystem (e.g. different ads, different parties) stemming from the difference in time between testing, publication, and re-test
- Differences in user profiling on the test devices, leading to different ad targeting

While these random factors imply that our results are not deterministically reproducible on the detailed level, the big picture would remain the same in a re-test, barring any major technical or functional changes by the app developers. Structural factors, such as the use of advertising platforms and brokers such as MoPub, should also remain the same.

Finally, we note that the app vendors generally did not force us to update the apps during testing[41]. Because of this, we expect that real-world users are distributed across a variety of app versions, in most cases probably including the exact same app versions that we tested on.

[41] There is one exception to this: Grindr forced us to update from 5.12.2 to 5.24.1 during the final re-test in late December 2019. Version 5.12.2 was used for testing between July and November.

5 About the report

5.1 Test execution

Project name	Out of control
Client	Norwegian Consumer Council
Conducted by	mnemonic AS
Consultants	Andreas Claesson (lead investigator) and Tor E. Bjørstad
Internal QA	Inger Karin Andersen, Andreas Furuseth
Start date	2019-05-28
End date	2020-01-13

Table 49. Project metadata

5.2 Document version control

All major document revisions are documented in the table below.

Version	Date	Consultant(s)	Comment
1.0	2020-01-13	Andreas Claesson, Tor E. Bjørstad QA team	Approved for publication
0.9	2019-12-13	Andreas Claesson, Tor E. Bjørstad	Complete version for QA
0.5 to 0.8	2019-11-07 to 2019-12-04	Andreas Claesson, Tor E. Bjørstad	Incremental working drafts shared internally within project team
0.4	2019-10-30	Tor E. Bjørstad	Initial draft shared to indicate overall report structure
0.1	2019-08-09	Tor E. Bjørstad	Initial methodology draft

Table 50. Document version control

5.3 Project timeline

The project has been carried out in multiple phases throughout the latter half of 2019.

- A pilot phase and proof of concept was carried out, starting at the end of May, and running through June

- The main phase of the project began on July 3rd, and continued through the summer holidays, roughly until the end of August
- September was used for verification and analysis
- Reporting has taken place from October to December
- Final polish and verification have taken place in December and early January 2020

Appendix A: List of apps and versions

The following apps and versions were used for the test.

App	Package name	Version
Grindr	com.grindrapp.android	5.12.1 / 5.12.2 5.24.1[50]
Perfect365	com.arcsoft.perfect365	7.83.3 / 7.99.8
My Days	com.chris.mydays	2.9.5
OkCupid	com.okcupid.okcupid	30.3.2 / 30.3.3
My Talking Tom 2	com.outfit7.mytalkingtom2	1.4.2.514
Muslim: Qibla Finder	com.hundred.qibla	4.1.24
Tinder	com.tinder	10.18.0
Clue	com.clue.android	5.16.0
Happn	com.ftw_and_co.happn	24.7.0
Wave Keyboard	com.wave.keyboard	1.63.4

Table 51. List of apps and versions

To simplify analysis, we have tried to keep the app version constant during the test, rather than continually updating as new versions are released.

[50] Version 5.24.1 was briefly used for re-testing during December 2019, as it was not possible to continue testing on the old version. This is the only instance we have seen of an app forcing its users to update.

Appendix B: List of identified third parties

The following **135 third parties** were explicitly identified during the test, as having either an SDK integration or some type of interaction with one or more of the apps, such as a HTTP request. Table 52 gives a brief introduction to each of them. The descriptive quotes are all sourced from the respective home pages.

Due to mergers and acquisitions within this technology space, the companies change names or ownership frequently, which makes it hard to identify some parties and complicates the overview. We have attempted to identify situations where a company operates under multiple names or brands on a best-effort basis.

