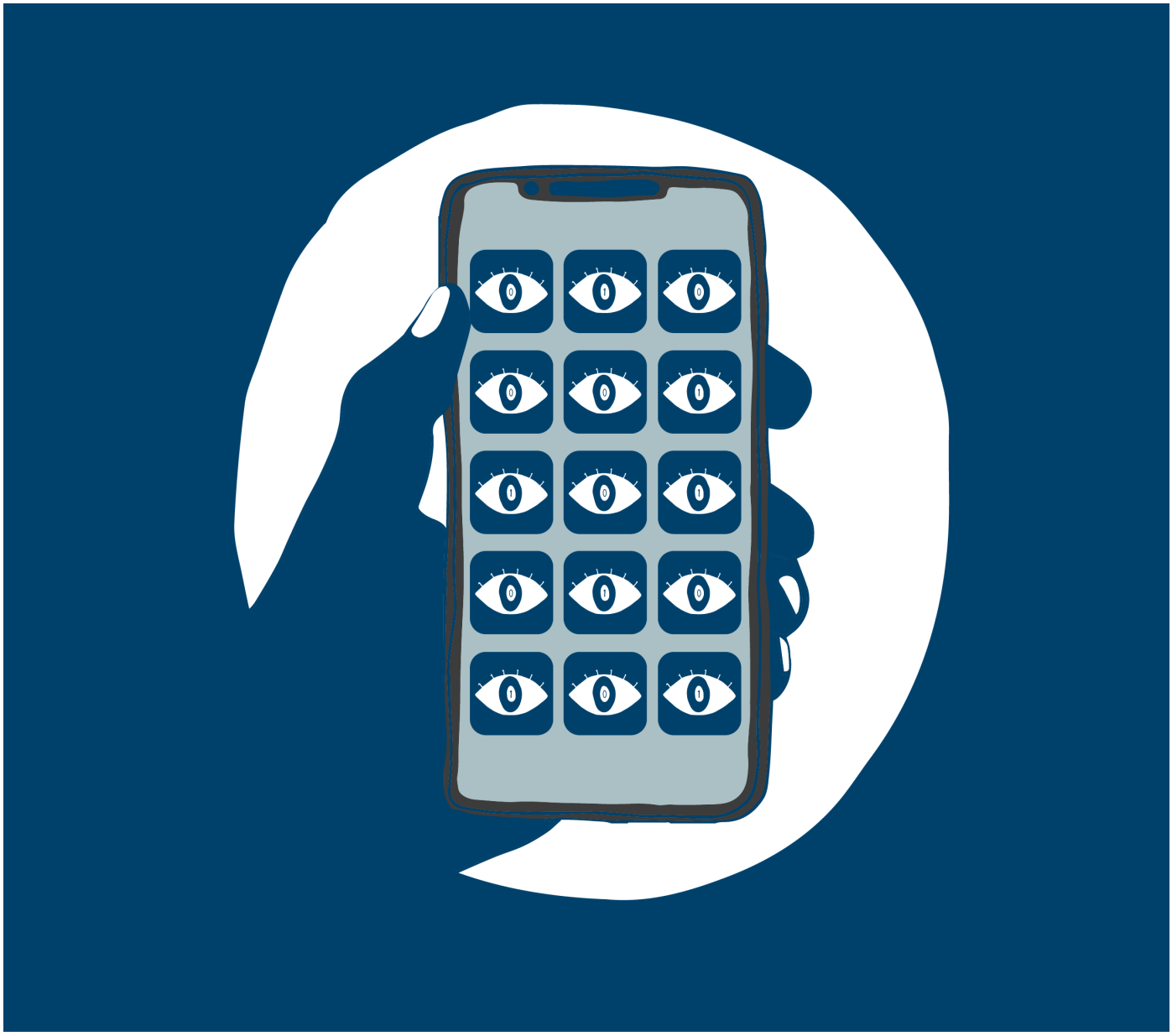


# OUT OF CONTROL

How consumers are exploited by the online advertising industry

14.01.2020

FORBRUKERRÅDET

# Table of contents

# 1 Summary

As we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of showing targeted advertising. In this report, we demonstrate how every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour.

These actors, who are part of what we call the digital marketing and adtech industry, use this information to track us over time and across devices, in order to create comprehensive profiles about individual consumers. In turn, these profiles and groups can be used to personalize and target advertising, but also for other purposes such as discrimination, manipulation, and exploitation.

Although the adtech industry operates across different media such as websites, smart devices, and mobile apps, we chose to focus on adtech in apps. In order to expose how large parts of this vast industry works, we commissioned the cybersecurity company Mnemonic to perform a technical analysis of the data traffic from ten popular mobile apps. Because of the scope of tests, size of the third parties that were observed receiving data, and popularity of the apps, we regard the findings from these tests to be representative of widespread practices in the adtech industry.

The technical tests revealed a number of serious privacy infringements. Some of the key findings are summarized below:

- Altogether, the ten apps were observed **transmitting user data to at least 135 different third parties** involved in advertising and/or behavioural profiling.
- The **Android Advertising ID**, which allows companies to track consumers across different services, was **transferred to at least 70 different third parties** involved in advertising and/or profiling. This identifier was often transmitted in combination with other personal data such as GPS location and IP address. This extensive collection, combination and use of persistent identifiers enables tracking across apps and devices, and the creation of **comprehensive profiles on individual consumers**.
- All of the apps shared user data with multiple third parties, and all except one shared data beyond the device's Advertising ID. This information included the IP address and GPS location of the user, personal attributes including gender and age, and various user activities. Such information can be used to track and target these users with ads, to profile them, and consumers like them, and to infer many



highly sensitive infer attributes including sexual orientation and religious beliefs.

- The dating app **Grindr** shared detailed user data with a large number of third parties that are involved in advertising and profiling. This data included IP address, Advertising ID, GPS location, age, and gender. Twitter's adtech subsidiary **MoPub** was used as a mediator for much of this data sharing, and was observed passing personal data to a number of other advertising third parties including the major adtech companies **AppNexus** and **OpenX**. Many of these third parties reserve the right to **share the data they collect with a very large number of partners**.
- The makeup app **Perfect365** shared user data with **more than 70 third parties**. This data included the Advertising ID, IP address, and GPS location. Many of the third parties that were receiving this data are in the business of **collecting, using and selling location data** for various commercial purposes.
- The period tracker app **MyDays** shared the user's GPS location with numerous third parties involved in behavioural advertising and profiling.
- The dating app **OkCupid** shared **highly personal data about sexuality, drug use, political views, and more** with the analytics company **Braze**.
- Google's advertising service **DoubleClick** was receiving data from eight of the apps, while **Facebook** was receiving data from nine apps.

Our legal analysis of these finding shows that a large amount of this data sharing and processing appears to be **illegal under the General Data Protection Regulation**.

Conclusion

- **20 months after the GDPR has come into effect, consumers are still pervasively tracked and profiled online and have no way of knowing which entities process their data and how to stop them.**
- **The adtech industry is operating with out of control data sharing and processing, despite that should limit most, if not all, of the practices identified throughout this report.**
- **The digital marketing and adtech industry has to make comprehensive changes in order to comply with European regulation, and to ensure that they respect consumers' fundamental rights and freedoms.**



- On the basis of these findings, we urge data protection authorities to enforce the GDPR, and for advertisers and publishers to look toward alternative digital advertising methods that respect fundamental rights.

| App | Summary of findings |
|---|---|
| Clue | Sends birth year to **Amplitude**, **Apptimize**, and **Braze**.<br>Sends Advertising ID to **Adjust**, **Amplitude**, and **Facebook**. |
| Grindr | Sends GPS coordinates to **AdColony**, **AppNexus**, **Braze**, **Bucksense**, **MoPub**, **OpenX**, **Smaato**, **PubNative**, **Vungle**, and others. Sends the IP address to **AppNexus** and **Bucksense**, and information about "relationship type" to **Braze**.<br>Sends Advertising ID to all of these third parties and others, except **Braze.** |
| Happn | Sends country, gender and age segment of the user to **Google**.<br>Sends Advertising ID to **Adjust** and **Facebook**. |
| Muslim: Qibla Finder | Sends IP address to **Appodeal**.<br>Sends Advertising ID to **AppLovin**, **Appodeal**, **Facebook**, and **Liftoff**. |
| My days | Sends GPS coordinates and Wi-Fi access point information to **Neura**, **Placed**, and **Placer**. Sends IP address and a list of installed apps on the phone to **Placed**. Sends Advertising ID to **AppLovin**, **Liftoff**, **Google**, **Ogury Presage**, and **Placed**. |
| My Talking Tom 2 | Sends IP address to **Mobfox**, **PubNative**, and **Rubicon Project**.<br>Sends Advertising ID to **AppsFlyer**, **AppLovin**, **Facebook**, **IQzone**, **ironSource**, **Mobfox**, **Outfit7**, and **Rubicon Project**. |
| OkCupid | Sends GPS coordinates and answers to personal questions to **Braze**. Sends detailed device information to **AppsFlyer**. Sends Advertising ID to **AppsFlyer**, **Facebook** and **Kochava**. |
| Perfect365 | Sends various location data such as GPS coordinates and Wi-Fi access point information to **Fysical**, **Safegraph**, and **Vungle**. Sends GPS coordinates unencrypted to **Receptiv**. Sends Advertising ID to **Amazon**, **Chocolate**, **Facebook**, **Fluxloop**, **Fyber**, **Fysical**, **InMobi**, **Inner-Active**, **Ogury Presage**, **Safegraph**, **Receptiv**, **Unacast**, **Unity3d**, and **Vungle**. |
| Tinder | Sends GPS position and "target gender" to **AppsFlyer** and **LeanPlum**.<br>Sends Advertising ID to **AppsFlyer**, **Branch**, **Facebook**, and **Salesforce** (**Krux**). |
| Wave Keyboard | Sends Advertising ID to **Crashlytics**, **Facebook**, **Flurry**, **OneSignal**. |

The Norwegian Consumer Council is a government funded organisation that represents consumer interests.

This report was written with help from the researchers Wolfie Christl of Cracked Labs and Zach Edwards of Victory Medium, legal expertise from the privacy NGO noyb, and with technical testing performed by Andreas Claesson and Tor E. Bjørstad from the cybersecurity company Mnemonic. The illustrations throughout the report were created by Copyleft Solutions.[1]

[1] Copyleft Solutions https://copyleftsolutions.com/

The project was produced with additional funding from the Norwegian Ministry of Children and Family, and from the research project AlerT, which is led by the Norwegian Computing Center.[2]

## 1.1 Introduction

Throughout this report, we will show how the online marketing and adtech industry operates. As we will argue, these practices are out of control, rife with privacy violations and breaches of European law, and highly problematic from an ethical perspective. We draw on a number of sources, including technical testing, publicly available documentation, and European data protection law, to expose these illegal practices.

We argue that the comprehensive tracking and profiling of consumers that is at the heart of the adtech industry are by their very nature exploitative practices. The system in its current form is based on the comprehensive and systemic illegal collection and use of personal data. Consequently, companies involved in either using or purchasing services from actors that are using illegally obtained data, should be aware that they are likely to fall afoul of European data protection law.

In order to show how personal data about consumers is being collected by digital marketing and adtech companies, we commissioned the security company Mnemonic[3] to analyse the data traffic from ten popular mobile apps. Based on these tests, we mapped the practices of several third party adtech companies that were observed receiving personal data, which is data that can be used to identify individual consumers. The processing of personal data means that data protection law applies to these practices.

Because the industry and technology underpinning digital marketing is extremely complex, this report provides necessary background information about the different technologies and types of companies involved in the processes behind showing online ads. In chapter 2, we provide a description of the adtech industry, including how the technology works and what roles different actors play in the process. This background information was compiled together with the researcher Wolfie Christl of Cracked Labs, an independent NGO based in Austria.[4]

[2] "ALerT - Awareness Learning Tools for Data Sharing Everywhere" https://www.nr.no/en/projects/alert-awareness-learning-tools-data-sharing-everywhere
[3] Mnemonic https://www.mnemonic.no/
[4] Cracked Labs https://crackedlabs.org/

The Norwegian Consumer Council is not the only organisation scrutinizing the adtech industry. The industry is under investigation by a number of other groups and regulatory authorities. Therefore, chapter 2 also contains an overview of ongoing actions from civil society and regulatory authorities against the industry. These ongoing actions show that the practices of many actors in the adtech industry are legally questionable for a variety of reasons.

In addition to being used to display targeted advertising, the profiling and categorization of consumers that many adtech companies engage in contribute to different types of harm, both for individual consumers and for society as a whole. In chapter 3, we outline some different types of harm that may arise as a direct or indirect result of the data exploitation of many actors in the adtech industry.

Some of the harm of this data exploitation stems from significant knowledge and power asymmetries that render consumers powerless. The overarching lack of transparency of the system makes consumers vulnerable to manipulation, particularly when unknown companies know almost everything about the individual consumer. However, even if regular consumers had comprehensive knowledge of the technologies and systems driving the adtech industry, there would still be very limited ways to stop or control the data exploitation.

Since the number and complexity of actors involved in digital marketing is staggering, consumers have no meaningful ways to resist or otherwise protect themselves from the effects of profiling. These effects include different forms of discrimination and exclusion, data being used for new and unknowable purposes, widespread fraud, and the chilling effects of massive commercial surveillance systems. In the long run, these issues are also contributing to the erosion of trust in the digital industry, which may have serious consequences for the digital economy.

Chapter 4 describes the methodology of the testing. This includes what data flows can be expected from a data flow analysis, as well as the limitations of the testing methods.

Because user interfaces on consumer facing services often is the only way that consumers are informed and provided choices about how their data is collected, shared and used, we looked at whether apps themselves provide meaningful information and choice to the end user. Chapter 5 includes descriptions of the processes consumers have to go through when using and/or

registering for each of the apps we tested, documented through screenshots and snippets from the privacy policies provided by the app publishers.

None of the apps provided the information necessary for the consumer to make an informed choice when launching the apps. Furthermore, we found a near complete lack of in-app settings to regulate or prevent the sharing of personal data with third parties. This illustrates that consumers are often not given enough information to choose whether they accept being tracked and profiled. If the consumer does not want their apps to transmit personal data to commercial third parties, the only option is often not to install the apps in the first place.

The data flow analysis performed by Mnemonic revealed a large number of data transmissions to adtech companies and data brokers. In chapter 6, we describe the results from Mnemonic's testing, and supplement these results with public documentation that describes the practices of the adtech companies that were observed receiving personal data.

For example, several companies operating as location data brokers, meaning they compile and sell geolocation information about consumers, were observed continuously receiving precise GPS coordinates from a number of apps. Furthermore, some companies that are engaged in behavioural profiling were observed receiving a large number of different data points about the user and the device, implying that this data is used to create profiles that can be used to target messages based on predicted behaviour.

To illustrate the complexities of how the mobile adtech system may work for just a single app, in chapter 7 we present an in-depth look at the advertising technology used by the dating app Grindr. When performing a data flow analysis of Grindr, Mnemonic observed a particularly interesting app architecture setting up a number of transmissions including potentially sensitive personal data. This led us to commission an additional audit of the app from the researcher Zach Edwards of Victory Medium, a technology company based in the United States that specialize in auditing local data flows.[5]

This audit showed how the Twitter-owned adtech company MoPub is acting as an advertising mediator in Grindr, facilitating transmissions containing personal data from Grindr to other adtech companies. These MoPub-mediated transmissions included the combination of the unique identifiers such as the Android Advertising ID and the IP address, which allows third party companies

[5] Victory Medium https://victorymedium.com/

to track consumers across devices. Simultaneously, several other companies were observed receiving personal data through software integrations in the app.

In Europe, the collection and processing of personal data is regulated by the General Data Protection Regulation. This is a legal regime that is meant to protect personal data and limit how and under what circumstances personal data can be collected and used. The extent of tracking and complexity of the adtech industry is incomprehensible to consumers, meaning that individuals cannot make informed choices about how their personal data is collected, shared and used. Consequently, the massive commercial surveillance going on throughout the adtech industry is systematically at odds with our fundamental rights and freedoms.

As we describe in chapter 8, most of the adtech companies that Mnemonic observed receiving personal data have a questionable legal basis for harvesting and using consumer data. If these companies do not have a legally valid basis for processing personal data, the backbone of much of the adtech system may be systemically in breach of the GDPR. This legal analysis was conducted with assistance from the European privacy NGO noyb.[6]

Since systemic commercial surveillance is omnipresent throughout much of the adtech industry, we believe that significant measures are needed to curb any illegal processing activities. In chapter 9, we provide some general recommendations about what industry actors and national authorities should do to reduce the extent of privacy violations and other harmful effects of the currently dominating adtech system.

In order to shift the significant power imbalance between consumers and third party companies, the current practices of extensive tracking and profiling have to end. Companies that are either directly involved in, or perusing the services of companies that are illegally using personal data, must change their practices to respect consumers' rights, and consequently operate within the confines of European law. For companies that do not cease any illegal practice, national regulators and enforcement authorities must take active enforcement measures, to establish legal precedent to protect consumers against the illegal exploitation of personal data.

[6] Noyb – European Center for Digital Rights https://noyb.eu/

# 2 Background: The digital marketing and adtech industry

As connectivity has become ubiquitous in our daily lives, the internet has also given rise to an industry of companies that operate by collecting as much information as possible about us. Everything from our preferences, movement, habits, physical attributes, and a vast amount of seemingly inconsequential information about our devices is being logged when we browse the internet, use our phones, make transactions, and move around the physical world. This information can be used to deliver individually tailored or more useful services, but could also have potentially harmful consequences for our privacy, our autonomy, and for society at large.

## 2.1 Profiling and targeted advertising

Digital content is to a large degree funded by advertising, which means that rather than paying for services with money, companies monetize our behaviour, attention and personal data. In order to maximize the potential revenue for advertisers, online advertising is becoming increasingly individualized and tailored to specific groups or individuals. Most of us carry our smartphones around at all times, which has opened up new possibilities for marketers to grab our attention and influence how we act at any moment. In order to create and serve accurate and relevant advertising and create personalized digital environments, this individualization depends on knowing as much about each one of us as possible.

One main underpinning of this surveillance economy is that we are secretly assigned several types of unique identifiers, or serial numbers, to which a vast amount of different information is attached. These personal identifiers are also used to track consumers across services and devices, which all feed data into the profiles that are compiled about every individual.

Through these identifiers, each of us is being categorized, bought and sold on a massive marketplace operating largely outside of the consumer sphere, in an industry collectively known as the digital marketing and adtech industry.[7] Our personalities, predispositions and secret desires are continuously monitored and collected by a vast amount of more or less obscure companies, all for the purpose of persuading us to buy particular products or act in a certain way.

[7] Throughout this report, the terms “adtech”, “adtech industry”, “online advertising industry”, and “digital marketing and adtech” are used interchangeably to refer to the broader groups of companies fulfilling different roles in this industry.

By combining big data analysis with behavioural psychology, some actors in this system profess to be capable of predicting what consumers want before the want arises. This leveraging of behavioural psychology in combination with predictive algorithms has given rise to what can be broadly defined as data-driven persuasion.[8]

Companies engaging in behavioural advertising operate on the premise that, by targeting consumers with precisely the right message at the right moment, the chances of conversion and the profit revenue from those interactions increase.[9] This supposedly reduces unnecessary ad spending by removing irrelevant messaging to consumers, which is perceived as a flaw in the more "traditional" marketing methods, where ad space is purchased statically (such as a TV commercial or magazine ad).[10]

For example, at a basic level, a business in Oslo may want to target advertising to potential customers in the Oslo area, rather than in a national newspaper. If the business sells niche products, it can target consumers who are interested in its particular products. If the data is fine-grained enough, it could potentially target a consumer who has a history of browsing for similar products, and that commutes right by the storefront at certain points of the day. Thus the rise of the always-connected consumer has given advertisers a vastly expanded toolbox with which to shape the ways we think and act.

In addition to household names such as Google, Facebook, Twitter, and Amazon, the adtech industry consists of a large number of third party data and marketing companies that most of us have never heard of. This hidden industry is explained in detail below.

## 2.2 Actors in adtech and digital marketing

The key actors involved in today's digital marketing and adtech data economy are numerous, and serve many different roles and purposes. Adtech companies can be separated into four main categories, although the categories sometimes

[8] "How companies use personal data against people", page 29, Wolfie Christl https://crackedlabs.org/en/data-against-people

[9] "Micro-Moments Now: 3 new consumer behaviors playing out in Google search data", Google [accessed December 11, 2019] https://www.thinkwithgoogle.com/consumer-insights/micro-moments-consumer-behavior-expectations/

[10] There has been raised serious doubts about the cost-effectiveness of behavioural advertising compared to alternative models. See for example "Behavioral Advertising: The mirage built by Google", Jason Kint https://digitalcontentnext.org/blog/2019/06/06/behavioral-advertising-the-mirage-built-by-google/

intersect. These categories are publishers, marketers, third party vendors, and major platforms.[11]

Publishers provide information and interactive services to users. This includes all kinds of websites and mobile apps (e.g. online news, weather sites, dating apps), games, video and music streaming services, and many other kinds of digital services and software. As they operate in digital environments, they sell their capability to influence users, typically by offering ad space for sale, or they directly sell data on the users of their services. Throughout this report, the relevant publishers are providers of mobile apps.