The **total number of unique domains** (i.e. *.example.com) observed in test traffic is **216**. However, this figure includes multiple domains that belong to the same company, and excludes companies who have SDKs, but where we did not see traffic. For example, all of googleadservices.com, google-analytics.com, googleapis.com, googlesyndication.com, googletagservices.com, googleusercontent.com, googlevideo.com, and of course google.com are in the list of unique domains. There are also some domains where we were unable to identify the owner. We have not actively tried to deduplicate and consolidate the full list of domains by hand.

Name	Home page	Quote
33across (Tynt)	https://www.33across.com/	*"We build technology that delivers consumer attention"*
Aarki	https://www.aarki.com/	*"Elevate your mobile marketing"*
Acuity Ads	https://www.acuityads.com/	*"We are a decision science company that empowers businesses to make smarter decisions"*
AdBuddiz	https://www.adbuddiz.com	*"Full screen ads"*
AdColony	https://www.adcolony.com/	*"Elevating mobile advertising by focusing on the highest quality consumer experiences"*
Adelphic	https://www.adelphic.com/	*"Adelphic's enterprise-ready programmatic software helps agencies, brands and other large media buyers engage with consumers across all devices and formats"*
AdForm	https://site.adform.com/	*"Adform is one of the leading advertising technology companies in the world and provides the software used by buyers and sellers to automate digital advertising."*
Adition	https://www.adition.com/	*"Der Full Stack für das effiziente Management Ihres digitalen Werbegeschäfts und Ihrer Programmatic Advertising Kampagnen"*

Adjust	https://www.adjust.com/	*“the Mobile Measurement Company: we unify all your marketing”*
Admedo	https://www.admedo.com/	*“the only fully transparent Programmatic Marketing Platform on the market with all the tools needed in one UI at one cost.”*
Admixer	https://admixer.com/	*“Our core business is Publisher's wealth and our goal is to simplify ad serving processes of digital ad management for all sides.”*
Adobe (Everesttech)	https://www.adobe.com/advertising/adobe-advertising-cloud.html	*“the only independent ad platform that unifies and automates all media, screens, data, and creativity at scale”*
Adtelligent (Vertamedia)	https://adtelligent.com/	*“enable publisher ad technology independence”*
Amazon Advertising	https://advertising.amazon.com/	*“Ad solutions to help you find, attract, and engage millions of Amazon customers at every stage of their journey”*
Amobee (Turn, Singtel)	https://www.amobee.com/	*“unifies all advertising channels—including TV, programmatic and social—across all formats and devices”*
Amplitude	https://amplitude.com/	*“helps you use customer data to build great product experiences that convert and retain users.”*
AOL (One by Aol, Millennial Media, Nexage)	https://www.onebyaol.com/sites/all/themes/aolplatforms/pf/	*“the most engaging, high-impact premium ad capabilities”*
AppLovin	https://www.applovin.com/	*“Boost your revenue and engage your users—all in one place”*
AppMonet	https://appmonet.com/	*“Connecting brands to apps and apps to brands”*
AppNexus (Xandr, AT&T)	https://www.appnexus.com/ https://www.xandr.com/	*“AppNexus Powers The Advertising That Powers The Internet”*
Appodeal	https://www.appodeal.com/	*“Publishers First Ad Monetization”*
AppsFlyer	https://www.appsflyer.com/	*“the world's leading mobile attribution & marketing analytics platform”*
Apptimize	http://apptimize.com/	*“the most powerful solution for optimizing the entire user experience across messaging channels and digital properties”*
AreaMetrics	https://areametrics.com/	*“Geo-location data that powers business intelligence”*