Marketers are entities that want to acquire and retain valuable customers, and thus find and influence users across the digital world. This includes, retailers, grocery stores, consumer goods brands, device makers, car vendors, the travel and hospitality industry, telecom and financial services providers, and many other providers of products and services.

However, the distinction between publishers and marketers is not by itself sufficient to describe the wide diversity of existing business models in today's digital marketing industry. Blurring the boundaries, publishers often take on the role of marketers when they want to acquire and retain their own users. For example, many providers of mobile apps engage in digital marketing to influence potential users to install those apps.

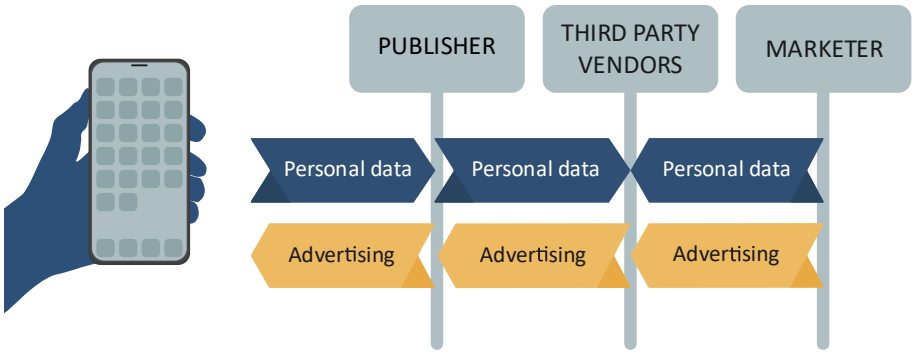
Besides publishers and marketers, who have direct relationships with their users and existing customers, a number of other actors in the digital marketing and adtech industry is normally hidden from consumers.

Unlike publishers and marketers, third party vendors mostly do not have any direct relationships with users. This group of actors includes thousands of interconnected entities, including advertising networks, analytics vendors, and data brokers.[12] Some of these third party vendors provide services directly to publishers and marketers, while others provide services to other third parties. These third party vendors often process extensive personal data about

[11] Much of the information in this chapter was provided with assistance from Wolfie Christl of Cracked Labs. Additional details can be found in his reports, including "Corporate Surveillance In Everyday Life", Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[12] "Marketing Technology Landscape Supergraphic (2019): Martech 5000 (actually 7,040)", Scott Brinker https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/

consumers, largely without the consumers' knowledge.[13] Publishers and marketers often do not have much control over how third party vendors use this data beyond offering their basic services.[14]




*1 How personal data flows through the adtech industry.*

In addition to publishers, marketers, and third party vendors, a large part of the adtech industry consists of **major platforms**. These major platforms, such as Google and Facebook, often take on multiple roles in the industry. For example, through Google's search engine and its video platform YouTube, Google acts as a publisher, selling digital advertising based on user data. Similarly, the major platforms Facebook and Twitter act as publishers when they sell "sponsored" posts and other kinds of advertising on their platforms.

At the same time, all of the major platforms also act as third party vendors, providing digital advertising services off their platforms through their subsidiaries. For example, Twitter runs MoPub, a mobile app advertising platform.[15] As will be described in chapter 7, Twitter's MoPub facilitate a large number of advertising transactions throughout the mobile app environment.

Facebook also runs a mobile app advertising platform[16] and an 'audience network'.[17] Similarly, Google dominates the digital advertising world not only as a publisher, but also as a third party vendor and intermediator, [18] through

[13] "Corporate Surveillance In Everyday Life", Wolfie Christl
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[14] "Behavioural advertising and personal data", Johnny Ryan
https://brave.com/Behavioural-advertising-and-personal-data.pdf
[15] MoPub https://www.mopub.com/
[16] "Facebook App Ads", Facebook for developers
https://developers.facebook.com/docs/app-ads/
[17] "Facebook Audience Network", Facebook for developers
https://developers.facebook.com/products/audience-network/
[18] "An EU Competition law Analysis of Online Display Advertising in the Programmatic Age", Damien Geradin and Dimitrios Katsifis
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299931

services such as Google AdMob and other services for publishers and marketers.[19] The roles of Google and Facebook in the adtech industry cannot be overstated, as they control large parts of the supply chains. This is elaborated upon in chapter 6.4.

## 2.3 Alternative business models for digital marketing

Although personalised advertising based on tracking and profiling is the dominating business model online, it is not the only way to monetize content on the internet. In addition to alternative models such as subscription services, there are alternative technical solutions to show digital advertising without relying on processing and sharing personal data.

For example, **contextual advertising** relies on targeting ads based on the content that the consumer is looking at, rather than on the profile of the consumer herself.[20] Therefore, contextual advertising ideally does not rely on the processing of personal data.[21] However, through the use of technologies such as machine learning, contextual advertising can also be used for sophisticated targeting purposes.[22]

As a concrete example, after the GDPR came into entry in Europe, the New York Times decided to stop using targeted advertising to European users. Instead, the news provider began targeting based on context and general geographic parameters. Despite not relying on tracking and profiling to tailor ads, the publisher's ad revenue kept increasing.[23]

[19] "Introducing simpler brands and solutions for advertisers and publishers", Google [accessed December 11, 2019] https://www.blog.google/technology/ads/new-advertising-brands/

[20] "Study of Effects of Contextual Targeting", Kobler https://kobler.no/contextual-insights/

[21] Although contextual advertising generally does not target ads based on personal data, it can also rely on the processing of personal data, depending on its implementation. For example for frequency capping, attribution, verification, etc.

[22] See for example "Better bandit building: Advanced personalization the easy way with AutoML Tables", Google Cloud https://cloud.google.com/blog/products/ai-machine-learning/how-to-build-better-contextual-bandits-machine-learning-models

[23] "After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue", Jessica Davies https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/

There are also technical solutions that allow for showing targeted advertising by processing all personal data on the consumers' device, which means that third parties do not touch the data.[24]

Although such alternative models for advertising do not necessarily alleviate all the potentially problematic aspects of advertising, they demonstrate that behavioural tracking and profiling is not necessary to monetize online content.

## 2.4 Tracking and personal data processing by third party vendors

Every time a consumer visits a website or uses a mobile app, data about the consumer is not only transmitted to the publisher, but also to several third party vendors. This process is usually referred to as **tracking**. A large-scale study on the top 1 million websites found that websites send data to at least 34 third parties on average.[25] Another large-scale study on nearly 1 million mobile apps found that apps send data to 10 third parties on average.[26]

A wide range of third party vendors are involved in the provision of digital marketing. One intended effect of this industry is to single out and influence individual consumers into acting in certain ways (e.g. purchase a product). The combination of a large amount of re-identifiable data and the intent to single out individuals means that most data companies in adtech and digital marketing are clearly processing personal data on consumers.[27]

Tracking occurs because publishers embed third party software into their websites and apps, which may include what is known as web bugs, beacons or tags, or as part of libraries or **software development kits** (SDKs).[28]

[24] "The First Global Ad Platform Built On Privacy" https://brave.com/brave-ads-waitlist/

[25] "Online Tracking: A 1-million-site Measurement and Analysis", Steven Englehardt and Arvind Narayanan http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[26] "Third Party Tracking in the Mobile Ecosystem", Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt https://dl.acm.org/citation.cfm?doid=3201064.3201089

[27] "Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation", Frederik Zuiderveen Borgesius https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733115

[28] "Corporate Surveillance In Everyday Life" page 44, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

An SDK is a library of third party tools and code that publishers (app developers) can use to add functionality from other developers and service providers. When installing an app, any SDKs that are integrated in the app receive access to the mobile device. Such SDKs can be used for providing different integrations and tools, for both functional, analytics, and tracking and advertising purposes. The SDK often facilitates data transmissions directly to the third party vendor who provided the SDK. This can be used for tracking or to otherwise covertly harvest data.[29] Without significant technical expertise, consumers cannot know whether such third party SDK integrations are present in an app.

In many cases, these third parties transmit user data to further vendors that were not directly the ones embedded by publishers. These further recipients are usually referred to as fourth parties.[30]

Some of these third party tracking services provide user functionality or are actually visible to users, for example as Facebook "Like-buttons" or embedded YouTube videos. However, consumers may not actually be aware that these technologies are used for tracking purposes. Similarly, some analytics-related trackers provides functionality to publishers while being invisible to consumers. These trackers usually give publishers insights about how their services are used, how users engage with these services, or otherwise provide functionality to help with fixing errors.

A third category of companies providing tracking services is predominantly involved in showing advertising. These third party vendors, who we will collectively refer to as **adtech companies**, provide the systems that allow ads to be shown on the website or in the app that the consumer is visiting. This involves providing the technological framework for showing ads, and the gathering and processing of data used to make sure the right ad is shown to the right consumer, at the right time. The systems behind these ads make it possible to target ads at specific segments or individuals, through what is commonly referred to as **behavioural** or **programmatic advertising**.

Some third party vendors provide tracking services that function purely as a way to collect, compile, and sell data about the user. These companies, which are usually called **data brokers**, collect data from a large variety of sources for their own commercial purposes. Data brokers often monetize consumer profiles and segments through sharing or otherwise making these available to further third

[29] "The Loophole That Turns Your Apps Into Spies", Charlie Warzel
https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html
[30] "Managing Fourth Party Tags", TRUSTe Technology Blog
https://www.trustarc.com/developer/?p=335

or fourth parties. Many of these third and fourth party services process extensive personal data about users, as will be detailed below.

In many cases, the boundaries between these categories of third party vendors are blurry, meaning that an analytics company may also be selling consumer profiles, or an advertising company could also provide analytics. Unless described in the privacy policy of the app or website, it is difficult to distinguish what kind of service an individual third party is providing in any particular case.

### 2.4.1 Data brokers

The term data broker describes companies that aggregate, combine and trade massive amounts of data about consumers from a wide variety of sources, largely without consumers' knowledge. They collect publicly available information, buy or license data from other companies, or collect it in partnership with other vendors. Traditionally, this includes companies in the field of direct marketing, as well as in risk assessment, including credit reporting, identity verification, and fraud prevention. In this report, we will focus on the use of consumer data for marketing purposes.[31]

We define a data broker as a company that processes personal data on consumers, which primarily is not obtained from the consumers themselves but from other companies, in order to sell or license this data – or information derived from it – to further companies.[32] This is not an extensive definition, but accurately describes many of the companies detailed in this report.[33]

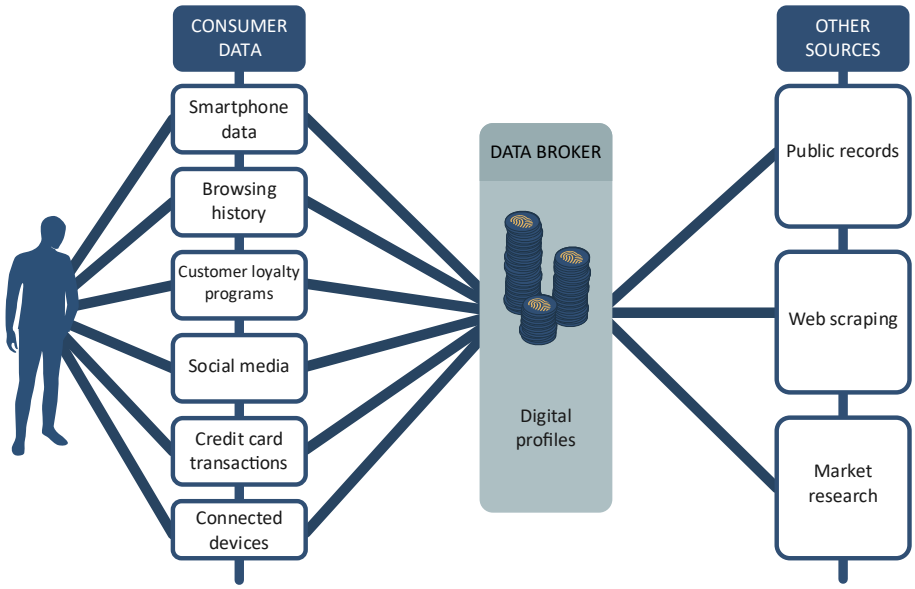
Large consumer data brokers such as Acxiom have been compiling extensive databases on whole populations based on personal identifiers such as names

[31] "Networks of Control", page 76, Wolfie Christl and Sarah Spiekermann https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf

[32] See e.g. the definition in the recently introduced data broker legislation in the U.S. state of Vermont, "Analysis: Vermont's data broker regulation", International Association of Privacy Professionals https://iapp.org/news/a/analysis-vermonts-data-broker-regulation/, and the definition in "Data brokers in an open society", Upturn https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf

[33] In some cases, data brokers do not directly supply data to other companies, but let these companies utilize data obtained from further companies within the data brokers' systems. For example, traditional direct marketing firms do not only sell or license address lists to other companies, but also provide direct mail services that allow their clients to select the recipients based on the direct marketing firms' consumer database, and then send it to those recipients – without actually sharing data with their clients. See for example "Datenverarbeitung für die Adressvermietung im Lettershop-Verfahren", Deutsche Post Direkt https://www.deutschepost.de/content/dam/dpag/images/D_d/DDP/Downloads/datenschutz/dp-dp-direkt-informationen-zur-dv-fuer-av-und-adressabgleich-201805.pdf

and postal addresses for a long time.[34] Similarly, many companies in the adtech and digital marketing industry are aggregating real-time data obtained through trackers on the web and embedded in mobile apps, in order to compile extensive and detailed profiles on consumers.




*2 Data brokers combine data from many different sources.*

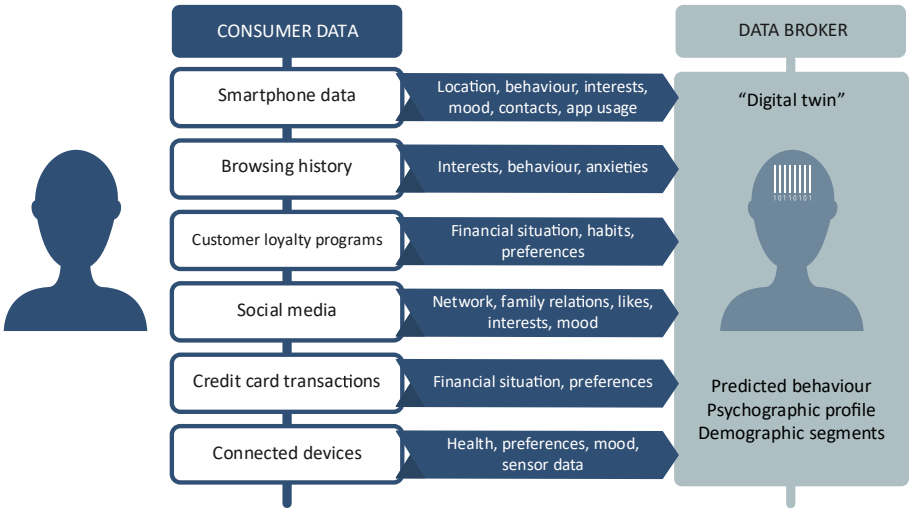
In other words, data brokers collect their data from both the offline and online world, which they compile and combine. When combined, this data is used to create very detailed profiles about individual consumers, which are then sold or otherwise traded to other companies, who may be using the information for different purposes. Such profiles may contain data about behaviour and habits, movement data, metadata about app use and website visits, and much more. In other words, these companies create detailed mirror-images or digital twins of individual consumers, which is used in ways that consumers cannot control.

While some companies openly admit to trade with massive amounts of personal data on billions of consumers, others are more secretive, not disclosing much information about their practices, or trading data in very complex and opaque ways.[35]

[34] "Corporate Surveillance in Everyday Life", page 54, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[35] One can also distinguish between data brokers in a narrow sense, which includes companies that openly sell personal data to interested parties, and data brokers in a wider sense, including companies who provide or re-sell audience segments for targeting across services.

The data making up consumer profiles can include data from our smartphones (such as app usage, Advertising IDs and other user identifiers, contacts, etc.), our web browsing, customer loyalty programs, social media profiles, credit card transactions, connected devices, and public records. Some specialized data brokers only process very narrow categories of personal data, while others process and combine many different categories of personal data.




*3 Different data sources are combined to create "digital twins".*

Usage data is an important part of creating lists or categories of consumers or **audience segments**, which are used to target groups of people based on common characteristics.[36] These lists are also used to score and rank consumers according to their perceived value for advertisers, similarly to the practices used in credit monitoring.[37] For example, as described in chapter 7, our team observed keywords such as "gay" and "bi" being transmitted during the technical tests, which is indicative of potential audience segments.

Audience segments can be created based on parameters such as geographic location, demographics (age, gender, children, occupation, etc.), psychographics (interests, opinions, financial status, lifestyle, etc.), behaviour (browsing habits, user status, etc.), and technology (browser fingerprinting,

[36] "Networks of Control", page 85, Wolfie Christl
https://crackedlabs.org/en/networksofcontrol

[37] For more about the listing and scoring of consumers, see "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too", Kashmir Hill
https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html

phone status, etc.).[38] Some data brokers maintain lists of tens of thousands of audience segments.[39] For example, the data broker Adobe, who also publishes the software Adobe Photoshop, lists thousands of health-related audience segments for sale on its website.[40]

The commercial benefits of combining customer data and data gathered through other sources may explain why many publishers, technology, and telecoms companies such as AT&T have been moving into the digital advertising and data industry. Companies such as Adobe, Comcast, Telenor, Verizon, AliBaba, Facebook, Google, and Amazon have all spent significant resources acquiring adtech companies in recent years.[41]

A company that is already in possession of large amount of customer data may be looking to monetize or otherwise operationalize the data they have. One way of doing so is by entering the data marketplace or adtech industry through an acquisition. Customer databases normally include information such as names, email addresses and/or home addresses, that can be linked to very granular data collected through a data broker or other adtech subsidiary in order to generate new insights and marketing opportunities. As an example of this, in 2016 Google merged identifiable data from its consumer-facing services with data processed by its adtech subsidiary DoubleClick.[42]

### 2.4.2 Third party data providers

Third party data that is resold through so-called data management platforms and other adtech vendors originates mainly from publishers, marketers and data aggregators. This data is often distributed across vendors in the form of

[38] "What is Audience Segmentation? How Can it Help Publishers?", Rashmita Behera https://www.adpushup.com/blog/audience-segmentation/
[39] "Corporate Surveillance in Everyday Life", page 59, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[40] "Available Third Party Health Segments 2019", Adobe Advertising Cloud [accessed November 29, 2019] https://www.adobe.com/content/dam/acom/en/privacy/pdfs/Adobe-Advertising-Cloud-Health-Segments-2019.pdf
[41] For an overview of acquisitions of adtech companies, see "Dissolving Privacy, One Merger at a Time: Competition, Data and Third Party Tracking", Reuben Binns and Elettra Bietti https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269473
[42] This data merger stirred up controversy, particularly because Google had previously pledged to not merge this data when they acquired DoubleClick in 2007. "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking", Julia Angwin https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking

audience segments or audience lists, which consist of lists of personal identifiers referring to individuals with certain characteristics.[43]

There is a large number of different companies that serve as data suppliers to different data brokers.[44] These data providers can be other data brokers, but also analytics companies, credit card companies, and many other service providers and publishers.[45]

For example, mobile data providers collect data on billions of consumers, either directly or indirectly, from app publishers or through third party software that is embedded by app publishers as part of SDKs.[46] Finally, in some cases, it is not clear where data brokers who sell third party data obtain their data.[47]

### 2.4.3 Measurement, attribution, and ad verification

In the early days of online advertising, marketers paid publishers per ad impression. Today, payment is often based on how users act after being exposed to a digital ad. For example, publishers are paid if the user clicks on an

[43] "Corporate Surveillance in Everyday Life", page 72, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[44] For example, the large adtech company LiveRamp currently lists 120 data providers in its partner directory, including Alliant, Claritas, comScore, CoreLogic, Experian, Infogroup, IRi, Kantar, LiveNation, MasterCard, Nielsen, Samba TV, ShareThis, V12, Visa, Ziff Davis, 33across, Epsilon (Publicis), IHS Markit, Equifax, Neustar, The Weather Company (IBM), TiVo Research, TransUnion, Yelp, Dish Network, and Weborama. Its mobile data providers include Cuebiq, Factual, GroundTruth, NinthDecimal, PlaceIQ, Pushspring, Zeotap, Gravy Analytics, Reveal Mobile, Startapp, Twine, and Dataxpand. "Partner Integrations", LiveRamp [accessed November 4, 2019] https://liveramp.com/partners/

[45] In the case of data providers such as MasterCard, Visa, Weather Company, Yelp or the publisher Ziff Davis it is quite clear where the provided data comes from, because they have direct relationships with users. As LiveRamp's list of data providers shows, large data brokers such as Experian, Infogroup, Epsilon, Equifax or TransUnion also provide information to other data brokers.

[46] The U.S. company Kochava, for example, claims to collect and sell data on 1,3 billion users across 6 billion devices through software embedded in 10000 different apps. "Harness Your Data for Growth", Kochava [accessed December 11, 2019] https://www.kochava.com/data-marketplace/

[47] The Swiss mobile data company 42matters, for example, claims to provide 180 million "profiles" from devices and apps, but does not disclose how they obtain data on mobile users. Similarly, the German "mobile data exchange" AdSquare, claims to provide 450 million user profiles from 120+ data providers, but it is not clear where they actually obtain data from.
"Audience Data", 42matters [accessed December 11, 2019] https://42matters.com/audience-data
Adsquare [accessed December 11, 2019] https://www.adsquare.com/

ad or even performs subsequent actions such as registering for a service, installing a mobile app, or purchasing a product.[48]

Therefore, measuring user behaviour after ad exposure – or **attribution** of certain subsequent behaviours to ad impressions – is key to today's digital advertising. As attribution vendors need to observe many different kinds of user behaviours, from web and app usage to purchases, they potentially process extensive personal data on users.[49]

Vendors in the area of **measurement** help publishers and marketers to track what audiences they are actually reaching. They serve as independent third parties that verify what other actors in the supply chain claim to provide. Even the major platforms have partnerships with a small selection of measurement vendors and allow them to track and verify parts of their services.[50]

Other third party vendors help advertisers verify whether users are really exposed to ads ("viewability"), whether ads are displayed only next to quality content rather than unethical or illegal content ("brand safety"), and whether ad impressions and clicks are not fraudulent ("ad fraud").[51]

Vendors that provide services in fields such as measurement, viewability, brand safety and ad fraud prevention, also potentially process extensive personal data on consumers.

For example, the effectiveness or attribution of an ad can be measured by tracking whether a consumer physically visited a store after seeing an online ad, something Google has referred to as "closing the loop".[52] Measuring ad

---

[48] For example, see "Incentive Problems in Performance-Based Online Advertising Pricing: Cost per Click vs. Cost per Action", Yu (Jeffrey) Hu, Jiwoong Shin, and Zhulei Tang https://pubsonline.informs.org/doi/10.1287/mnsc.2015.2223

[49] For example, see "Digital Attribution Primer", Interactive Advertising Bureau [accessed December 11, 2019] https://www.iab.com/wp-content/uploads/2016/10/Digital-Attribution-Primer-2-0-FINAL.pdf

[50] "A solution for every need", Google Measurement Partners [accessed December 11, 2019] https://measurementpartners.google.com/find-a-partner/
"Grow your business with our measurement partners", Facebook Business [accessed December 11, 2019] https://www.facebook.com/business/m/measurement/partners

[51] "Advertising Quality Measurement Buyer's Guide", Interactive Advertising Bureau [accessed December 11, 2019] https://www.iab.com/wp-content/uploads/2018/09/Ad-Quality-Checklist_8-30-18.pdf

[52] "New digital innovations to close the loop for advertisers", Brad Bender [accessed December 11, 2019] https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers

effectiveness in this way is only possible based on large-scale monitoring of the whole population, because it relies on massive sets of location and movement data.

## 2.5 Unique identifiers

Although some pieces of data may seem innocuous when considered in isolation, the combination of different data can create elaborate pictures of individual consumers. In order to append different types of data to the same user profile, it is common for adtech companies to use unique identifiers, that are matched and combined to facilitate tracking across services and devices.

### 2.5.1 Matching identifiers through ID syncing

Adtech companies often claim to process «anonymized» or «de-identified» data, which they claim cannot identify individuals. However, this often amounts to using pseudonymous identifiers, which are unique numbers assigned to a device or an individual. There are many different types of pseudonymous identifiers used to track consumers, and the identifiers typically vary in persistence and availability.[53]

Despite industry claims to the contrary, many of these pseudonymous identifiers can be linked, synchronized or matched across companies in order to tie them to individual consumers. Data transmissions that contain unique identifiers relating to an individual are considered personal data as defined in the GDPR. Furthermore, a 2016 ruling in the Court of Justice of the European Union stated that dynamic IP addresses can also constitute personal data.[54] This means that unique identifiers are personal data as defined by the GDPR.

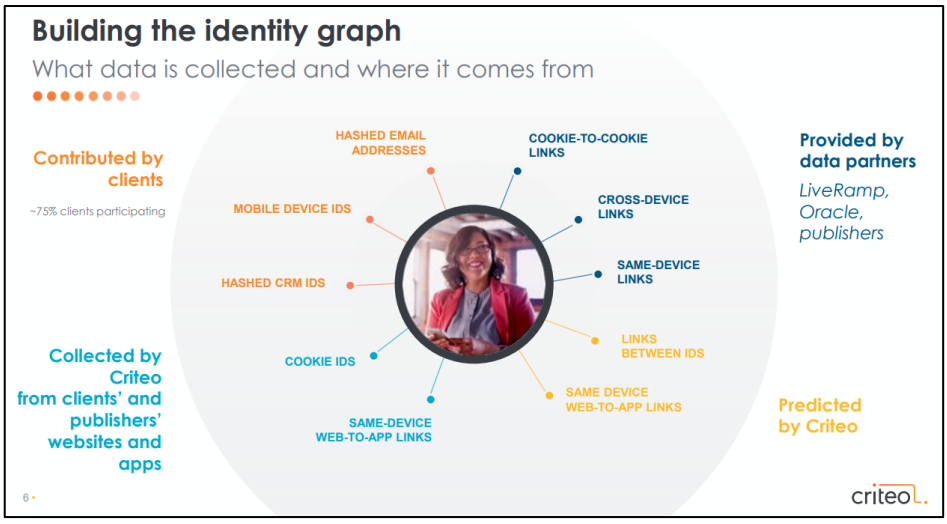
Identifiers such as cookie identifiers, mobile device identifiers, and identifiers derived from email addresses are the most relevant identifiers for cross-service and cross-device tracking.[55] Several adtech companies maintain their own user

[53] For example, adtech companies such as LiveRamp and Oracle maintain comprehensive databases that link identifiers derived from email addresses, mobile device IDs and many other types of pseudonymous identifiers referring to a person to each other. See "Corporate Surveillance in Everyday Life", page 54, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[54] "Your dynamic IP address is now protected personal data under EU law", Glyn Moody https://arstechnica.com/tech-policy/2016/10/eu-dynamic-static-ip-personal-data/

[55] "Networks of Control", page 90, Wolfie Christl https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf

identifiers and have built "identity graphs" in order to link their own identifiers to identifiers used by other vendors.[56]




*4 Source: "Identity Resolution & Criteo Shopper Graph", Criteo https://criteo.investorroom.com/download/July+2019_Criteo-Shopper-Graph.pdf [accessed November 29, 2019]*

If adtech companies were to rely only on more ephemeral identifiers such as temporary identifiers, they would constantly have to rebuild profiles on consumers. This has created an incentive to find and use persistent unique identifiers such as device identifiers, some IP addresses, and the Android Advertising ID.[57]

When the unique identifier is persistent, profiles on consumers can be continually enriched and expanded, rather than having to be constantly rebuilt. However, although persistent identifiers are easier to track over time, the existence of many different such identifiers could potentially complicate things as consumers move between different vendors, services and devices, that may all be using their own identifiers.

[56] For example, the French third party vendor Criteo claims to maintain unique identifiers for 2 billion users. The "Criteo ID" is linked to device IDs and identifiers derived from email addresses, which are collected from its marketing clients, as well as to cookie IDs that are collected from both marketing clients and from publishers' websites and apps. In addition, identity matching data provided by adtech companies such as LiveRamp and Oracle is used.

[57] For an overview of different types of mobile identifiers, see "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance", Bennett Cyphers and Gennie Gebhart https://www.eff.org/wp/behind-the-one-way-mirror#Identifiersonmobile

To get around the issue of multiple identifiers, adtech companies use methods such as **cookie syncing** or **ID syncing** to match different identifiers and tie them to specific individuals. This allows companies to recognize and track users over time across services and devices, and continuously append data from different sources to the same individual consumer.[58]

In its guide for marketers, the Interactive Advertising Bureau describes the need for cross-service and cross-device tracking in order to better understand consumers.

> *In order to deliver truly personalized and relevant messaging, marketers should not only work with cross-device identity vendors, but also with attribution providers and internal data teams to help them not just connect and match devices with unique, people based IDs, but also to gain an understanding of the consumer behind the device.* [59]

Website tracking is often reliant on cookie technologies, and cookies will vary between different websites. Cookie syncing allows third party companies to link and combine cookies from different websites to persistently track consumers. [60]

In the mobile environment, adtech companies rely on a variety of unique identifiers such as Advertising IDs to track consumers. To increase their capability to perform cross-service and cross-device tracking, many adtech companies use ID syncing to combine different identifiers and assign them to the same user.

For example, in its support documents, the data broker Adobe describes how it uses ID syncing to match several identifiers to the same individual.

> *"ID synchronization matches IDs assigned by the ID service to IDs assigned to site visitors by our customers. For example, say the ID service has assigned a visitor ID 1234. Another platform knows this visitor by ID 4321. The ID service maps these IDs together during the synchronization process. The results add new data points to what our customers know*

---

[58] "Networks of Control", page 90, Wolfie Christl https://crackedlabs.org/en/networksofcontrol

[59] "Mobile Identity Guide for Marketers", Interactive Advertising Bureau [accessed December 11, 2019] https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf

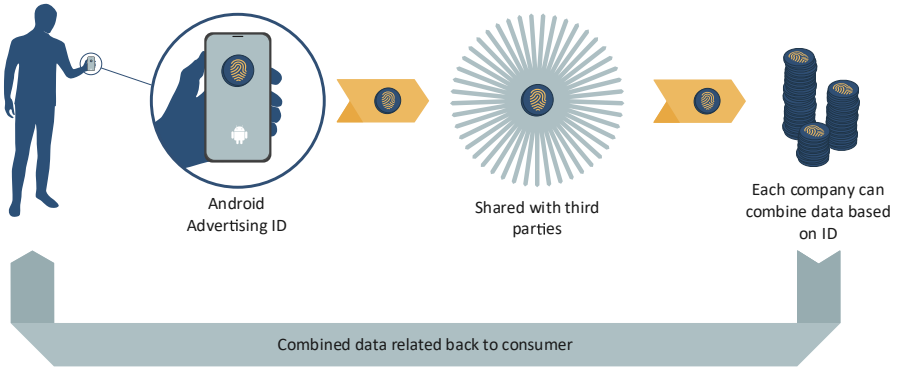
[60] "The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR", Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann https://arxiv.org/pdf/1811.08660.pdf

> *about their site visitors. And, if the ID service can't match an ID, it creates a new one and uses that ID for future synchronization."*[61]

In other words, companies can use technical measures such as ID syncing to track individuals across services and devices, by matching different identifiers gathered from a variety of publishers and other third party vendors. This allows companies to combine user data collected in different contexts, in order to enrich their user graphs/profiles, which allows for more sophisticated targeting across channels and devices.

### 2.5.2 Google Play Android Advertising ID

The Google Play Android Advertising ID is a unique identifier assigned to every Android device. According to Google, this identifier allows "ad networks and other apps anonymously identify a user".[62] This unique identifier is akin to a resettable serial number assigned to a user's device, and consequently referring to the user of the device. The Advertising ID is available to all apps on the device without requiring any special permissions or consent from the user. This is often used by adtech companies to link digital profiles in order to track consumers across services and devices.[63]




*5 The Android Advertising ID is used to combine data from different services.*

[61] Understanding ID synchronization and match rates, Adobe [accessed December 11, 2019] https://docs.adobe.com/content/help/en/id-service/using/intro/match-rates.html

[62] "Advertising ID", Android Developers [accessed December 11, 2019] http://www.androiddocs.com/google/play-services/id.html

[63] Including by consumer data brokers such as Oracle, and major platforms such as Facebook.
"Mobile integrations", Oracle [accessed December 11, 2019] https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/mobile_integration.html
"Targeting by Mobile Advertiser IDs", Facebook for Developers [accessed December 11, 2019] https://developers.facebook.com/docs/app-ads/targeting/mobile-advertiser-ids/

The Advertising ID is usually shared with third party companies through trackers embedded in apps, for example through SDKs, to allow these third parties to track and profile users across apps and services.

During the technical testing, the Android Advertising ID of the test device was observed to be transmitted to at least 70 third parties.[64]

| App | Number of third parties receiving Advertising ID |
|---|---|
| Clue | 4 |
| Grindr | 18 |
| Happn | 2 |
| Muslim: Qibla Finder | 5 |
| My days | 5 |
| My Talking Tom 2 | 8 |
| OkCupid | 3 |
| Perfect365 | 16 |
| Tinder | 5 |
| Wave Keyboard | 4 |

Although the Android Advertising ID can be manually reset by the user through the device settings, this does not necessarily work to limit the tracking capabilities of the identifier. If the Advertising ID is transmitted together with other identifiers, third parties can simply append the new Advertising ID to the other identifier, and resume tracking the user.

Therefore, according to Google's terms of use for advertisers, the Android Advertising ID "must only be used for advertising and user analytics" and "must

[64] Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/

not be connected to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) without explicit consent of the user".[65]

Some third parties also operate their own proprietary identification numbers, which often cannot be reset by the user. These are often used together with Android Advertising IDs and with persistent device identifiers, and may be shared between services. When a third party vendor collects data on a consumer from different sources, this data can be tied to different types of identifiers through ID syncing.

For instance, a consumer using apps on their Android device will be assigned a different identifier than when they use their computer. However, marketers can get around this by combining the identifiers through ID syncing, using data fields shared across devices such as an IP address.

Location data can also be a useful way to facilitate ID syncing, as described by the Interactive Advertising Bureau:

> *"Data gathered from opt-in users through their location enabled apps, is a key source of matching identifiers. Showing an ad to a consumer on either their mobile or desktop device and then identifying the consumer when they visit a store with their mobile device, can inform both attribution and purchase intent (and through integration with credit card data, verify actual purchase). The matched identity can be used for retargeting across devices and for better targeting of ads using the advertiser's first or third party data."*[66]

If a data broker already has access to the IP address and the Advertising ID, and the Advertising ID is reset by the consumer, the data broker can append the new Advertising ID to the IP address, and continue tracking the consumer through apps that did not transmit the persistent identifier.[67] A static IP address connected to a home network can be used this way to identify consumers across devices and services.[68] During the technical testing, Mnemonic found

---

[65] "Usage of Android Advertising ID", Google Developer Policy Center [accessed December 11, 2019] https://play.google.com/about/monetization-ads/ads/#!?zippy_activeEl=ad-id#ad-id

[66] "Mobile Identity guide for Marketers" page 10, Interactive Advertising Bureau [accessed December 11, 2019] https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf

[67] "Ad IDs Behaving Badly", Serge Egelman https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly/

[68] In an October 2019 blogspot, Google points to IP address as a user-level signal that can be used for fingerprinting to circumvent user controls. "A privacy-safe approach to managing ad frequency", Rahul Srinivasan [accessed December 11, 2019]

several companies receiving the IP address together with the Advertising ID, which is described in detail in chapter 7.2.

During the technical testing, Mnemonic also observed 13 third parties receiving other identifiers such as IP addresses and Wi-Fi SSIDs.[69] The implication of this is that many third party vendors can potentially track consumers across devices and over time.[70]

Additionally, many different types of data about device characteristics and user behaviour can be used to identify users.[71] Mnemonic observed that a large number of third parties received data that can potentially be used for device fingerprinting, such as device model, carrier, operating system, screen and memory metadata, time zone, lists of installed apps, and other metadata relating to the user and the device. Fingerprinting can be used to circumvent users' attempts to opt out of or otherwise protect themselves against being tracked.[72]

### 2.5.3 System level opt-out settings

Android users can opt out of some personalized advertising through their device settings by using an Android system-level setting called "Opt out of Ads Personalisation", or some variety thereof, depending on the Android version and phone model. According to Google, this is meant to give consumers more control over their privacy.[73]

Many publishers and third parties use these device-level opt-out options to argue or assume that consumers want to have their personal data shared with third parties. As shown throughout the report, apps and third parties state in

---

https://blog.google/products/marketingplatform/360/privacy-safe-approach-managing-ad-frequency/

[69] Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/

[70] For an overview of identifiers, see the ICO guidelines on personal data. "What are identifiers and related factors?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/

[71] "Fingerprinting mobile devices: A short analysis", Alejandro Gómez-Boix, Pierre Laperdrix, and Benoit Baudry, https://hal.inria.fr/hal-01611101/file/FP_mobile_devices_A_short_analysis%20.pdf

[72] "Think you're anonymous online? A third of popular websites are 'fingerprinting' you.", Geoffrey A. Fowler https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/

[73] Google Play Support – Advertising ID [accessed December 11, 2019] https://support.google.com/googleplay/answer/3405269?hl=en

their privacy policies that if the consumer did not use the opt out device-level settings, they regard this as consent to being tracked.

For example, rather than providing settings to limit tracking in the app itself, Grindr's privacy policy states that users may opt out of or reduce tracking in Grindr by using the system level settings:

> *"If you are using the Grindr Services on an Apple iOS device, you can opt out of behavioral targeting by going into Settings > Privacy > Advertising on your iOS device, or visiting Apple's website for more information. To opt out on an Android device, open the "Google Settings," click on "Ads" and enable "Opt out of interest based ads."*[74]

However, this setting is somewhat obscurely tucked away in the Android settings menu, and consequently many consumers may not be aware of its existence. One 2016 report noted that less than 17 % of consumers had actually used the settings, although 30 % erroneously thought that they had opted out.[75]

Generally, the GDPR contains several data protection principles, one of which is "data protection by default". One condition of this principle entails that privacy settings should be pre-selected to the most privacy-friendly choice.[76] This indicates that in order to comply with the GDPR, settings that allow for the transmission of personal data for tracking or profiling should be based on an active opt-in choice. In other words, assuming that the user has consented to tracking because they did not deactivate the system level settings is not in compliance with the GDPR. This is elaborated upon in the legal analysis in chapter 8.

Furthermore, the setting for opting out of personalised ads functions by instructing "apps not to use your advertising ID to build profiles or show you personalised ads", but does not remove or obfuscate the Advertising ID from the device. In contrast, the equivalent setting on Apple's iOS (on iOS 10 and up)

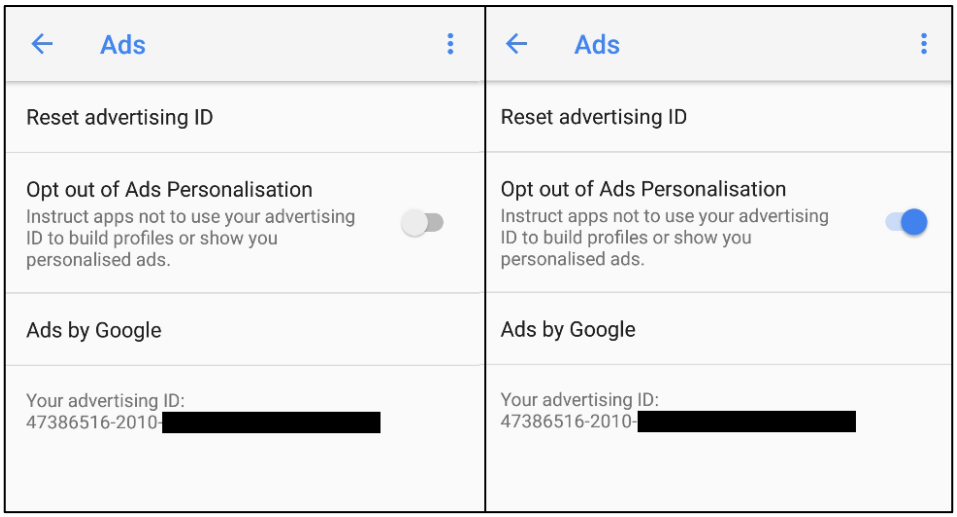
---

[74] Grindr privacy policy (last updated December 3, 2018) https://www.grindr.com/privacy-policy/

[75] "Use of limit ad tracking drops as ad blocking grows", Kate Kaye https://adage.com/article/privacy-and-regulation/limit-ad-tracking-drops-ad-blocking-grows/303911

[76] GDPR Art. 25(2) states that controllers should make sure that "by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

causes Apple's Advertising ID to be "replaced with a non-unique value of all zeros to prevent the serving of targeted ads".[77]




*6 The Android device-level settings to opt out of personalized ads. Before opting out (left) and after (right).*

The key difference between these two implementations is that the iOS setting effectively prevents third parties from receiving or using the Advertising ID because the ID has been made inaccessible. On Android devices, apps can still use the Advertising ID for other purposes involving individual-level personal data, even if the user opts out of personalised advertising.