BannerFlow	https://www.bannerflow.com/	*“Our Creative Management Platform lets you design, scale, publish, analyse, personalise, and optimise your display campaigns in-house.”*
Beeswax	https://www.beeswax.com/	*“provides sophisticated buyers with the transparency, flexibility, and control you need to make the most out of your programmatic spend.”*
Bidswitch	https://www.bidswitch.com/	*“neutral middleware that allows connected programmatic technology partners to seamlessly access new platforms and services; optimize bidstream performance and generate technical costs efficiencies”*
Bidtheatre	https://www.bidtheatre.com/	*“One platform to target and understand your digital audiences with banner & video campaigns, across all devices”*
Branch	https://branch.io/	*“Increase mobile revenue with enterprise-grade links built to acquire, engage, and measure across all devices, channels, and platforms”*
Braze (Appboy)	https://www.braze.com/	*“Humans are complicated. Customer engagement shouldn’t be.”*
Bucksense	https://www.bucksense.com/	*“In-house marketing, done right.”*
Bugsnag	https://www.bugsnag.com/	*“Bugsnag monitors application stability so you can make data-driven decisions on whether you should be building new features, or fixing bugs.”*
Cedato	https://www.cedato.com/	*“Our predictive video advertising software makes it possible for native video to run on any screen and placement, enhancing value, yield and viewing experience.”*
Celltick	https://www.celltick.com/	*“a global leader of mass mobile communication products for homeland security and mobile marketing serving over 1 billion mobile users in over 20 countries”*
Centro	https://www.centro.net/	*“Whether it’s driving performance across your campaigns, team, or business—you’ll do more using our technology”*
ChartBoost	https://www.chartboost.com/	*“the leading in-app monetization and programmatic advertising platform”*
Chocolate (Vdopia)	https://chocolateplatform.com/	*“Worlds' First Video SSP With 100% Server-Side Auctions”*

Colpirio	https://www.colpirio.com/home/	*“real-time behavioral targeting and product recommendation based on powerful machine learning and predictive analytics.”*
Comscore	https://www.comscore.com/	*“Measure what matters to make cross-platform audiences and advertising more valuable”*
Conversant (Dotomi, Publicis, Epsilon)	https://www.conversantmedia.com/	*“Evolve from digital distractions to real interactions”*
Criteo	https://www.criteo.com/	*“Grow your business with best-in-class advertising technology solutions.”*
DataXu (Roku)	https://www.dataxu.com/	*“helps marketing and media professionals use data to improve their advertising”*
Delta Projects	https://deltaprojects.com/	*“Our technology does all the heavy lifting, letting you speak directly to the right people at the right time.”*
District M	https://www.districtm.net/	*“district m’s complete programmatic ecosystem; which offers transparency, quality ad placements, and some of the lowest fees in the industry”*
Embrace	https://embrace.io/	*“We make finding and fixing errors on mobile too easy”*
EMX	https://emxdigital.com/	*“constantly improving the industry for marketers, publishers and platform partners by offering end-to-end managed service, proprietary monetization tools and patented technology advancements”*
Facebook	https://www.facebook.com/business/ads	*“Target future customers and fans”*
Flurry	https://www.flurry.com/	*“The World’s Most Adopted App Analytics”*
Fluxloop	https://fluxloop.com/	*“actionable insights through real-time location and behavioural data”*
Fyber (Inner-Active)	https://www.fyber.com/	*“a new era of app monetization”*
Fysical (Beaconsinspace)	https://fysical.com/	*“High Accuracy Place Visit Data”*
GetIntent	https://getintent.com/	*“Our highly customizable AI-powered programmatic suite empowers agencies, publishers, broadcasters and content owners with an essential tool to grow their programmatic revenues”*

Glispa (AvoCarrot)	https://www.glispa.com/	*"Data-driven programmatic exchange, made simple"*
Google (Doubleclick and others)	https://marketingplatform.google.com/	*"a unified advertising and analytics platform for smarter marketing and better results"*
GumGum	https://gumgum.com/	*"We use our proprietary computer vision technology to identify content relevant to marketers to deliver highly visible advertising campaigns and rich insights to brands and agencies"*
iBillboard	http://www.ibillboard.com/en/	*"Our mission is to help publishers and advertisers to use the online ad inventory to the satisfaction of both parties"*
IgnitionOne	https://ignitionone.com/	*"IgnitionOne Customer Intelligence seamlessly integrates with your existing advertising and marketing stack to help you find, value, and engage your customers in real-time."*
Improve Digital	https://www.improvedigital.com/	*"Improve Digital is the leading European Programmatic Advertising Platform for Publishers, Content Providers and Broadcasters"*
Infectious Media	https://www.infectiousmedia.com/	*"We want better advertising for everyone"*
InMobi	https://www.inmobi.com/	*"We help brands understand, identify, engage and acquire consumers"*
Instagram	https://business.instagram.com/advertising/	*"Drive awareness, increase customers and share your story among a highly engaged audience"*
Integral Ad Science	https://integralads.com/	*"For digital ads to make an impact on consumers, they have to be seen. We help you reach consumers by making sure all ads have the opportunity to be viewed. By real people."*
IQZone	https://iqzone.com/	*"Global in-app demand at scale"*
IronSource	https://www.ironsrc.com/	*"technologies that help app developers take their apps to the next level, including the industry's largest in-app video network, a robust mobile ad mediation platform, and a data-driven user acquisition platform"*
Kin Ecosystem	https://www.kin.org/	*"A new way to engage, grow, and monetize your digital community. The ultimate win win"*

Kochava	https://www.kochava.com/	*“Kochava enables people-based marketers to establish and enrich user identities, segment and activate audiences, and measure and optimize their campaigns across all connected devices”*
LeanPlum	https://www.leanplum.com/	*“Leanplum helps you create personalized customer experiences so you can convert more one-time users into customers”*
Liftoff	https://liftoff.io/	*“Acquire Users Who Generate the Best ROI for Your App”*
Linkedin	https://business.linkedin.com/marketing-solutions/ads	*“Reach your ideal customers on the world's largest professional network”*
Lotame	https://www.lotame.com/	*“Lotame's real-time data management technologies, global data marketplaces, and award-winning customer service make our unstacked data solutions the clear choice”*
MarsVideo	https://mars.video/	*“we engage in a range of direct brand campaigns from around the world, providing a full-service, multi channel monetization solution that meets both advertiser demand and publishers needs while using targeting and optimization techniques”*
Media.net	https://www.media.net/	*“Tap into one of the largest pools of advertisers in the world and let our ads maximize your monetization”*
MediaMath	https://www.mediamath.com/	*“the acclaimed independent advertising technology company for brands and agencies”*
Mintegral	https://www.mintegral.com/en/	*“We help advertisers and mobile publishers worldwide to bridge the gap between the East and West and simplify the challenges of cross-regional mobile marketing, driving truly global growth to their business”*
Moat	https://moat.com/	*“Real-time, multi-platform, and actionable marketing analytics”*
Mobfox	https://www.mobfox.com/	*“The preferred in-app advertising platform”*
MoPub	https://www.mopub.com/	*“monetization solutions for mobile app publishers and developers around the globe”*

MParticle	https://www.mparticle.com/	*"The best customer experiences begin with the right data"*
MyTarget	https://target.my.com/	*"Find new customers with myTarget — the self-service ad platform by Mail.ru Group that covers 96% of the Russian market"*
Neura	https://www.theneura.com/	*"Integrate real-world segments and triggers to your marketing campaigns at scale"*
Nielsen (Exelator)	https://www.nielsen.com/us/en/solutions/capabilities/nielsen-marketing-cloud/	*"Using built-in analytics and Nielsen Artificial Intelligence (AI), our cloud is constantly evaluating the success of your marketing and making adjustments in real-time.."*
Ogury Presage (Adincube)	https://www.ogury.com/	*"Consumers expect choice and control over their digital marketing experience"*
OneAudience	http://www.oneaudience.com/	*"Most mobile impressions are served to a scattered audience of unengaged strangers. oneAudience connects app developers, advertisers and publishers to real, verified mobile users"*
OneSignal	https://onesignal.com/	*"OneSignal is the market leader in customer engagement, powering mobile push, web push, email, and in-app messages"*
OpenX	https://www.openx.com/	*"People first, reaching every digitally addressable adult across every device, screen and household on the open web"*
Oracle (Bluekai)	https://www.oracle.com/marketingcloud/products/data-management-platform/	*"the industry's leading cloud-based big data platform that enables marketing organizations to personalize online, offline, and mobile marketing campaigns"*
Outfit 7	https://outfit7.com/advertising/	*"Working with most global mobile exchanges and ad networks is second nature to us"*
Pinterest	https://business.pinterest.com/en/using-ads-manager	*"Pinterest ads are great for getting your products and content in front of more people as they search, browse and discover on Pinterest."*
Placed (Foursquare)	https://www.placed.com/	*"Placed provides clients the most complete understanding of what consumers do in the physical world – and turns that information into actionable insights"*