> *"If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection."*[78]

If the app developer does not implement functionality respecting the users' choice to opt out, they can still access and use the Advertising ID for personalising ads.[79]

[77] "Advertising & Privacy", Apple Support [accessed December 11, 2019] https://support.apple.com/en-us/HT205223

[78] "Monetization and Ads", Google Play Developer Policy Center [accessed December 11, 2019] https://play.google.com/about/monetization-ads/ads/

[79] According to Android developer documentation, developers "must check for and respect the user's ad tracking preference". "Advertising ID", Android Developers [accessed December 11, 2019] http://www.androiddocs.com/google/play-services/id.html

In other words, on Android phones, this setting seems to be entirely based on trust, while on iOS the equivalent setting removes the ID, functionally preventing anyone from not respecting the consumers' choice. However, the setting to disable or limit ad tracking is disabled by default on both Android and iOS devices.

Making matters worse, the technical testing showed that, in many cases, the use of the system-level opt out settings had very limited effects on the sharing of personal data. Many third parties received the Advertising ID even if the user opted out of personalised advertising, and AdColony and AppsFlyer also received further personal data even if the setting was enabled. This happened even though Grindr had sent a signal that the user opted out of personalised advertising.[80]

Even if the consumer uses the device settings to opt out of personalized ads, or to reset their Advertising ID, this does not anonymize them if other identifiers are also being shared. The variety of identifiers being transmitted to third parties makes it exceedingly difficult to opt out of being tracked.

## 2.6 Real-time bidding

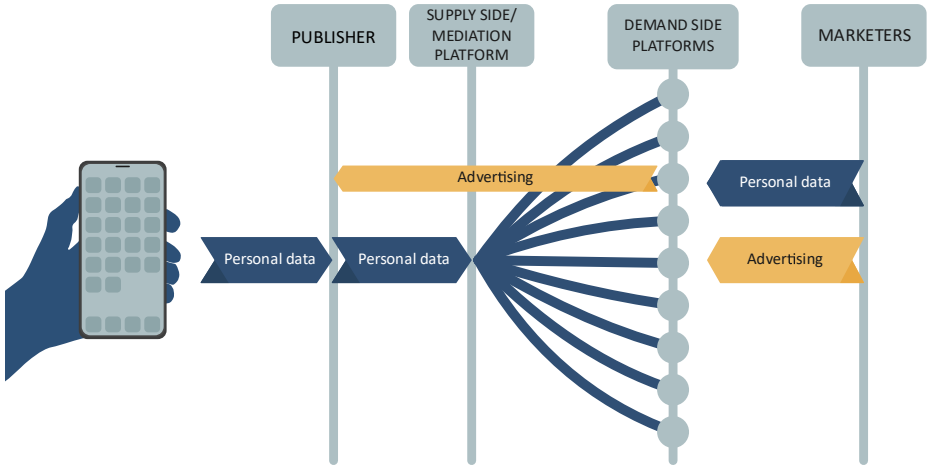
The system known as **real-time bidding** (RTB) underpins a significant portion of the online advertising industry. When an ad is displayed to us on a website or in an app, which is called an impression, this is often the result of a complicated RTB process, where potentially tens or even hundreds of advertisers automatically bid to display their ads. These auctions are based on a large amount of parameters determining the value of the individual consumer and the content currently served to the consumer via a website or app. All of this is an automated process that happens in milliseconds for every ad impression.

For example, a single mother who is interested in children's products may be an attractive target for a toy marketer, while a teenager who is feeling unattractive may be worth a lot to marketers trying to sell cosmetic surgery.

The system used to facilitate real-time bidding is very complicated and involves a large number of actors, who may fulfil a number of roles. The process can take various forms, such as **open auctions**, where any actors may participate, and **private auctions**, where publishers give bidders access based on various attributes. Additionally, rather than auctioning off ad space, publishers and

[80] Mnemonic, "Review of communications from apps", chapter 3.12 https://www.forbrukerradet.no/out-of-control/

marketers may have a direct agreement and fixed pricing, which is known as **preferred deals**.[81] A somewhat shortened and simplified overview of the RTB process is provided below.[82]




*7 Personal data is broadcast as part of the Real-time Bidding process.*

The real-time bidding process involves a variety of different actors. **Supply side platforms** (SSPs)[83] aggregate information about available ad space for specific users from several publishers, in order to sell it in the most profitable way.[84] The SSP can be compared to an auctioneer, where the inventory for sale is consumers' attention.

**Demand side platforms** (DSPs), in contrast, allow marketers to buy ad placements for specific users with certain characteristics or behaviours. Ad

---

[81] "Differentiating Between Open Auction, Private Auction, & Preferred Deal in Programmatic Advertising", Aarki https://www.aarki.com/blog/differentiating-between-open-auction-private-auction-preferred-deal-in-programmatic-advertising

[82] For a detailed explanation of the system and actors, see "The Great Data Race", page 10-16, Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/the-great-data-race/

[83] Also called "sell-side platforms" or "monetization platforms"

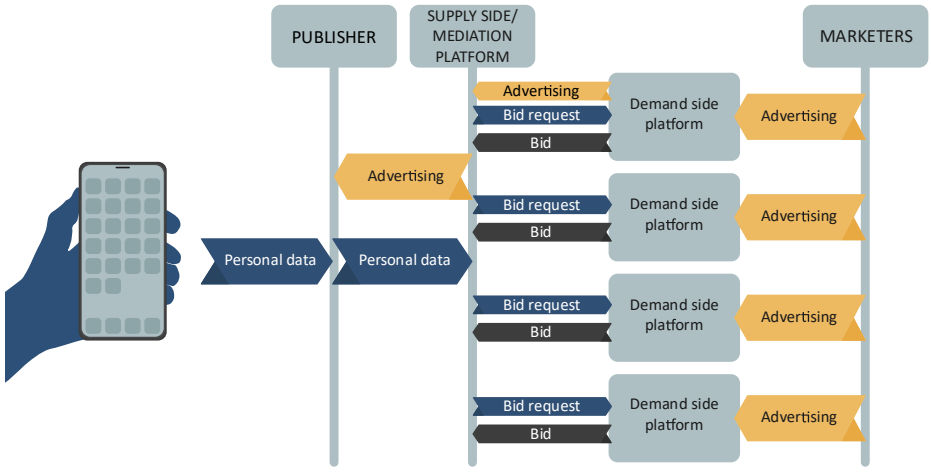
[84] Examples of supply side platforms include OpenX, Rubicon Project and Index Exchange. All of these companies also run ad exchanges. Examples of demand side platforms include The Trade Desk, MediaMath and Adform. Several vendors provide both supply side and demand side technology, including AppNexus, Amazon, Verizon, and above all, Google. "WTF is programmatic advertising?", Digiday https://digiday.com/wp-content/uploads/2018/06/digiday-wtf-programmatic-bible.pdf
"Privacy & market concentration: Intended & unintended consequences of the GDPR", Garret Johnson and Scott Shriver https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686
"Amazon Emerges As Google Challenger In Advertiser Perceptions SSP Report", Sarah Sluis https://adexchanger.com/platforms/amazon-emerges-as-google-challenger-in-advertiser-perceptions-ssp-report/

exchanges facilitate automated ad trading between publishers and marketers, mostly intermediated by SSPs and DSPs. Supply side platforms often include ad exchanges as a part of their services. Additionally, both publishers and marketers often use third party ad servers to show ads to users and to store log data about every ad transaction.[85]

Every time a person visits a website or uses an app with in-app advertising using real-time bidding, personal data flows to several vendors in the supply chain. This data may include data about a users' location, behaviour, sexual preferences, and much more.

When visiting a website, the whole process occurs in real-time and involves a high degree of automation and interconnection between many vendors. The system functions similarly in apps on mobile phones, although there may be additional delays between real-time bidding transactions and ad placements on mobile devices.

Typically, whenever an ad is about to be loaded on a website, specific software integrated in the website broadcasts a **bid request** based on information about the user, which may include information such as the URL of the website, geolocation, device information, various unique identifiers, IP address, and sometimes additional profile data compiled by data brokers. These bid requests are facilitated by vendors such as supply side platforms and ad exchanges.

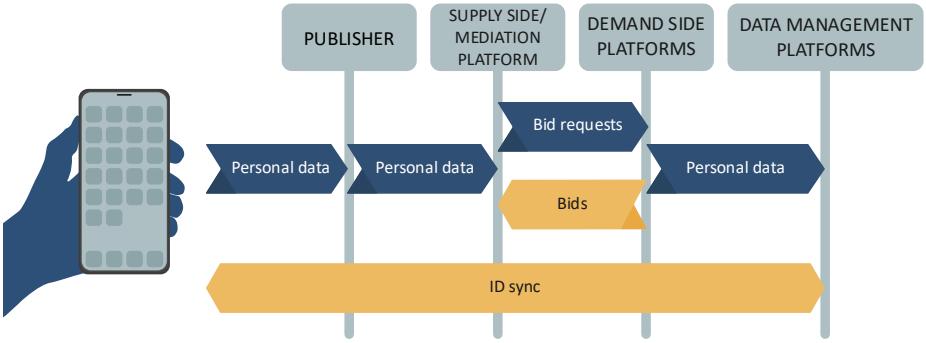



*8 Bid requests are sent to multiple DSPs as part of the RTB process.*

[85] "An EU competition law analysis of online display advertising in the programmatic age", Damien Geradin and Dimitrios Katsifis
https://www.tandfonline.com/doi/full/10.1080/17441056.2019.1574440

Bid requests are broadcast to a number of demand side platforms and other third party vendors, which can change between sessions. The DSPs decide whether to place a bid to show an ad on behalf of the marketer. Additionally, the data contained in the bid request can be collected by many of the companies involved in the process, including by data management platforms (DMPs).[86]

Data management platforms are used by publishers and marketers to combine data on their existing customers, including behavioural data collected from their websites and apps, with data from third party providers. They provide mechanisms to further analyse and refine data on consumers, and then analyse and utilize it across the web, mobile apps and other services.[87] As a part of the RTB process, DMPs also provide instructions to DSPs about which consumers to target based on the profiles that they compile.[88]




*9 Data management platforms can combine data received from the RTB process.*

As data management platforms often resell large amounts of third party data to many clients, in addition to compiling and combining the data, they can also be categorized as a type of data broker. Most of them maintain massive identity databases that help other companies to link digital profiles across contexts and vendors.[89]

---

[86] This process is described in the report "Behavioural advertising and personal data", Johnny Ryan. https://brave.com/Behavioural-advertising-and-personal-data.pdf

[87] "Corporate Surveillance in Everyday Life", page 47, Wolfie Christl https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[88] "Networks of Control", page 89, Wolfie Christl and Sarah Spiekermann https://crackedlabs.org/en/networksofcontrol

[89] Major DMP vendors include Oracle, Adobe, Salesforce, Nielsen, Neustar, Lotame, The ADEX, KBM Group (owned by the major advertising agency group WPP). Several adtech companies also provide DMP functionality, including MediaMath, AdForm, and Google.
"The Forrester Wave™: Data Management Platforms, Q2 2017", Forrester https://www.forrester.com/report/The+Forrester+Wave+Data+Management+Platforms+Q2+2017/-/E-RES136171

Because consumers often use apps on a more persistent basis than they use particular websites, one unique data flow that occurs in this environment is cached ads, where several videos or banner ads are downloaded for the user so that they can be displayed as a user scrolls through a feed or opens pages across an app.[90] These cached ads still typically occur via traditional auctions, but behind the scenes, through server to server transmissions.

In apps, advertising networks are often directly integrated into the app itself through a Software Development Kit. These SDKs are typically chosen by the app developer due to their ability to integrate between each other, or due to them providing a unique separate value.[91] Instead of supply side platforms, apps often use **advertising mediation platforms**, which are platforms that are directly integrated into apps through an SDK.

Advertising mediation platforms are services that facilitate advertising transactions in mobile apps. Mediation allows app developers to manage multiple advertising networks through one mediator. The mediation platform gives "multiple ad networks access to an app's inventory, creating an arena in which ad networks must compete for their ad to be served".[92]

This allows app developers to manage multiple advertising networks at once via one mediation interface, rather than integrating separate SDKs for each ad network. Advertisers place bids through the mediation platform, and the winner displays an ad in the app.

In this system, money changes hands after the ad has been placed or cached. Once the ad has been cached or displayed in the app or on the website, the winning DSP bidder pays the SSP, and the SSP pays the publisher that showed the ad to the user.

In short, before you are shown an advertisement on a website or in an app, potentially sensitive information about you may be broadcast to a number of

---

"Analytics 360 Suite products", Google Marketing Platform Help
https://support.google.com/marketingplatform/answer/6365892?hl=en

[90] "Pre-Caching", Twitter MoPub [accessed December 11, 2019]
https://developers.mopub.com/dsps/best-practices/pre-caching/

[91] In chapter 7, we show which apps were clearly coordinated through the MoPub mediation and which apps have a slightly more direct relationship with Grindr through their SDK.

[92] "Glossary", IronSource [accessed December 11, 2019]
https://www.ironsrc.com/glossary/ad-mediation/

different categories of companies. Different advertisers place bids on your attention through various demand side platforms, and within milliseconds an advertiser is declared the winner, meaning that you typically see an ad for a particular breakfast cereal, payday loan, or online casino.

The bid request, including personal data, is broadcast to all the DSPs, regardless of whether they win the bid or not. After all, the DSP needs to know who they are bidding on.

Some of these DSPs may store the data they received and use it for other purposes, even if they did not win the bid. Whenever a bid request is broadcast, more information about your identity and your habits is collected and stored to be used for the next bid request. Meanwhile, other data companies, such as DMPs, could also be hoovering up this data, and use it for other purposes.[93]

## 2.7 Push from civil society and regulators

Due to the privacy implications of the various companies and systems described above, the adtech industry has come under fire from both civil society and regulators on both sides of the Atlantic.

In 2018, complaints were lodged in several countries in Europe by numerous NGOs against the real-time bidding scheme supported by the Interactive Advertising Bureau, called OpenRTB,[94] and Google's Authorized Buyers RTB protocol.

[93] For example, the Norwegian-owned cross-device advertising company Tapad receives much of their data from the RTB system. Similarly, the third party data provider Gravy Analytics and AdSquare also collects data from bid requests.
"Tapad CEO On Cross-Device Graphs And Where Its Data Comes From (Hint: Not Telenor)", James Hercher https://adexchanger.com/data-exchanges/tapad-ceo-on-cross-device-graphs-and-where-its-data-comes-from-hint-not-telenor/
"Frequently Asked Questions", Gravy Analytics [accessed December 11, 2019] https://gravyanalytics.com/frequently-asked-questions/
"Data Quality: Turning the Challenge into an Opportunity" page 15, AdSquare [accessed December 11, 2019]
https://www.adzine.de/uploads/AdTrader_Data_Quality_adsquare_Luise_Weiss_freigegeben.compressed.pdf

[94] OpenRTB is the real-time bidding scheme supported by the Interactive Advertising Bureau (IAB), which was first introduced in 2010. The IAB is an umbrella organization with members from all segments of the adtech industry. Their OpenRTB scheme was debated by their members and the public, deployed into public advertising auctions on the internet and has evolved for years as the core architecture to share user data and conduct advertising auctions on the internet. Digital advertising based on OpenRTB is supplied with audience data from both websites and from apps.

According to these complaints, the IAB and Google's use of RTB is in breach of the General Data Protection Regulation.[95] These complaints address the broadcasting of personal data taking place every time an RTB-driven ad is shown.

As the complaints allege, personal data is broadcast through bid requests every time an ad is shown on a website, to a large number of adtech companies, including to demand side platforms and data management platforms. According to the complaints, this broadcasting of personal data constitutes a serious ongoing data breach on a massive scale.

The UK-based NGO Privacy International has filed complaints against seven data brokers and credit referencing agencies for profiling activities that they allege contravene the GDPR.[96] According to Privacy International, these data brokers' practices of collecting massive amounts of personal data from consumers around the world, in order to create detailed profiles on individuals, are illegal. The complaints argue that the companies do not have a valid legal basis for conducting these activities, and that the companies are engaging in mass exploitation of individuals' data.

In October 2018, the French data protection authority CNIL issued a decision against the French DSP Vectaury. Although a minor company in the adtech world, Vectaury was found to possess the personal data of more than 67 million people. The CNIL ruled that the adtech company did not have a valid legal basis for processing personal data.[97] Vectaury had operated by asking consumers for consent through the IAB consent framework, which the CNIL deemed to be insufficient.

As we will elaborate upon in chapter 8, this CNIL decision indicates that the IAB framework, or at least the Vectaury implementation of it, is not compliant with

---

"About OpenRTB", Interactive Advertising Bureau [accessed December 11, 2019] https://www.iab.com/guidelines/real-time-bidding-rtb-project/

[95] "Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR", Johnny Ryan https://brave.com/adtech-data-breach-complaint/

[96] "Privacy International files complaints against seven companies for wide-scale and systematic infringements of data protection law", Privacy International https://privacyinternational.org/press-release/2424/press-release-privacy-international-files-complaints-against-seven-companies

[97] "How a small French privacy ruling could remake adtech for good", Natasha Lomas https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/

the GDPR on the grounds that consent cannot be bundled or passed on through contractual agreements. According to the CNIL, such consent frameworks do not effectively ensure that third party vendors can prove the validity of the consent gathered by the publisher that passed on the personal data.

In 2019, the aforementioned complaints from Brave and different European NGOs prompted an investigation by the British Information Commissioner's Office (ICO), who published a report outlining a number of problematic cases of GDPR noncompliance within the adtech industry.[98] At the time of writing this report, none of the complaints have resulted in enforcement actions from data protection authorities, although the ICO confirmed many of their preliminary conclusions in November 2019.[99]

The ICO report makes a number of conclusions regarding the legality of some common practices amongst adtech companies, particularly regarding the RTB process. According to the regulator, the collection and processing of personal data that these companies engage in, is systematically noncompliant with the GDPR. The companies do not properly inform consumers about their practices, and they fail to collect explicit and informed consent for the processing of sensitive personal data.

According to the ICO, the entire adtech industry is shrouded in opacity, which contravenes the data protection principle of transparency. The comprehensive data collection and sharing that is at the centre of the adtech industry is also in conflict with central data protection principles such as purpose limitation, data minimisation, and accountability.[100]

The ICO also points to a comprehensive lack of safeguards regarding the collection and use of personal data. Special categories of personal data are being transmitted to a vast network of third parties without sufficient control mechanisms, and there is little to no guarantee of security of personal data

[98] "Update report into adtech and real time bidding", Information Commissioner's Office https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

[99] "ICO: adtech players are holding on to personal data", Omar Oakes https://www.campaignlive.co.uk/article/ico-adtech-players-holding-personal-data/1666221

[100] "The principles", Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

within the system.[101] The Commissioner summarized the current adtech system as disproportionate, intrusive and unfair.

> *"the creation and sharing of personal data profiles about people, to the scale we've seen, feels disproportionate, intrusive and unfair, particularly when people are often unaware it is happening.".*[102]

In the USA, there have also been several investigations and regulatory actions related to data brokers. In 2014, the Federal Trade Commission (FTC) investigated how data brokers compile segments of vulnerable consumers. The FTC concluded that the way that data brokers largely operate lacks transparency and oversight, and that consumers had little or no control over the data collection and profiling undertaken by these companies.

> *"The extent of consumer profiling today means that data brokers often know as much – or even more – about us than our family and friends, including our online and in-store purchases, our political and religious affiliations, our income and socioeconomic status, and more. It's time to bring transparency and accountability to bear on this industry on behalf of consumers, many of whom are unaware that data brokers even exist."*[103]

Although the US does not have a comprehensive national data protection legislation, there have been some regulatory initiatives on a state-by-state level. In 2018, the state of Vermont passed a law regulating some activities undertaken by data brokers, mandating certain security measures and attempting to increase transparency by introducing a data broker registry.[104] Similarly, in 2019, California introduced amendments to the California Consumer Privacy Act, including requiring that all data brokers have to register with the state's Attorney General.[105]

---

[101] In the GDPR, special categories of personal data include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". GDPR Art. 9(1)

[102] "Update report into adtech and real time bidding", Information Commissioner's Office https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

[103] "FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information", Federal Trade Commission https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

[104] "Vermont's New Data Privacy Law", Adam Schwartz https://www.eff.org/deeplinks/2018/09/vermonts-new-data-privacy-law

[105] "CCPA and California's New Registration Requirement", Shalin R. Sood https://www.natlawreview.com/article/ccpa-and-california-s-new-registration-requirement

# 3 The harmful effects of profiling and behavioural advertising

Because online tracking, profiling, and behavioural targeting is so pervasive and systemic across the internet, it is difficult to measure the extent of the harm that may arise as a result of the practices. However, there are a number of individual and collective harmful effects that can be pointed out.