Placer	http://placer.ai/	*“Unprecedented visibility into consumer foot-traffic”*
Platform 161	https://platform161.com/	*“a leading demand-side platform (DSP), working with advertisers and agencies”*
Playground XYZ	https://playground.xyz/	*“the world’s first real time stack to capture, measure and optimise Attention Time: how long users spend actually looking at your content”*
PubMatic	https://pubmatic.com/	*“PubMatic is a publisher-focused sell-side platform for an open digital media future”*
PubNative	https://pubnative.net/	*“PubNative builds monetization technologies to empower publishers to maximize ad revenue without compromising on user experience”*
Pulsepoint	https://contextweb.com/	*“connects brands with proprietary, qualified audiences on targeted, contextualized media at scale, in real time.”*
QuantCast	https://www.quantcast.com/brand-solutions/	*“We see the paths, interests and behaviors of everyone on the Internet—helping you reach your audience when it counts”*
RhythmOne (Taptica, Tremor Video)	https://www.rhythmone.com/	*“we provide innovative solutions for brands to connect with consumers — helping to drive outcomes for advertisers and publishers across all screens”*
Rocket Fuel	http://www.rocketfuelinc.com/	*“a real-time targeting company that transforms digital media buys into optimization engines, driving campaign results from awareness to sales.”*
Rubicon Project	https://rubiconproject.com/	*“The global exchange for advertising”*
SafeDK (AppLovin)	https://www.safedk.com/	*“One solution for performance, ad visibility, and privacy of 3rd party SDKs in your mobile app”*
Safegraph	https://www.safegraph.com/	*“Unlock innovation with the most accurate Points-of-Interest (POI) data, business listings, & store visitor insights data for commercial places in the U.S.”*
Salesforce (Krux)	https://www.salesforce.com/products/marketing-cloud/data-management/	*“Audience Studio adds robust data management tools to the world’s most complete CRM platform”*
Scoota	https://www.scoota.com/	*“Next-generation dynamic, biddable programmatic DOOH, today”*

Sense360	https://sense360.com/about/	*“Helping world-class companies make consistently great decisions, faster and with conviction”*
Sift	https://sift.com/	*“Digital Trust & Safety powers Dynamic Friction, so you can see every step of the user journey and serve up the right experiences at the right time”*
Simpli.fi	https://simpli.fi/	*“Our clients leverage Simpli.fi's ability to customize audiences to local needs, provide superior performance on high volumes of localized campaigns, and drive higher ROI in their digital business.”*
Smaato	https://www.smaato.com/	*“We empower app developers and mobile publishers to reach their full monetization potential by connecting them with the world’s top advertisers”*
Soomla	https://soomla.com/	*“SOOMLA provides app marketers, monetization managers and product teams with unique in-app advertising insights”*
Sovrn (Lijit)	https://www.sovrn.com/	*“You produce the content the world depends on for information, commerce, and entertainment. We help you turn your passion into income.”*
Splicky	https://www.splicky.com/en/web/home	*“we have managed to simplify the mobile advertising marketplace for the advertiser by offering one platform with access to multiple mobile and DOOH ad exchanges”*
Sportradar	https://www.sportradar.com/ads/	*“Sportradar ad:s is a holistic marketing solution that capitalises on our deep understanding of bookmakers’ needs, providing one-of-a-kind marketing solutions for sports betting operators”*
StackAdapt	https://www.stackadapt.com/	*“the #1 programmatic native advertising platform helping agencies accelerate customer engagement and acquisition”*
Startapp	https://www.startapp.com/	*“uses first-party data and insights to enhance the mobile experience for mobile publishers, advertisers, and consumers”*
Start Magazine	https://developers.thestartmagazine.com/	*“By targeting users' interests and demographics, we add a quality monetization stream to your app”*
Superawesome Ads	https://www.superawesome.com/	*“SuperAwesome powers the kids digital media ecosystem. Our kidtech is used by hundreds of brands and content-owners to enable safe digital engagement with the global kids audience.”*