An individual harm is the direct negative effects on a particular consumer, where the data collected about the consumer are used in a way that produces a negative effect, such as being excluded from certain services or receiving higher prices for products or services. A collective harm arises from the indirect effects on society or groups of consumers as a whole. For example, if online surveillance has the effect of dissuading individuals from looking for information online, this creates a collective harm to society over time because public debate may become less informed.

The harmful effects of commercial surveillance, profiling and behavioural targeting expand beyond privacy concerns. In a 2019 report, Amnesty International describe the systematic surveillance made possible by tech giants such as Google and Facebook as a systemic threat to human rights. According to Amnesty International, data-driven persuasion is a serious threat to human rights such as freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination.

> *"These capabilities mean there is a high risk that the companies could directly harm the rights to freedom of thought, conscience and religion and freedom of opinion and expression through their use of algorithmic systems."*[106]

## 3.1 Consumers do not want to be tracked, but feel powerless

Setting aside the fact that much of the personal data collected through the adtech system may be used for other purposes than targeted advertising, and that it is possible to show digital advertising without profiling the user, it is pertinent to ask whether consumers are actually bothered by profiling and tracking. After all, a relevant ad may be perceived as better or less annoying than an individually tailored ad.

[106] "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights", Amnesty International
https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

A growing number of recent studies are showing that in general, consumers are not comfortable with comprehensive online tracking and profiling. Many find targeted advertising "creepy" or intrusive, even if they do not understand how ads are being targeted and how much data collection is going on.[107] These studies indicate that consumers do not want their personal data being used for purposes beyond providing the service they signed up for.

A 2019 RSA survey showed that 68 % of respondents regarded "tracking online activity to tailor advertisements" to be unethical, while only 29 % agreed that providing more data leads to better products and services.[108]

Similarly, a recent study from the Norwegian Computing Center showed that 86 % of Norwegian consumers disagreed with the statement "Providers of digital services, such as an app, should have the right to share information about me with third parties".[109] Similarly, 69 % of respondents agreed with the statement "It should become more difficult to store personal data that can be used for creating digital profiles", while only 11 % disagreed.[110]

Other studies have shown that consumers are particularly concerned about their location being tracked. For example, one 2018 study showed that 75-80 % of respondents felt vulnerable when their location data was shared.[111]

On a similar note, a 2019 study on cookie consent notices showed that if consumers were asked to actively opt in to third party tracking for personalization and advertising, less than 0.1% of respondents agreed to be tracked.[112] This indicates that if given a choice where they actively had to accept

---

[107] One 2018 industry study found that 75% of respondents found "most forms of personalization at least somewhat creepy" "What Brands Should Know About Creating Memorable Experiences", Inmoment https://www.inmoment.com/wp-content/uploads/2018/02/2018_CX_Trends_Report-1.pdf

[108] "RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses", RSA https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf

[109] "Nordmenn og deling av persondata", page 46, Norwegian Computing Center https://www.nr.no/sites/default/files/files/NR-Rapport_Nordmenn-og-deling-av-persondata_ALerT2019.pdf

[110] Ibid. page 63

[111] "Privacy and Location Data: Global Consumer Study March 2018", HERE Technologies https://www.here.com/sites/g/files/odxslz166/files/2019-02/HERE%20Technologies%20Privacy%20and%20Location%20Data%20Global%20Consumer%20Study%20March%202018%20-%20Reviewed.pdf

[112] "(Un)informed Consent: Studying GDPR Consent Notices in the

tracking and personalization, a large majority of consumers would decline the offer.

The widespread use of ad blockers is a another concrete symptom of consumer sentiment against tracking for advertising purposes. Although available statistics about the prevalence of ad blockers vary in conclusions,[113] several studies have found privacy concerns and the intrusiveness of targeted ads as important reasons for consumers blocking online advertising.[114] As a side note, because of negative effects on publisher revenue, Google have banned most ad blockers from the Google Play store.[115]

Despite being concerned about the pervasive data sharing and commercial surveillance online, consumers often feel powerless to limit the tracking. Although there seems to be a discrepancy between what consumers want (less tracking) and how they often act online (click "I accept", share data with apps), this could be explained both by the complexity of the system, and by a general feeling of resignation in the face of massive and seemingly unavoidable data collection.[116]

## 3.2 Power asymmetries and lack of transparency

Large parts of the adtech industry operate in the shadows, and consumers are often not even aware of the existence of the system. This creates a significant power asymmetry, where any given adtech company may be armed with thousands of data points about an individual and a large arsenal of insights derived from behavioural psychology, while the individual has no idea about the company even existing. Because of this imbalance, it is extremely difficult for consumers to opt out or otherwise protect themselves from being profiled and categorized. When we are not aware of being targeted by this arsenal of data and persuasion techniques, the chances of being influenced or otherwise manipulated increase.

---

Field", Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holtz https://arxiv.org/pdf/1909.02638.pdf

[113] "Is ad blocking past 2 billion worldwide?", Doc Searls https://blogs.harvard.edu/doc/2019/03/23/2billion/

[114] "Global Ad-Blocking Behaviors In 2019 - Stats & Consumer Trends (infographic)", Daniyal Malik https://www.digitalinformationworld.com/2019/04/global-ad-blocking-behaviors-infographic.html

[115] "Google just took a much clearer stance on banning ad blocking apps (but ad blocking browsers are still OK)", Lara O'Reilly https://www.businessinsider.com/google-just-took-a-much-clearer-stance-on-banning-ad-blocking-apps-but-ad-blocking-browsers-are-still-ok-2016-3

[116] "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation", Joseph Turow, Michael Hennessy and Nora Draper https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

The opaqueness of the adtech system is exacerbated by the sheer number of third parties that can be involved in a single transaction. A consumer using a particular app may understand that the app requires some data collection in order to function. Some consumers may also know that in-app advertising is based on data collection and analysis. However, knowledge about which third parties are actually receiving data from the app is only available to consumers who are able to both read lengthy and legalistic privacy policies and perform a technical analysis of the app traffic.

If one actually attempts to read the privacy policy of any given app, the third parties who may receive personal data are often not mentioned by name. If the third parties are actually listed, the consumer then has to read the privacy policies of these third parties to understand how they may use the data. These other third parties may be sharing data with their own third party partners, and so on. In other words, it is practically impossible for the consumer to have even a basic overview of what and where their personal data might be transmitted, or how it is used, even from only a single app. The system behind even the most seemingly basic transaction could include hundreds of third parties, that all have their own purposes and policies concerning data processing.

Under the General Data Protection Regulation (GDPR) consumers in Europe have a number of fundamental rights concerning their personal data, including the right to object, the right to an explanation, and the right of erasure.[117] However, these rights become impossible for the individual to exercise when the extent of data collection, use and sharing is so massive and complex. The lack of transparency throughout the adtech system also exacerbates a number of other problematic issues, which are highlighted below.

## 3.3 Manipulation

Although the use of marketing to persuade or manipulate consumers is not a new phenomenon, the increasing personalisation further tilts the scales of power in favour of the marketers.[118] When companies engage in comprehensive tracking, categorization, and profiling based on vast amounts of data, this places the consumer at a significant disadvantage. If a company knows your habits, your inclinations, and your desires, it is substantially better

[117] See chapter 8 for a detailed legal analysis of the widespread processing of personal data throughout the adtech industry.
[118] "The Great Data Race", page 40-41, Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/the-great-data-race/

equipped to manipulate you than if it only knew that you have an interest in cars because you watch Top Gear or bought a car magazine.

Advertising can be a powerful medium, and when left unchecked it can be used to target consumers in vulnerable positions.[119] With ubiquitous technology such as smartphones, advertisers are no longer confined to guessing when the consumer will respond to an ad. They can analyse vast amounts of user data to pinpoint the right moment, and measure every interaction in real time to further refine the message and timing. For example, Google touts the advantages of reaching consumers at the exact "micro-moment" when the consumer is uniquely receptive because they need or want something.[120]

One iteration of targeted advertising is known as "emotional targeting", which analyses a person's emotional state based on parameters such as behaviour, sentiment analysis, facial recognition, and more, in order to increase the chances of influencing behaviour.[121] This technology is designed to circumvent the defence mechanisms most of us passively employ when we see traditional advertising. This means that we are all in a potentially vulnerable position when faced with behavioural targeting.

Detailed targeting can also effectively be used to single out consumers or groups who are particularly vulnerable or otherwise receptive. For example, in a 2013 US Congressional hearing, data brokers were found to compile lists of consumers using segments such as "rape sufferers" and "AIDS/HIV sufferers".[122]

## 3.4 Discrimination

The significant information asymmetry between consumers and many adtech companies enable new forms of price discrimination.[123] Extensive knowledge about purchase histories, browsing habits and economic situations can be

[119] "Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'", Sam Levin https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

[120] "The basics of Micro-Moments", Google [accessed December 11, 2019] https://www.thinkwithgoogle.com/marketing-resources/micro-moments/micro-moments-understand-new-consumer-behavior/

[121] "Emotional and Sentiment Targeting", ADmantX [accessed December 11, 2019] https://www.admantx.com/emotional-and-sentiment-targeting/

[122] "Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'", Kashmir Hill https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/

[123] "Cookie monsters: why your browsing history could mean rip-off prices", Arwa Mahdawi https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsters-why-your-browsing-history-could-mean-rip-off-prices

leveraged to determine the maximum price a consumer is willing to pay for a product or service, and adjust the pricing accordingly.[124] If the price of a product or service differs on an individual level, it also becomes impossible for consumers to compare offers. Similarly, (dis)information campaigns using targeted messaging are difficult to uncover and survey, because two people will never see the same message.

The use of segmentation for advertising can also be exploited for other discriminatory purposes, for example by excluding certain groups of people from seeing specific offers and messages. Although many data brokers and adtech companies may avoid using prohibited or controversial categories such as race, sexual preferences or religion to target ads, there are numerous proxy properties that can serve as substitutes. For example, as will be elaborated upon in chapter 7, the use of the dating app Grindr is a strong indicator of sexual orientation, because it is primarily aimed at gay, bi, trans and queer people.

In 2017, Facebook was discovered to allow the targeting of ads to "Jew haters", and provided audience segments based on proxies such as "ethnic affinity", which enabled advertisers to exclude African-Americans from seeing certain housing ads.[125] In 2019, Facebook came under fire again for allowing advertisers to discriminate based on age.[126] Such practices are exceedingly difficult to identify by both consumers and by authorities, since identification of the exclusionary practices relies on knowing what you are *not* seeing.

Automatic segmentation of consumers can also lead to potentially harmful categorizations, demonstrated by Facebook's algorithms automatically creating categories such as "interested in treason" and "children interested in alcohol".[127] Even if these automatically created categories may be inaccurate or of dubious use to marketers, they could be abused by rogue actors or repressive governments.

---

[124] "How companies use personal data against people", page 31-32, Wolfie Christl https://crackedlabs.org/en/data-against-people

[125] "Facebook (Still) Letting Housing Advertisers Exclude Users by Race", Julia Angwin, Ariana Tobin and Madeleine Varner https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin

[126] "Housing companies used Facebook's ad system to discriminate against older people, according to new human rights complaints", Marie C. Baca https://www.washingtonpost.com/technology/2019/09/18/housing-companies-used-facebooks-ad-system-discriminate-against-older-people-according-new-human-rights-charges/

[127] "Children 'interested in' gambling and alcohol, according to Facebook", Alex Hern https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook

Discrimination may also take other forms, such as excluding individuals and groups from job postings and housing ads. The concept of being excluded or otherwise discriminated against based on assumed interests has been referred to as "discrimination by association".[128]

## 3.5 Purpose creep

Although many actors in the adtech industry are predominately focused on showing and targeting ads, data brokers are not confined to using their accumulated data and profiles for advertising purposes. The information that they collect, and the profiles and segments derived therefrom, is valuable to a vast variety of other actors.

When the use of personal data moves out of advertising and into markets such as credit scoring and insurance, the consequences could be life-changing for individual consumers.[129] The effects of automated decisions may be difficult to see for the affected individual, and there is an added risk of the decisions being incorrect. If data sets are incomplete or erroneous, or are used irresponsibly, the consequences can be disastrous. If the consumer does not know that they are the victim of an erroneous decision, there is no way to protest or correct the situation.

For example, in 2019, an Indian fintech company was found to use data collected from mobile apps as part of its credit scoring system.[130] In this case, consumers who had downloaded a music app to their phones were having their contact lists, user IDs, and GPS coordinates siphoned by the fintech company, who in turn used this as part of its system to help lenders decide whether to approve loan applications. The consumers would have no idea that this was happening, and consequently could not protest or protect themselves.

The risks of manipulation arising from the combination of big data and behavioural psychology are not uniquely commercial. Similar technologies are

[128] "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising", Sandra Wachter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639

[129] "Now wanted by big credit bureaus like Equifax: Your alternative data", Steven Mendelez https://www.fastcompany.com/90318224/now-wanted-by-equifax-and-other-credit-bureaus-your-alternative-data

[130] "How Sai Baba Was Made To Spy On Your Phone For Credit Ratings", Gopal Sathe https://www.huffingtonpost.in/entry/fintech-apps-privacy-snooping-credit-vidya_in_5d1cbc34e4b082e55373370a

also used by political campaigns to influence voters.[131] The most infamous example of this is the Cambridge Analytica scandal, where a data company used voter and consumer data from Facebook and other sources in an attempt to influence elections in several countries. The modus operandi of Cambridge Analytica included identifying undecided voters, or supporters of political opponents who were deemed easily persuaded to stay home, and target these voters with messages meant to discourage them from voting. These techniques, which one whistle-blower called a "psychological warfare tool", were applied in elections around the world.[132]

Although Cambridge Analytica was dissolved after the scandal, former employees are reportedly working on the Trump 2020 campaign, through the company Data Propria.[133] Both Cambridge Analytica and Data Propria leverage behavioural analytics and big data analytics in an attempt to influence behaviours:

> *"We use behavioral science to understand the motivations, needs and individual differences of our clients' audiences, and use those insights to personalize communications and affect behavior change. We also use psychological insight to optimize communications and 'nudge' behavior independent of segments. All of our work starts with the end in mind, looking to impact tangible, real-world metrics for our clients."*[134]

Similarly, in the run up to the 2020 US elections, the Trump re-election campaign was reportedly using the services of a data company that uses data from data brokers to influence voters. [135] According to the company, this data includes location data and behavioural data, which was harvested from mobile apps.

> *"While voter files are extremely valuable, some campaign managers are beginning to realize that each voter's smartphone is the ultimate voter file. Mobile data can tell them everything from the device operating system (iOS or Android) to what other apps are on the device, what Wi-Fi networks the device joins and much more. And that doesn't even cover the*

---

[131] "Personal Data: Political Persuasion - The Guidebook and Visual Gallery", Tactical Tech https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry/

[132] "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower", Carole Cadwalladr https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[133] "June 15, 2018: Trump 2020 campaign secretly working with former Cambridge Analytica staffers: AP", Jeff Horwitz https://www.chicagotribune.com/nation-world/ct-trump-campaign-cambridge-analytica-20180615-story.html

[134] "Work With Us", Data Propria career posting for a behavioural scientist [accessed October 8, 2019]. https://datapropria.com/careers/

[135] "The Trump Campaign is Deploying Phone Location-Tracking Technology", Lee Fang https://theintercept.com/2019/12/11/the-donald-trump-campaign-is-deploying-phone-location-tracking-technology/

> *information it's possible to infer, such as gender, age, lifestyle preferences and so on.*
>
> *Knowing who's in their voter file, campaign managers can use mobile data and mobile advertising to identify and engage voters who give off similar digital signals to their identified supporters. In the cutthroat world of politics, campaign marketers now have access to more power and precision than they've ever had."*[136]

The use of consumer data to influence voters blurs the line between consumer protection, data protection, and civil rights. It shows how data collected for one purpose may be reused in unpredictable contexts and for nebulous purposes, and can potentially impact society in major ways.

Although you may want Facebook to have information regarding what you are interested in and who your friends are in order to get the most out of the social network, it is not given that you would approve of a company like Cambridge Analytica taking this data to attempt to influence your vote. Even if you were OK with that, as we have shown above, trying to control which companies who have access to what data for what purposes is practically impossible.

## 3.6 Security and fraud

The accumulation and spread of consumer data that is happening across the adtech industry creates significant security risks to both individual consumers and to society at large. Detailed profiles on individuals can fall into the wrong hands, and be used for nefarious purposes such as identity theft and blackmail. The large number of actors who have access to this information increases the risk that criminals will be able to gain access through a data breach.

The credit referencing agency Equifax was infamously exposed to such a data breach in 2017, where the sensitive personal data of 143 million American consumers, including names, social security numbers, addresses, credit card numbers and more, were exposed.[137] Consequently, consumers were targeted with fraud attempts from criminals who either had access to the data, or who took advantage of the data breach by posing as Equifax representatives.[138]

---

[136] "Before the Gold Rush: A New Way to Reach Voters", Phunware [accessed December 13, 2019] https://www.phunware.com/blog/before-gold-rush-new-way-reach-voters/

[137] "Equifax Data Breach Settlement", Federal Trade Commission https://www.ftc.gov/equifax-data-breach

[138] "Two years after huge Equifax breach was revealed, consumers are still too vulnerable to identity theft'," Sarah O'Brien https://www.cnbc.com/2019/09/06/two-years-after-equifax-breach-consumers-still-vulnerable-to-id-theft.html

In November 2019, a data set of 1.2 billion records, including personal data, was discovered exposed online. A large portion of this data set originated from the data broker People Data Labs, who claims to have data for sale on 1.5 billion people. According to security researchers, this data had likely been bought legitimately from People Data Labs before being exposed online by a client.[139]

In some cases, widespread sharing of personal data can become a matter of physical safety. For example, users of the dating app Grindr have been located and targeted in countries where homosexuality is illegal.[140] Proxy attributes such as location data and interests, that are often used for behavioural advertising, could also reveal sensitive information related to topics such as sexual preferences or religious beliefs.[141] If personal data is spread to hundreds of companies, repressive governments may only need to gain access to the databases of one of these in order to single out individuals, or perform large-scale surveillance.

## 3.7 Chilling effects and freedom of expression

Although much of the online adtech industry is practically invisible to the consumer, massive data collection has the potential to create chilling effects. Studies have shown that when individuals feel that their behaviour is being recorded and can possibly be used against them, they will moderate themselves accordingly.[142] In the system of ad tracking, practically everything is recorded and can be used for unpredictable purposes. This may affect how we use the internet, and have negative consequences on freedom of speech.

For example, if a consumer thinks that their online search history could have an effect on their health insurance premiums, they may be dissuaded for searching for information about their medical conditions, or to abstain from any behaviour that could lead to inferences about their physical wellbeing. Similarly, if a consumer believes that online shopping prices will be dynamically adjusted

[139] "1.2 Billion Records Found Exposed Online in a Single Server", Lily Hay Newman https://www.wired.com/story/billion-records-exposed-online/

[140] "Egyptian police 'are using Grindr to find and arrest LGBT people'". Matt Payton https://www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-app-arrest-lgbt-gay-anti-gay-lesbian-homophobia-a7211881.html

[141] "Facebook's ad data may put millions of gay people at risk", Chris Stokel-Walker https://www.newscientist.com/article/2214309-facebooks-ad-data-may-put-millions-of-gay-people-at-risk/

[142] "Government Surveillance and Internet Search Behavior", Alex Marthews and Catherine E. Tucker https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

according to their search history, they may be reluctant to compare prices or look for alternatives.

Chilling effects can have serious long-term consequences for freedom of expression, for democratic institutions, and for society at large. Although these issues are complex and not solely technical problems, the massive online industry of tracking and profiling consumers may be considered an enabling factor.

## 3.8 Reduced trust in the digital economy

The widespread tracking across the online world has the potential to seriously degrade consumer trust in digital services. As described above, many consumers are concerned about their privacy, but feel powerless to restrict or prevent online tracking and surveillance. In many cases, the only way to stop tracking is to avoid using certain products and services.