Taboola	https://www.taboola.com/	*"Drive marketing results by targeting your audience when they are most receptive to new messages"*
TapAd (Telenor)	http://www.tapad.com/	*"Tapad correlates data to connect brands to consumers globally across devices"*
TapJoy	https://www.tapjoy.com/	*"We make it easy for advertisers to connect with exclusive audiences in the world's most popular mobile games and apps"*
Tap Research	https://www.tapresearch.com/	*"Survey millions of people through the mobile apps they use every day"*
Tencent	https://ads.app.wechat.com/	*"Promote your business and achieve your goals through China's largest and most trusted Internet company"*
The Trade Desk	https://www.thetradedesk.com/	*"We built our media-buying platform to power a more engaging and inspiring ecosystem for everyone"*
TribalFusion	https://www.tribalfusion.com/TribalFusion/index.html	*"the leading site representation company, serving 20 billion monthly impressions and reaching over 230 million users worldwide per month"*
TrustArc	https://www.trustarc.com/	*"TrustArc simplifies privacy management for the GDPR, CCPA and 500+ other global regulations with our comprehensive technology platform"*
Tutela Technologies	https://www.tutela.com/	*"Tutela collects and analyzes anonymous mobile network coverage and experience statistics from millions of mobile devices to deliver actionable insights to telecoms and other mobile companies."*
33across (Tynt)	https://www.33across.com/	*"We build technology that delivers consumer attention"*
Unacast	https://www.unacast.com/	*"We combine location data, map data, and strategic intelligence to provide clients with the best possible picture of real-world human activity"*
Unity3d	https://unity.com/solutions/unity-ads	*"Integrate relevant ads natively into your game experience while maximizing revenue"*
Verizon Media Native (Yahoo)	https://gemini.yahoo.com/advertiser/home	*"Our native solutions empowered you with insightful data, brand-safe premium content, and advanced technologies to deliver engaging advertising campaigns that really drive results"*

Verve (Receptiv, Mediabrix)	https://www.verve.com/	*"Where people go tells you a lot about who they are. The many data signals generated by mobile devices enable observant marketers to understand the people using them — where they go, what they want, and what they will respond to best."*
Vungle	https://vungle.com/	*"It takes a technological mind and a human heart to create mobile ad experiences that really matter"*
WalkMe (Jaco)	https://www.walkme.com/	*"Empower users to keep pace with technology by enabling true digital adoption"*
Widespace (Azerion)	https://www.widespace.com/	*"We believe in activating the data of everything, making it usable to everyone through a mobile programmatic platform all powered by machine learning technology"*
Yandex	https://yandex.com/adv/	*"Advertising in Russia is easy with Yandex.Direct"*
Zemanta	https://www.zemanta.com/	*"We've engineered our technology stack – from our lightning fast interface to our bidding algorithms – for the content marketing era"*
Zeta Global	https://zetaglobal.com/	*"Zeta's proprietary Data and Marketing Clouds, along with the acquired industry-leading technologies, enable marketers to deliver valuable, truly personalized experiences in the moments that matter"*

Table 52. List of 135 identified third parties