As a consequence of the large scale commercial surveillance that is happening against consumers' wishes and interests, many consumers may avoid using digital services. This lack of trust can have the long-term effect of reducing the uptake of new innovative technologies. For example, a 2019 Deloitte survey of the Nordic countries showed more than 70 % being concerned with companies sharing personal data with third parties.[143] Indicating how this lack of trust may impact businesses, a 2018 RSA survey showed that 69 % of respondents would boycott a company that "repeatedly showed they have no regard for protecting customer data".[144]

The prevalence of tracking and profiling may also have negative effects on start-ups and other innovative entities that aim to create privacy-friendly alternatives. Although one aim of the implementation of the GDPR in Europe was to create a level playing field for businesses, this relies on consistent compliance. When a major part of the digital advertising market relies on expansive tracking and profiling, this creates an uneven playing field for companies that aim at respecting consumer and data protection rights.

For example, companies that use less invasive advertising technologies such as contextual advertising may suffer barriers to market entry. If service-providers

[143] "Deloitte Global Mobile Consumer Survey 2019 The Nordic cut", Deloitte https://www2.deloitte.com/no/no/pages/technology-media-and-telecommunications/topics/global-mobile-consumer-survey.html
[144] "RSA Data Privacy & Security Report", RSA https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf

and publishers that adhere to the law are put at a competitive disadvantage, this fuels a race to the bottom, where the companies that perform the most sophisticated tracking may squeeze out companies that try innovate on topics such as data protection and security. This situation has potentially serious consequences for innovation and competition.[145]

A race to the bottom may also have the side-effect of depressing the value of data, which may fuel further extensive sharing of personal data, leading to market inefficiencies from a competition point of view.[146]

## 3.9 Ad fraud and degradation of online services

A vast majority of online services are financed through advertising, much of which is served through the adtech system. For example, online newspapers and other publishers often have few direct contracts with advertisers, but use ad networks and adtech companies as intermediaries. This means that the publisher often has no idea what ads are being shown on the articles that they publish, and that different consumers will see different ads when they visit the same article. Similarly, the advertisers do not have any direct contact with the publisher, but buy ads through the adtech intermediaries. The intermediary facilitates a number of transactions that are often opaque to both the publisher and the advertiser, and has been described as a black box.[147]

Studies have shown that up to 70 % of advertising revenue online may go into the adtech supply chain.[148] Publishers are paid by the number of clicks on an ad, but due to the opaqueness of the adtech system there is a vast amount of ad fraud throughout the system.[149]

Ad fraud happens when, for example, bots with automated scripts visit webpages and/or watch videos or click ads. Consequently, adtech companies

[145] "Access to Consumers' Data in the Digital Economy", BEUC https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf
[146] "Too Much Data: Prices and Inefficiencies in Data Markets", Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asu Ozdaglar https://economics.mit.edu/files/17760
[147] "Report: Ad fraud to hit $23 billion, isn't going down", George P. Slefo https://adage.com/article/digital/report-ad-fraud-hit-23-billion-isnt-going-down/2174721
[148] "Where did the money go? Guardian buys its own ad inventory", David Pidgeon https://mediatel.co.uk/newsline/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/
[149] "Brave answers US Senators questions on privacy and antitrust – Questions from Senator Booker", Johnny Ryan https://brave.com/senate-qrfs-june2019/#_Toc11255960

and publishers end up overpaying for human eyeballs, and are paying a lot of money to show ads to bots. There are numerous ways that this is done both on publisher sites and in apps.

The most complex forms of ad fraud are highly technical complicated financial schemes, designed to generate and push revenue through adtech services, in order to get paid by ad networks and publishers for that traffic. For example, a 2018 investigation by BuzzFeed uncovered a massive ad fraud scheme, where more than 125 Android apps were being used to generate fake views.[150] This type of fraudulent activity, combined with the amount of money going to middlemen, raises questions about whether behavioural targeting is actually generating more revenue for publishers and marketers than traditional or contextual advertising.[151]

Since brands and advertisers have little control over where their ads are shown in the adtech system, there is an opportunity for unscrupulous adtech partners and ad networks to place ads on low-quality or fraudulent sites. The potential for ad fraud therefore has been claimed to incentivize low-quality content and misinformation online.[152] Thus, the click-driven advertising systems of the adtech industry may be partly responsible for a general degradation of online content, in addition to being saddled with significant fraudulent activities.[153]

# 4 Methodology: Observing data flows from apps to third parties

The research behind this report was performed in the months of June to November 2019. The research on the adtech industry and specific data brokers was performed by the researcher Wolfie Christl of Cracked Labs together with the Norwegian Consumer Council. In order to identify whether personal data was transmitted from apps to commercial third parties, the Norwegian Consumer Council also commissioned a technical test of ten apps from the

[150] "Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme", Craig Silverman https://www.buzzfeednews.com/article/craigsilverman/how-a-massive-ad-fraud-scheme-exploited-android-phones-to

[151] "Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests", Keach Hagey https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195

[152] "How the Adtech Market Incentivizes Profit-Driven Disinformation", Joshua Braun https://promarket.org/how-the-adtech-market-incentivizes-profit-driven-disinformation/

[153] The role of adtech as an enabler to monetize disinformation is covered in detail by the Disinformation Index. https://disinformationindex.org/

security company Mnemonic. The technical tests were performed in Norway between June and September 2019.

After having analysed the results of the technical tests and the legal documentation from the companies in question, an analysis of the legal grounds for processing personal data was conducted by the Norwegian Consumer Council with assistance from noyb.

## 4.1 Method

The technical tests aimed to reveal and document data transmissions from the apps to third parties, and the contents of those data flows. The scope of the testing performed for this report was limited to apps running on Google's Android operating system. There are several reasons for analysing apps on an Android phone rather than a phone running Apple's iOS. First of all, Android is by far the largest mobile operating system worldwide.[154] Furthermore, as is described in chapter 6.4, Google is a key player in the adtech industry, controlling significant parts of the adtech supply chain. This made it particularly interesting to see how Google's operating system provided or restricted adtech-related tracking opportunities.

Additionally, compared to other systems such as Apple's iOS, the Android operating system has a more open architecture, which traditionally has been more exposed to security issues and weaknesses. Due to Android's architecture, it is easier to observe data transmissions from the device running the app. This does not mean that the problems discussed in this report are necessarily unique for Android.[155]

The ten apps that were tested were chosen by looking at the most popular apps on Google Play in certain categories where sensitive category personal data was deemed likely to be processed, such as data about health, religion, children, and sexual preferences.

A large number of apps were scanned using the free online tool Exodus Privacy, which automatically unpacks the apps to give an overview of integrated trackers and software development kits.[156] From these cursory scans, the number of

[154] "Smartphone Market Share", IDC https://www.idc.com/promo/smartphone-market-share/os

[155] The methodology for technical testing is described in detail in Mnemonic, "Review of communications from apps", https://www.forbrukerradet.no/out-of-control/

[156] Exodus Privacy is a French non-profit organization that provides open source tools for scanning mobile apps for trackers. http://exodus-privacy.eu.org

apps was narrowed down based on number of integrated trackers, combined with an analysis of whether these trackers were likely to be used for purposes beyond what is necessary for the functioning of the app. Therefore, this research cannot provide a complete overview of the app environment, but focuses on a number of popular apps that may transmit data to a larger number of third parties than others.

The apps that were tested were the dating apps Grindr,[157] Happn,[158] OkCupid,[159] and Tinder,[160] the fertility/period tracker apps Clue[161] and MyDays,[162] the makeup app Perfect365,[163] the religious app Muslim: Qibla Finder,[164] the children's app My Talking Tom 2,[165] and the keyboard app Wave Keyboard.[166]

Based on the results from the technical tests, we chose to focus on several third parties that received sensitive category personal data from these apps. Due to time constraints, we simply could not analyse every company that was observed receiving data from the apps. Together with Wolfie Christl, the Norwegian Consumer Council researched the third parties and scrutinized their practices for data collection and processing. This research provided the basis for selecting certain third parties to analyse further.

When analysing the data flow from the Grindr app, our team observed Twitter's MoPub acting as a mediation network, which was facilitating personal data transmissions to other third parties. This particular SDK architecture, in addition to the sensitive nature of the Grindr app, prompted the commission of the researcher Zach Edwards to audit and analyse the app in depth. This is described in detail in chapter 7.

---

[157] Grindr https://play.google.com/store/apps/details?id=com.grindrapp.android
[158] Happn https://play.google.com/store/apps/details?id=com.ftw_and_co.happn
[159] OkCupid https://play.google.com/store/apps/details?id=com.okcupid.okcupid
[160] Tinder https://play.google.com/store/apps/details?id=com.tinder
[161] Period Tracker Clue - Ovulation and Cycle Calendar
https://play.google.com/store/apps/details?id=com.clue.android
[162] MyDays - Ovulation Calendar & Period Tracker
https://play.google.com/store/apps/details?id=com.chris.mydays
[163] Perfect365 https://play.google.com/store/apps/details?id=com.arcsoft.perfect365
[164] Muslim: Qibla Finder, Prayer Times, Quran, Azan
https://play.google.com/store/apps/details?id=com.hundred.qibla
[165] My Talking Tom 2
https://play.google.com/store/apps/details?id=com.outfit7.mytalkingtom2
[166] The Keyboard app was chosen because custom keyboards normally have access to a lot of functions on the phone. Wave Keyboard Background - Animations, Emojis, GIF
https://play.google.com/store/apps/details?id=com.wave.keyboard

Based on analyses by Christl and Edwards, the NCC performed the below analysis outlining the central findings regarding the apps and relevant third parties. This was followed by a legal analysis, performed with assistance from noyb, where the industry and system was examined in light of the General Data Protection Regulation.

## 4.2 Expected and unexpected data transmissions

In general, most apps can be expected to transmit data to third parties for a variety of purposes. In order to make sure the app functions as intended, the service provider may use one or more third party service providers that process data on their behalf. In the digital environment, the publisher cannot perform all of these tasks themselves, so it is common that some tasks are outsourced. In these cases, the partnership normally is bound by a contract that stipulates the limits of what the third party may use data for.

Common reasons for sharing data with third parties include to ensure basic functionality, for crash reports and analytics, to show advertising in the app, and/or for tracking and profiling the user.

For example, it is reasonable that an app for cloud storage actually sends uploaded files to the cloud server. Similarly, an app that integrates social media functions would be expected to send certain data to the social media company. Similarly, when showing in-app advertising, it is fair to expect that the app will notify the ad server that it should place an ad. However, this does not necessitate telling the ad server the geolocation, sexual preferences, political views, gender, religious convictions, or other personal information such as unique identifiers referring to the user.

## 4.3 Limitations of the data flow analysis

During the technical testing, Mnemonic observed data transmission to many third parties that either could not be identified for various reasons, for example due to technical limitations or because the content of the transmissions were unclear (e.g. obfuscated or encrypted). Several third parties were observed receiving data transmissions that did not include personal data, and therefore they will not be touched upon below. The limitations of the technical testing is described in detail in Mnemonic's technical report.

As all of the apps included a number of integrated SDKs typically used for tracking and advertising purposes, it can be assumed that there are other possible data transmissions that simply were not triggered during the testing.

This means that the data transmissions described below and in Mnemonic's technical report may just be part of the picture. In other circumstances, personal data may be sent to other third parties that were not observed during the testing. Details about the methodology and testing setup can be found in the technical report from Mnemonic, which is available online.[167]

| App | #SDKs | Companies with integrated SDK |
|---|---|---|
| Clue | 6 | Adjust, Amplitude, Apptimize, Braze/Appboy, Google Crashlytics, Google Firebase. |
| Grindr | 18 | AdColony, AppsFlyer, Braze/Appboy, Google Crashlytics, Facebook, Fyber, Google Firebase, OpenX, Inneractive, AdColony, Millennial Media, Moat, MoPub, OpenX, SafeDK, Smaato, Tencent, Vungle. |
| Happn | 7 | Adjust, Braze/Appboy, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, Mopub. |
| Muslim: Qibla Finder | 20 | AdColony, Amazon Advertisement, AppLovin, AppMetrica, AppNext, Appo-deal, Facebook Ads, Google Ads, Google Firebase, InMobi, Integral Ad Science, Ironsource, Moat, MoPub, Nexage, StartApp, TapJoy, Unity3d, Vungle, Yandex. |
| My days | 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. |
| 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. |
| OkCupid | 10 | AppsFlyer, Braze/Appboy, Embrace, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, Kochava, MoPub, MParticle. |
| 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, Sense360, SerServ, Tap Research, Tencent, Unacast, Unity3d, Vungle. |
| Tinder | 7 | AppsFlyer, Branch, Facebook Ads, Google Ads, Google Crashlytics, Google Firebase, LeanPlum. |
| Wave Keyboard | 14 | AppLovin, Avocarrot (Glispa), Chartboost, Facebook Ads, Flurry, Fyber, Google Ads, Google Crashlytics, Google Firebase, OneAudience, OneSignal, PubNative, Unity3d, Vungle. |

A necessary limitation of a data flow analysis is that it can only cover direct transmissions from the apps. Any app provider or third party could potentially be sharing data with other third and fourth parties through server-to-server transmissions, but this cannot be proven through a data flow analysis. In some cases, indications of such further data transmissions can be found in public documentation, such as developer documentation for implementation of tracking technologies. In order to fill in some of the gaps of the technical testing, we provide documentation from the third party vendors to exemplify how they may be using the data once they have received it.

[167] Mnemonic, "Review of communications from apps", https://www.forbrukerradet.no/out-of-control/

Due to the dynamic nature of digital services in general, and the complexity of the adtech industry in particular, the specific results obtained from the tests may be dependent on parameters such as the test window, the fact that Mnemonic's testers were located in Norway, and contextual data being accumulated by the adtech actors during the test itself. The results of our tests constitute a snapshot which is representative of the reality for potentially hundreds of millions of consumers who had installed and were using the apps during the timeframe when the tests were performed. However, the services may have changed after the tests were performed.

# 5 Information and choice in apps

Of the ten apps that were tested, the majority were found to transmit data to unexpected third parties. The data sharing was unexpected because the apps did not clearly inform the user about these third parties upon starting the apps for the first time, and/or when asking the user to consent to data processing.

Sometimes, some of the data sharing is described in the apps' privacy policy, but these documents are long and complex, and cannot realistically be expected to be read by the consumer.[168] Additionally, the majority of the apps did not provide any meaningful options or settings in the app to prevent or reduce the sharing of data with third parties.[169]

[168] The Norwegian Consumer Council has previously described the complexities of privacy policies and terms of service. https://www.forbrukerradet.no/appfail-en/

[169] Several of the privacy policies stated that users can opt out by using the Android system-level device settings. These settings are not easy to find, and many consumers probably do not know that the settings exist. See chapter 2.5 for more details on the system level settings.

| App | Google Play downloads | Clear information that they share data with non-service provider third parties in the consent flow? | Clear information in the consent flow that shared data is used for targeted ads? | In-app options to reduce data sharing with third parties? |
|---|---|---|---|---|
| Clue | 10,000,000+ | ✗ | ✗ | ✗ |
| Grindr | 10,000,000+ | ✗ | ✗ | ✗ |
| Happn | 50,000,000+ | ✓ | ✗ | ✗ |
| Muslim: Qibla Finder | 10,000,000+ | ✗ | ✗ | ✗ |
| My days | 5,000,000+ | ✗ | ✗ | ✗ |
| My Talking Tom 2 | 100,000,000+ | ✓* | ✓* | ✓* |
| OkCupid | 10,000,000+ | ✗ | ✗ | ✗ |
| Perfect365 | 50,000,000+ | ✓ | ✓ | ✗ |
| Tinder | 100,000,000+ | ✗ | ✗ | ✗ |
| Wave Keyboard | 10,000,000+ | ✗ | ✗ | ✗ |

*Only provided information and options when the user said they were born in 2002 or earlier.

In the following sections, we provide an overview of the apps that were tested, including the consent flows when starting the apps and/or registering for an account. We outline whether the apps give sufficient information, about whether they share data with third parties, and about whether this happens for purposes other than the functioning of the apps. According to the GDPR, such information should be provided upfront to the consumer in a clear and understandable manner, and not be hidden in legal documents.[170] If it is not possible to provide this information in a clear and understandable manner, these practices should not happen.

The below overview focuses on how each of the apps inform consumers of data sharing, and whether they provide choices to prevent this sharing. This provides the background for the next chapter, which provides information about a number of the third parties that Mnemonic observed receiving personal data from the apps during the technical tests.

## 5.1 Review of ten apps

When registering for or otherwise starting an app for the first time, it is common practice that the user is presented with a prompt asking for

[170] The conditions for consent and for information are described in the GDPR Art. 7 and Art. 13. This is elaborated upon in chapter 8.

confirmation that the user has read the privacy policy and terms and conditions. The user is asked to make a choice based on the information presented in these documents, which are usually many pages long. If the user does not accept this, the only option is usually to uninstall the app.

Under the General Data Protection Regulation, which applies for all processing of personal data regarding individuals in the EU and the EEA, there are several legal grounds for processing of personal data. One of these legal grounds is consent. As will be discussed in chapter 8, the processing of personal data may also be based on legal grounds such as legitimate interests and the fulfilment of a contract. For the purposes of this chapter, we will focus on how user consent is obtained.

The legal concept of consent under the GDPR requires that the user has received clear and easily understandable information about what they are consenting to. Consent also needs to be explicit, meaning that users must actively opt in, rather than having to jump through hoops to opt out of data sharing. Additionally, consent should be freely given, which means that processors/service providers cannot pressure users to agree to data sharing, for example by denying service to users who do not want their personal data being used for other purposes.

The ways that consent is presented and framed to the consumer are therefore crucial in order to provide a proper understanding of what one is agreeing to. There should be a clear choice, and service providers should provide granular choices in cases when data collection is not necessary for the functioning of the service. The provision of a service should never be conditional on accepting unnecessary collection of personal data, which means that the use of a dating app should not require the user to consent to their personal data being used for profiling and behavioural advertising, for example. Finally, the choices and consent prompt should be unambiguous, to ensure that there is no misunderstandings about what the consumer is consenting to.[171]

The extent of data sharing described in chapter 6 calls into question whether it is practically possible for the apps to ask for consent in any meaningful way. It is often incomprehensible for the consumer how personal data is shared, how it may be used, and what the short or long term consequences of these practices may be. Furthermore, personal data may be transmitted to numerous commercial third parties that may have their own purposes of processing, and

[171] For a more detailed analysis of how consent may be undermined by using manipulative and skewed design, wording, and framing, see the Norwegian Consumer Council work on dark patterns. https://www.forbrukerradet.no/dark-patterns/

may share it with further companies. In such cases, it seems impossible to present information to the consumer in an understandable manner. The solution to this should not be to rely on other legal bases than consent, but rather to limit the data processing and sharing to what is necessary for providing the service.

### 5.1.1 Perfect365: One-Tap Makeover

Perfect365 is a popular app that lets users add filters to their portraits, creating the visual effect of having applied different types of makeup. The app has been installed more than 50 000 000 times on Google Play. The Perfect365 company is a subsidiary of the major US-based imaging and facial recognition company ArcSoft.[172]

In October 2019, Perfect365 was found transmitting location data to the data company Factual Inc., which in turn was sharing this information with political campaigns in the US.[173]

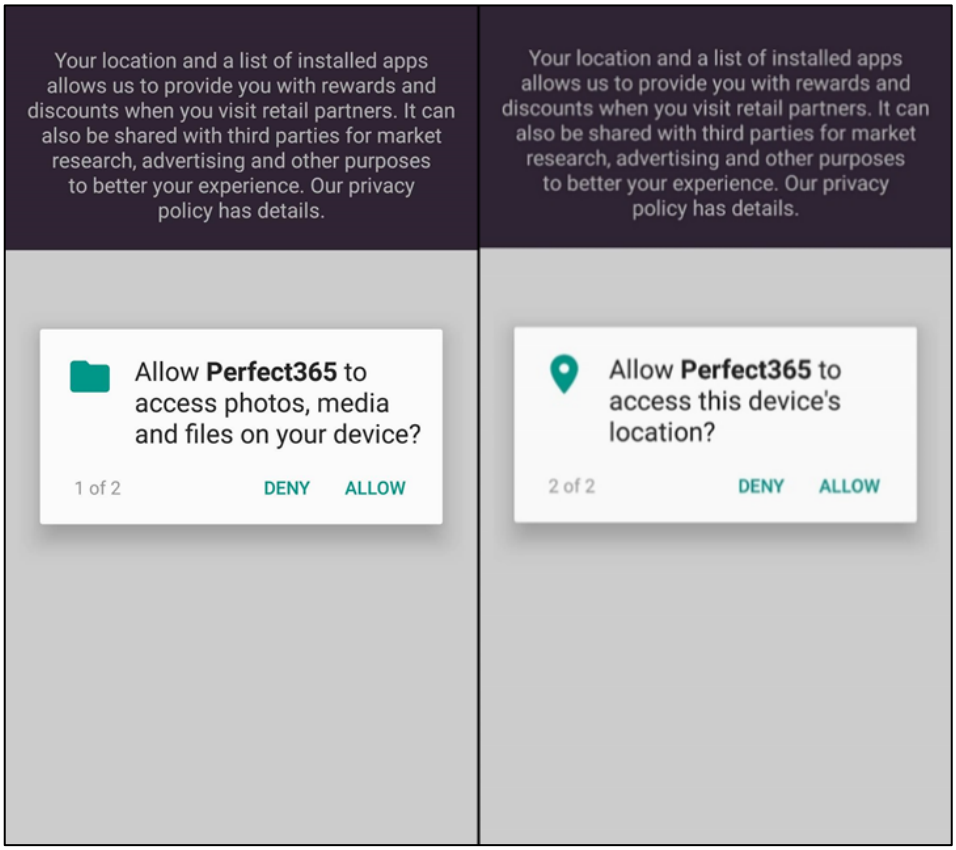
Upon first starting Perfect365, the user is informed that location data is shared with unspecified third parties.

> *"Your location and a list of installed apps allows us to provide you with rewards and discounts when you visit retail partners. It can also be shared with third parties for market research, advertising and other purposes to better your experience. Our privacy policy has details."*

This is accompanied by a permission request asking for access to the device's location.

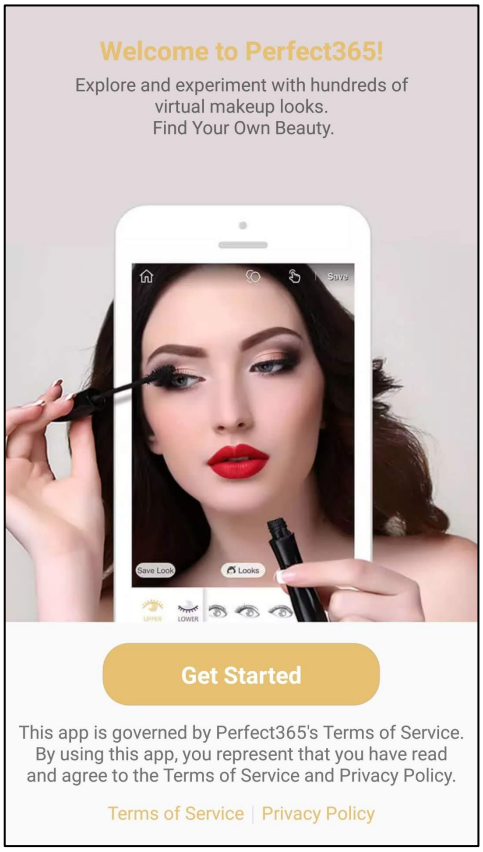
[172] ArcSoft is also working with a number of Chinese companies, and went public in China in 2019. https://www.scmp.com/tech/gear/article/3022041/chinese-billionaire-built-ai-helps-samsung-huawei-phones-take-better

[173] "Political Campaigns Know Where You've Been. They're Tracking Your Phone", Sam Schechner, Emily Glazer and Patience Haggin https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889




*10 Perfect365 permissions prompt.*

The app goes on to state that *"By using this app, you represent that you have read and agree to the Terms of Service and Privacy Policy"*. However, there are no consent prompts to affirm or decline this, just a button to "Get Started". The app does not contain any privacy settings or other in-app ways to stop or limit the sharing of data with third parties.




*11 Perfect365 opening screen.*

The privacy policy of Perfect365 names a number of consumer data aggregators and data brokers, including Unacast,[174] OneAudience[175] and Tutela,[176] although out of these, only Unacast was observed receiving data directly from Perfect365 during Mnemonic's tests.[177]

The privacy policy elaborates upon how Perfect365 may collect and share data with third parties, but emphasizes that this only happens after the user has given their consent.

> *"We may collect device and usage information such as: precise geolocation data pertaining to User's devices (only upon your consent)".*

[174] Unacast privacy policy (last updated February 11, 2019) https://www.unacast.com/privacy#policy
[175] "Create better audiences", OneAudience [archived May 25, 2019] https://web.archive.org/web/20190525211043/http://www.oneaudience.com/mobile-audience-creation/
[176] "Methodology", Tutela [accessed December 11, 2019] https://www.tutela.com/methodology
[177] The references to these companies have been removed, but is archived here. [archived June 8, 2019] https://web.archive.org/web/20190608081442/https://www.perfect365.com/about/privacy-policy/

This data collection also happens when the app is not in use.

> *"We may collect this information when the App runs in the background on your device."* [178]

The Perfect365 privacy policy goes on to state that the app may share "non-personally identifiable information", geolocation and device data with unaffiliated third parties, which may be combined with other identifiers for advertising purposes.

> *"We may share or disclose non-personally identifiable information, aggregated, usage information, geolocation Information or device-level information (such as anonymous usage data, platform types, number of clicks, location data etc.) with unaffiliated partners and third parties (e.g. advertisers, advertising networks and platforms, agencies, other marketers, retailers) that wish to market products or services to you. In particular, we may collect and share precise location information including the presence of connected devices via Bluetooth through methods such as partner mobile "SDKs". This information may be used by itself, aggregated, or combined with mobile identifiers (such as IDFAs and Android IDs), and shared with other parties, for purposes related to advertising, attribution (e.g., measuring ad performance), analytics, and research."*[179]

As the core functionality of Perfect365 is to add make-up filters to pictures, it is not clear why it requires the collection of precise GPS coordinates in order to function. In any case, Perfect365 seems to regard the user having enabled location in the system level settings as giving consent for the app collecting GPS coordinates.

> *"We do not collect geolocation information from you unless we obtain your explicit consent through the device's settings menu."*[180]

Under the GDPR, GPS coordinates that are collected over time constitutes personal data. Although Perfect365 provides some information about sharing personal data for marketing purposes, it does not provide users with any real choices to prevent this. Furthermore, having location enabled in the device settings does not constitute meaningful consent. Consequently, Perfect365 appears to lack the valid consent it claims to have to share personal data for advertising purposes.

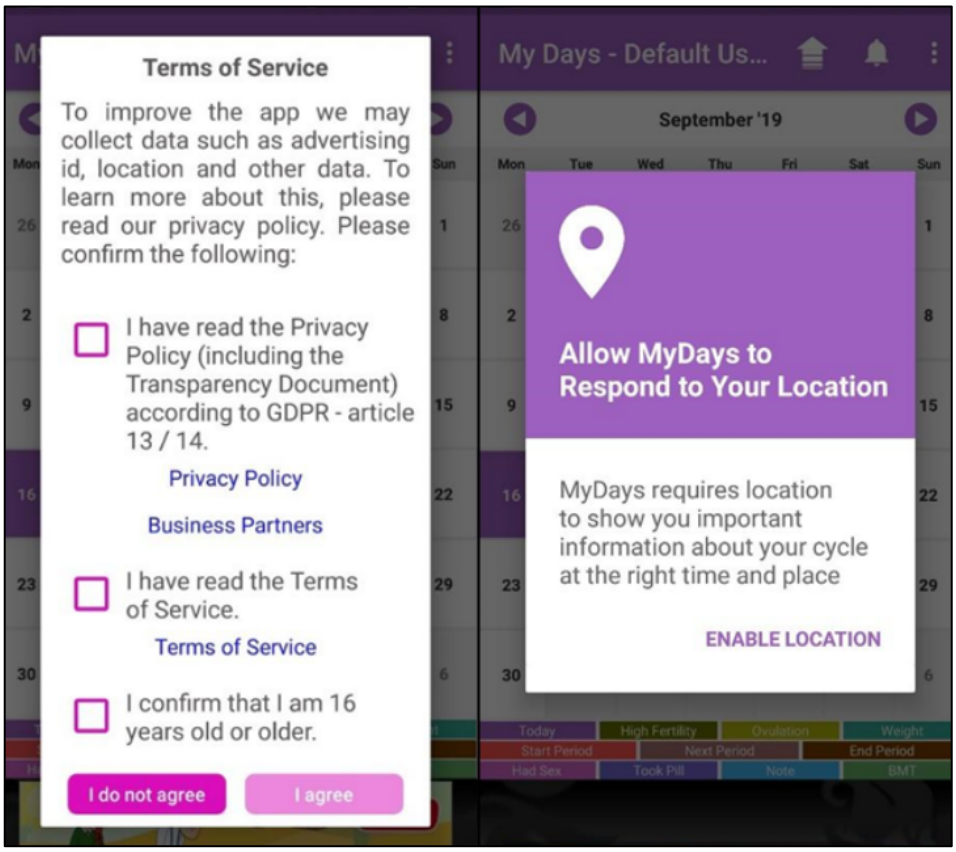
---

[178] Perfect365 Privacy Policy (Last updated April 25 2019)
https://www.perfect365.com/about/privacy-policy/
[179] Ibid.
[180] Ibid.

### 5.1.2 MyDays - Ovulation Calendar & Period Tracker

MyDays is a period tracker and fertility app run by the German company Christian Albert Mueller. The app lets users track a large variety of information related to fertility and lifestyle, including sexual activity, dieting and moods. The app has more than 5 000 000 installs through Google Play.

Before using the app, users have to tick off a box stating that they *"have read the Privacy Policy (including the Transparency Document) according to GDPR - article 13/14"*. The popup notification informs that the app may collect advertising ID, location, and *"other data"* in order to *"improve the app"*. Upon confirming to have read the privacy policy and terms of service, the user is asked to enable location tracking "to show you important information about your cycle at the right time and place". The app provides no settings related to privacy or advertising.




*12 MyDays registration screen.*

According to its privacy policy, MyDays collects and shares location data for advertising purposes. MyDays is relying on the GDPR legal basis of legitimate interest to process and share location data with advertisers.

> *When you use our platforms, applications and services, your location data is processed to serve you with content, which may also include location-based advertising. We may share location and positioning data and information with our partner companies. Legal basis for processing is Art. 6(1)(f) GDPR.*[181]

The privacy policy lists a number of third parties that may receive personal data from MyDays for purposes such as targeted advertising and behavioural profiling. This includes Google AdMob, Vungle, Neura, Placed, Cuebiq, Tappx, Google AdWords, and Facebook. Users of MyDays are encouraged to read the privacy policies of these third parties.

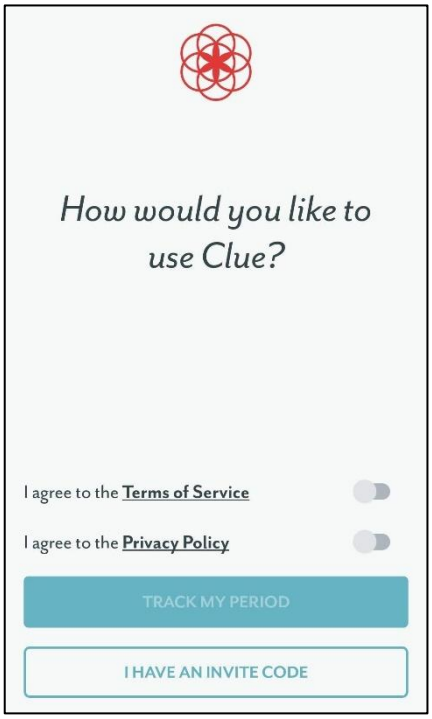
As described in chapter 8, the publisher's legitimate interest to share personal data for advertising purposes is unlikely to weigh heavier than the users' fundamental rights and freedoms, so it is questionable that MyDays has a valid legitimate interest for sharing location data for advertising purposes. Although MyDays asks for consent to its privacy policy upon registration, it bundles the data sharing with consent to using the app. This is also not compliant with the conditions for consent as set forth in the GDPR.

### 5.1.3 Period Tracker Clue - Ovulation and Cycle Calendar

The German period tracker and fertility app Clue has more than 10 million installs on Google Play. Users can input a lot of data related to fertility, health and lifestyle into the app. The app is provided by the Berlin-based company BioWink.[182]

Before installing the app, the user has to consent to the privacy policy and terms & conditions, but there is no clear information in the app about what this entails, which means that the user would have to read the legal documents to understand what they are consenting to. The app does not provide any in-app settings related to privacy or advertising.

[181] MyDays privacy policy (last updated November 26, 2019) https://mydays.club/info/privacy-policy/
[182] "Legal Note", Clue https://helloclue.com/imprint




*13 Clue registration screen.*

In its privacy policy, Clue explains that it may collect usage data along with a unique identifier to serve targeted advertising, and seems to regard using the app as a valid consent to this collection.

> *"By using our app and our website you consent that Clue may use cookies and third-party services, and collect your usage data under a unique identifier, for the purposes of tracking, analysis, and improvement of our website and app, as well as advertising purposes such as retargeting."*[183]

The privacy policy includes a list of third parties that may receive personal data from Clue for analytics and advertising purposes. This list includes Google Analytics, Braze, Amplitude, Apptimize, Adjust, and Facebook Audiences. If the user wants to opt out, they have to either send Clue an email, or contact the third parties directly.

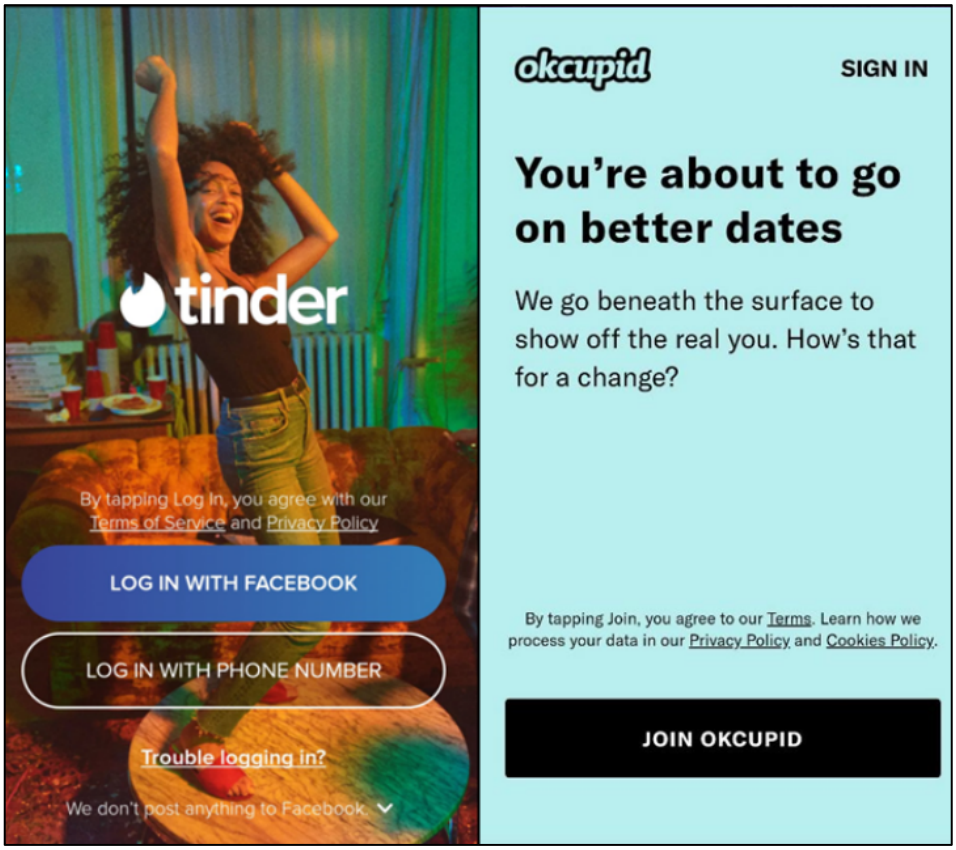
Although Clue asks for consent to the privacy policy upon registration, it does not provide any choices related to data collection and sharing. Under the GDPR, the use of a service cannot be made conditional on accepting tracking and sharing of personal data for further purposes, including for advertising. Consequently, any personal data Clue shares with third parties for advertising purposes may be in breach of the GDPR.

[183] Clue privacy policy (last updated March 8, 2019) https://helloclue.com/privacy

### 5.1.4 Tinder and OkCupid

Tinder and OkCupid are two very popular dating apps, with more than 100 million (Tinder) and 10 million (OkCupid) installs through Google Play. Both services are run by the Match Group, which is based in Los Angeles.

When starting the apps, both Tinder and OkCupid seem to assume implied consent when the user taps “Log In” or “Join”. Neither of the apps provide any in-app settings related to privacy or advertising.




*14 Registration screens for Tinder (left) and OkCupid (right).*

According to their privacy policies, which are very similar in content and form, in addition to sharing data with third parties for advertising purposes both Tinder and OkCupid reserve the right to share data with other Match Group companies:

> *“We also share some users' information with service providers and partners who assist us in operating the services, with other Match Group companies and, in some cases, legal authorities.”*[184]

[184] OkCupid privacy policy (last updated May 25, 2018) http://www.okcupid.com/legal/privacy

This means that data collected through Tinder may be shared with OkCupid and vice versa. The apps may also share data with Match.com, PlentyOfFish, and other Match Group brands, which includes at least 45 dating-related businesses.[185] This means that, according to the privacy policy, a Tinder-user could have their personal data used by PlentyOfFish, even if they never used that service.

The privacy policies do not specify which third parties may receive personal data from the apps for advertising or analytics purposes.

According to the privacy policies, both Tinder and OkCupid rely on a mix of legitimate interests and consent as the legal basis to process personal data that is not strictly necessary for providing the service. In general, the companies seem to rely on legitimate interests for advertising purposes, or "suggest offers we think might interest you".

In cases where the companies ask for consent to process personal data for "certain specific reasons", this consent may be withdrawn by contacting the companies.

> *"To process your information as described above, we rely on the following legal bases: […]*
>
> *Legitimate interests: We may use your information where we have legitimate interests to do so. For instance, we analyze users' behavior on our services to continuously improve our offerings, we suggest offers we think might interest you, and we process information for administrative, fraud detection and other legal purposes.*
>
> *Consent: From time to time, we may ask for your consent to use your information for certain specific reasons. You may withdraw your consent at any time by contacting us at the address provided at the end of this Privacy Policy."*[186]

Both Tinder and OkCupid fail to fulfil the GDPR conditions for informed and explicit consent, as they bundle all purposes for data processing in their privacy policies. The sharing of personal data between Match group subsidiaries is also problematic, and fails to respect the data protection principle of purpose limitation. Furthermore, the reliance of legitimate interests to use personal data

[185] "Nearly all of the big dating apps are now owned by the same company", Kaitlyn Tiffany https://www.vox.com/the-goods/2019/2/11/18220425/hinge-explained-match-group-tinder-dating-apps

[186] Tinder privacy policy (last updated May 25, 2018) https://www.gotinder.com/privacy?locale=en

to serve targeted advertising is unlikely to outweigh the fundamental rights and freedoms of the data subject, as discussed in chapter 8.

### 5.1.5 Grindr

According to its website, Grindr is "the world's largest social networking app for gay, bi, trans, and queer people". It has been installed more than 10 million times from Google Play. Although owned by the Chinese company Kunlun, Grindr is headquartered in the US. The service is location-based, showing users possible matches in the vicinity. There is both a free and a paid version of Grindr, but both types of account use the same app. For the purposes of this report, we used a free account.

In 2018, Grindr was at the centre of controversy when it was discovered to share users' HIV-status with the third party analytics companies Apptimize and Localytics.[187] This practice was ended by Grindr soon after, in the wake of a Norwegian Consumer Council complaint to the Norwegian Data Protection Authority for breaches of the GDPR.[188]

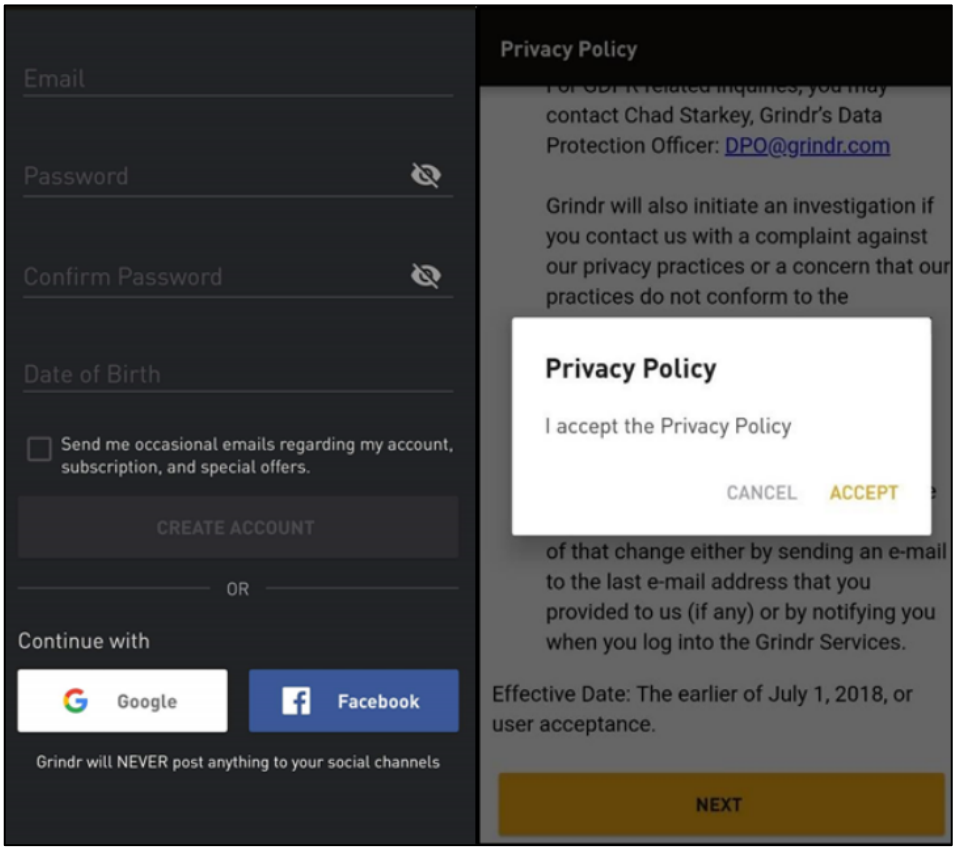
In 2019, security researchers exposed how Grindr could be used by rogue actors to pinpoint the location of users, demonstrating how location data can be abused.[189]

When first starting the app, Grindr users have to accept the privacy policy and terms and conditions in their entirety. There is no separate in-app information about how personal data may be used or shared.

[187] "Grindr Is Letting Other Companies See User HIV Status And Location Data", Azeen Ghorayshi https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy

[188] "Filing complaint against Grindr's sharing users' HIV-status and sexual preferences", Forbrukerrådet https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences/

[189] "Gay dating apps still leaking location data", Chris Fox https://www.bbc.com/news/technology-49265245




*15 Grindr registration screen.*

Grindr's privacy policy states that it will share certain data with advertisement third parties, but that these third parties are prohibited from tracking HIV-status and sexual preferences.

> *"Our advertisers also use their own cookies or other tracking technology which may collect information about you within the Grindr Services. We do not control use of these tracking technologies. We prohibit them from tracking or monitoring health information (e.g., HIV status) or certain sexual group identification (e.g., Tribe)."*[190]

Grindr provides settings related to what information other users can see about you, but does not have any in-app settings for controlling data sharing with third parties or the use of targeted advertising.

According to its privacy policy, Grindr relies on a mix of legal bases to process personal data, although it is not clear when each basis applies.

> *"By agreeing to our privacy policy, you consent to the collection of the information indicated below. In addition to consent, the information is*

[190] Grindr privacy policy (last updated December 3, 2018) https://www.grindr.com/privacy-policy/

> *collected to perform a contract, to comply with obligations, or for the legitimate interests of Grindr or a third party as described below."*[191]

The privacy policy also states that Grindr may share certain user and device data with third parties, including the Advertising ID, "a portion of your Profile Information" and "distance information". It goes on to say that any data processed by advertising partners is regulated by these third parties' own privacy policies.

> *"We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of your demographic information with our advertising partners. These third parties may also collect information directly from you as described in this Privacy Policy through technology such as cookies. The privacy policy of these third party companies applies to their collection, use and disclosure of your information."*

However, Grindr's privacy policy only names one such advertising partner, Twitter's MoPub, so it is not clear how the user would be able to read the privacy policy of any other potential advertising partners. This is explored and discussed in detail in chapter 7.

The vagueness of which legal basis Grindr is using for processing personal data is likely in breach of the GDPR, and makes it impossible for the user to know what they are consenting to. By stating that it does "not control the use of these tracking technologies", and by asking users to read the privacy policies of any third party companies that may receive personal data, Grindr is also attempting to shift accountability for the advertising technologies that it is using away from itself.

This is not compliant with the GDPR, as Grindr is the controller of any personal data collected and shared through its services. As will be discussed in chapter 7, Grindr only lists Twitter's MoPub as an advertising partner, and encourages users to read the privacy policies of MoPub's own partners to understand how data is used. MoPub lists more than 160 partners, which clearly makes it impossible for users to give an informed consent to how each of these partners may use personal data.

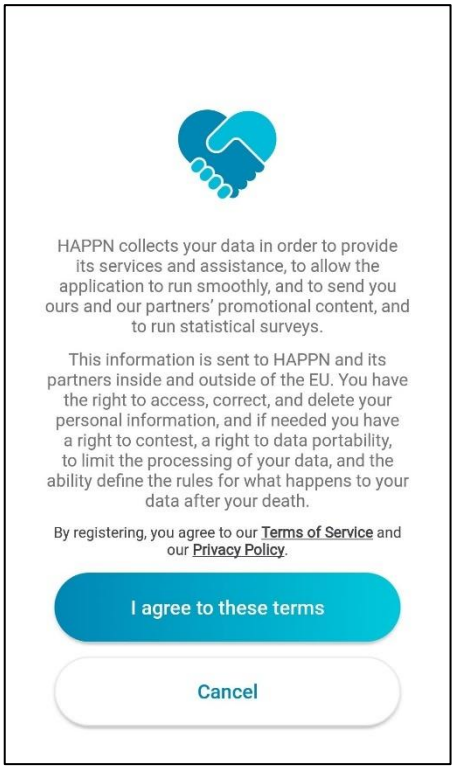
[191] Ibid.

### 5.1.6 Happn

The dating app Happn has been downloaded more than 50 000 000 times from Google Play. The Paris-based app provides dating based on geolocation, matching users who have crossed paths.

In 2016, a Norwegian Consumer Council report revealed that Happn was sharing personal data with several third parties, in breach of its own privacy policy.[192]

Once installed, Happn informs the user that it collects data "to send you ours and our partners' promotional content". It is not made clear whether this data is shared with other parties to provide targeted advertising, although it states that information is sent to "partners inside and outside of the EU".




*16 Happn registration screen.*

In its privacy policy, it is specified that Happn may share data for advertising purposes outside of the Happn app:

[192] "Happn shares user data in violation of its own terms", Forbrukerrådet https://www.forbrukerradet.no/side/happn-shares-user-data-in-violation-of-its-own-terms/

> *"Conducting marketing operations and advertising outside of the application: we conduct marketing operations and advertising outside of the HAPPN application outside of third-party sites, social networks and third-party applications in order to find profiles similar to yours and who could be interested by our Services. To find similar profiles, we use and transmit with an encrypted code to websites, applications and social networks your first and last names, email address, telephone number, postcode, country and mobile advertisement ID. The existence of your profile will never be disclosed to these similar profiles. These similar profiles (non-Members) will see HAPPN advertisements on websites, social networks and third-party applications."*[193]

Happn claims to have a legitimate interest for doing this, and users who want to opt out have to contact the company:

> *"You may also object to sharing data with third-party websites, social networks and third-party applications, by contacting us. "*

The privacy policy also states that it may employ "authenticated and reliable service providers and parties" for "marketing and advertising to address relevant offers, messages and content to HAPPN Members and HAPPN non-Members".[194] The names of these partners are not mentioned.

In the app, Happn provides privacy controls to protect users' privacy from other users, but does not give any control over how data is used or shared by Happn, or whether data is used for targeted advertising.

As we will discuss in chapter 8, it is questionable whether legitimate interests can be used to share personal data with third parties to serve targeted advertising. As Happn does not state what third parties it may share data with, it is also impossible for the user to give an informed consent. Consequently, it is questionable whether Happn has a valid legal basis for sharing personal data with third parties.

### 5.1.7 My Talking Tom 2

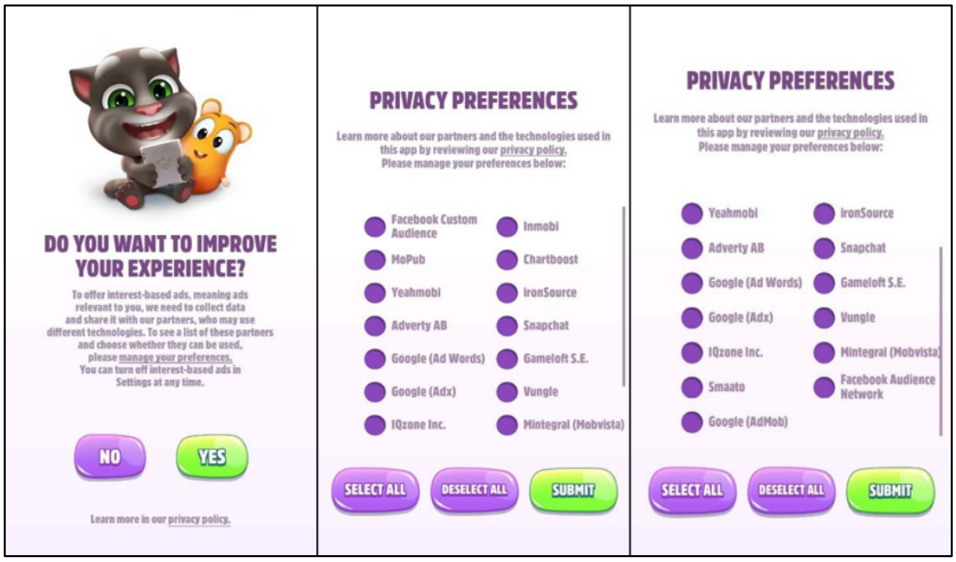
My Talking Tom 2 is a children's app with more than 100 000 000 downloads on Google Play. The game is developed by Outfit7, a subsidiary of the Chinese

[193] Happn privacy policy (last updated July 29, 2019) https://www.happn.com/en/privacy/
[194] Ibid.

chemical company Zhejiang Jinke.[195] In addition to publishing the Talking Tom series of games, Outfit7 also runs an advertising network that it claims gives access to 350 million active users in 230 countries and territories.[196]

My Talking Tom 2 does not have user accounts, and therefore there is no registration process. When starting the app, the user has to choose their age, through a prompt that also links to the app's privacy policy. If the user states that they were born after 2002, there are no further prompts. The testing for this report was done when selecting a birth year after 2002, as this was the standard setting, and it was deemed reasonable that typical users of the app would be small children.

If the user states that they were born in 2003, a new popup appears asking the user to consent to data collection "to improve your experience", and to sharing data with "our partners" to serve targeted ads. The user can click "manage your preferences" to see a list of partners, and select which ones My Talking Tom 2 is allowed to share data with. The list includes major platforms such as Facebook, Google, Snapchat, and numerous other adtech companies including MoPub, Vungle and Smaato. When using the app, in-app advertising pops up periodically regardless of the age of the user.




*17 My Talking Tom 2 registration screen.*

[195] "Why Did a Chinese Peroxide Company Pay $1 Billion for a Talking Cat?", Adam Satariano https://www.bloomberg.com/news/features/2017-05-17/why-did-a-chinese-peroxide-company-pay-1-billion-for-a-talking-cat

[196] "Advertise a big brand. Generate bigger smiles", Outfit7 [accessed December 11, 2019] https://outfit7.com/advertising/

In the Outfit7 privacy policy, it is stated that My Talking Tom 2 may share personal data for targeted advertising.

> *"We share information that can be used to personally identify your device (e.g. persistent identifiers such as IDFA, IDFV, advertising ID and IP address) for the purposes of developing and delivering our services, displaying advertisements, conducting analysis and research and for measuring our and our Partners's advertising campaign performance."*[197]

The privacy policy also includes a list of third parties that My Talking Tom 2 may share personal data with if the user consents. The user is asked to visit each of these third parties' own privacy policies "to review their data processing practices, including the technologies they use for the purposes of interest-based advertising".

The privacy policy goes on to state that, if the user did not consent to the sharing of personal data, Outfit7 uses legitimate interests as its legal basis for processing data for contextual advertising rather than behavioural advertising.

> *"We offer our Apps for free or at low cost and in order to do that we need to share information we collect from you with our third party advertising partners that assist us in delivering advertisements to you. When you use our Apps we rely on our legitimate interest to show contextual advertisements to you. Before sharing any information with our advertising partners for the purposes of interest-based advertising, we will always ask for your consent."*[198]

Although there is reason to question the use of contextual advertising in an app aimed at small children, My Talking Tom 2 differs from the rest of the tested apps by asking users over 16 years old to give a specific consent for each third party that may receive personal data. Since the developers of My Talking Tom 2 also runs an advertising network, one may question how any data collected by Outfit7 itself is used, but this is outside the scope of this report.

### 5.1.8 Muslim - Qibla Finder, Prayer Times, Quran, Azan

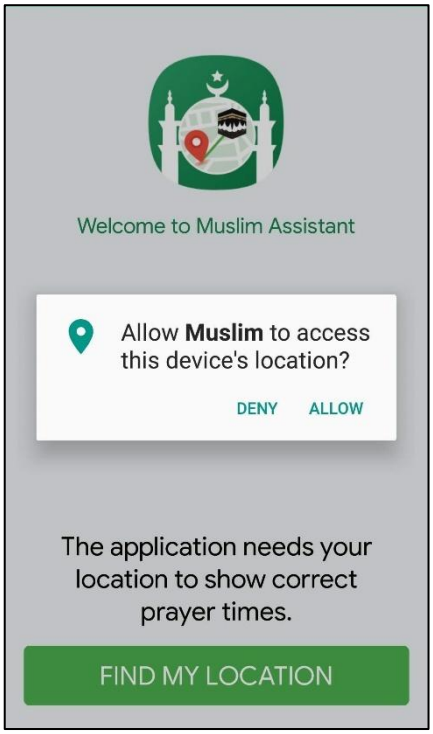
The app Muslim – Qibla Finder is a tool for Muslims, which can be used to receive reminders of events tied to religious matters. The app has been downloaded from Google Play more than 10 000 000 times, and is published by the Turkish company Muslim Assistant.

---

[197] Outfit7 EEA privacy policy for apps (last updated September 2019) https://outfit7.com/privacy/eea/en/

[198] Ibid.

Upon opening the app, Muslim – Qibla Finder asks for access to the device location, but does not ask for consent or otherwise display or reference any terms or privacy policy.




*18 Muslim: Qibla Finder permissions screen.*

The privacy policy refers to Turkish law, and does not contain any clear statements or information about data sharing, other than an affirmation that third parties show advertising in the app. These third parties are not named.

Although it is referred to as a privacy policy, the legal document is mainly focused on typical terms of service such as user infringements. The user has to pledge that they will only send "non-confidential" data to the service-provider, although it is otherwise unclear how any collected data may be used.

> *"You agree that all information and/or particulars sent or submitted by you through the App or Service are non-confidential and non-proprietary unless otherwise expressly indicated by you and may be collected, used and disclosed by Muslim Assistant in accordance with Muslim Assistant's Terms, as may be updated and/or amended by Muslim Assistant from time to time."*[199]

[199] Muslim Assistant privacy policy (not stated when last updated, accessed 08.10.2019) https://www.muslimassistant.com/privacy-terms.html

As Muslim - Qibla Finder is clearly made available to users within the EU and EEA, it should comply with the GDPR. The lack of any references to European law in the privacy policy means that any processing of personal data on EU and EEA users is likely in violation of the GDPR.

### 5.1.9 Wave Keyboard Background - Animations, Emojis, GIF

Wave Keyboard is a personalized keyboard app from the Romanian company Wave Design Studio. The app has been downloaded from Google Play more than 10 000 000 times.

Wave Keyboard does not provide any terms or privacy policy when opening the app, and does not ask for consent for data processing. Its privacy policy states that Wave Keyboard shares personal data with third parties to serve targeted advertising. However, it is not mentioned who these third parties may be.

> *"Notwithstanding anything else in this policy, we may work with partners who use mobile SDKs, including the OneSignal Messaging SDK, to passively collect information (collectively, "SDK Information"), which generally helps us deliver personalized notifications. This data may also be used to identify you in a unique manner across other devices or browsers for the purposes of customizing ads or content. Depending on the permissions granted to this application, this information may include personally identifiable information (PII) including your e-mail address. This information may also include precise location (i.e. GPS-level data) or WiFi information, apps you have installed and enabled, and your mobile identifier (e.g., Android Advertising ID)."*[200]

The app does not provide any in-app settings related to data collection or sharing, but users can pay to get rid of the ads that periodically pop up in the app.

In its privacy policy, Wave Keyboard does not specify any legal grounds for processing personal data, but seems to regard using the app as consent.

> *"By using the Application, you are consenting to our processing of your information as set forth in this Privacy Policy now and as amended by us. "Processing," means using cookies on a computer/hand held device or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information, all of which activities will take place in the European Union and United States."*[201]

[200] Wave Keyboard privacy policy (not stated when last updated, accessed October 10, 2019) http://www.wavekeyboard.com/privacy-policy/
[201] Ibid.

By not providing any choices or information, or even presenting a privacy policy at start-up, Wave Keyboard does not have a valid legal consent to process personal data. Under the GDPR, just the use of a service cannot be considered an explicit expression of consent. Thus, any personal data collected by the app and/or shared with third parties seems to lack a legal basis for processing.

# 6 Analysis of data flows and third parties receiving personal data

In this chapter we describe the third parties that were observed receiving personal data during Mnemonic's technical tests of the ten apps described in chapter 5. In addition to showing what personal data each company were observed receiving, we provide a short description of each company, and how they describe themselves on their websites. This is accompanied by a short review of the companies' privacy policies, focusing on their legal compliance and their legal basis for processing personal data. We will also present brief evaluations of each company's practices, using the General Data Protection Regulation as a benchmark. We go into further detail regarding the legal compliance and implications of these practices in chapter 8.

Altogether, Mnemonic observed data transmissions from the apps to 216 different domains belonging to a large number of companies. Based on their analysis of the apps and data transmissions, they have identified at least 135 companies related to advertising. One app, Perfect365, was observed communicating with at least 72 different such companies.[202]

[202] Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/


Some of these data transmissions may be necessary for the apps to function. However, there were many instances of personal data being sent to adtech companies that appear to use this information for purposes that consumers cannot reasonably expect, such as tracking and profiling.

## 6.1 Location data brokers

The technical testing showed location data being transmitted to several third party companies that can be classified as location data brokers. These companies use detailed geolocation derived from GPS coordinates and other sources to create profiles, audience segments, or aggregated data sets, which they can sell or otherwise share with or give access to other companies. They may collect very detailed movement histories of individual consumers, including data on hospital stays, visits to mental health professionals, and pub visits, often without the consumer being aware that this is happening.[203]

Information about where and how we move can reveal a lot about us. Most of us are easily identified just from where we live and where we go to work. Other movement data can reveal our religious affinity ('visits a synagogue weekly'),

[203] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

sexuality ('frequents gay bars') or political views ('attends climate strikes').[204] Studies have demonstrated that just four approximate location data points is sufficient to identify individuals in 95% of cases.[205]

In addition to getting the consumer's precise geolocation through the GPS receiver of a device, third parties can also track location through the use of Wi-Fi access point information, Bluetooth, and cell tower data.[206] This means that, even if a consumer explicitly turns off the GPS function on their smartphone, their location can be accurately triangulated by third parties through measuring the phone signal and distance to Wi-Fi access points and cell towers.

Through their testing, Mnemonic observed GPS coordinates data being transmitted to at least 23 third party companies, some of which are location data brokers.[207] Additionally, Wi-Fi access point data, Bluetooth data, and cell tower data was observed being transmitted to a number of third party vendors. In particular, the apps Perfect365 and MyDays were frequently observed transmitting location data to data brokers, even though neither of these apps seem to rely on location data for any of their core functionality.

### 6.1.1 Fysical

Fysical is a San Francisco-based location data broker that boasts of having the "most accurate dataset of place visitors on Earth".[208] Its website claims that Fysical maintains a "human movement SDK that is installed across hundreds of mobile applications". The data collected through this SDK is used to maintain a database that includes "human movement data on 25 % of the population".

---

[204] For a detailed overview of how the location data broker industry tracks and processes massive amounts of personal data, see "Twelve Million Phones, One Dataset, Zero Privacy", Stuart A. Thompson and Charlie Warzel https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

[205] "Unique in the Crowd: The privacy bounds of human mobility", Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel https://www.nature.com/articles/srep01376

[206] Geolocation can be triangulated by measuring a phone's signal strength from several cell towers. This technique was used by bounty hunters in the US, who had access to data from telecom providers. See "Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years", Joseph Cox https://www.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years

[207] Mnemonic, "Review of communications from apps", chapter 2.3.2 Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/

[208] Fysical [accessed December 11, 2019] https://fysical.com/

During the technical testing, Mnemonic observed Fysical continuously receiving GPS coordinates and the Advertising ID from the app Perfect365. Fysical was observed receiving the GPS coordinates up to several times per minute.[209]

Through the Fysical website, visitors are invited to contact the company to *"BUY or SELL DATA"*. Its collects data through an SDK that is integrated in hundreds of apps.

> *"We maintain a human movement SDK that is installed across hundreds of mobile applications. This generates the highest accuracy ground-truth location data"*[210]

Fysical used to be known as Beaconsinspace,[211] offering two core services; generating location data and monetizing it.

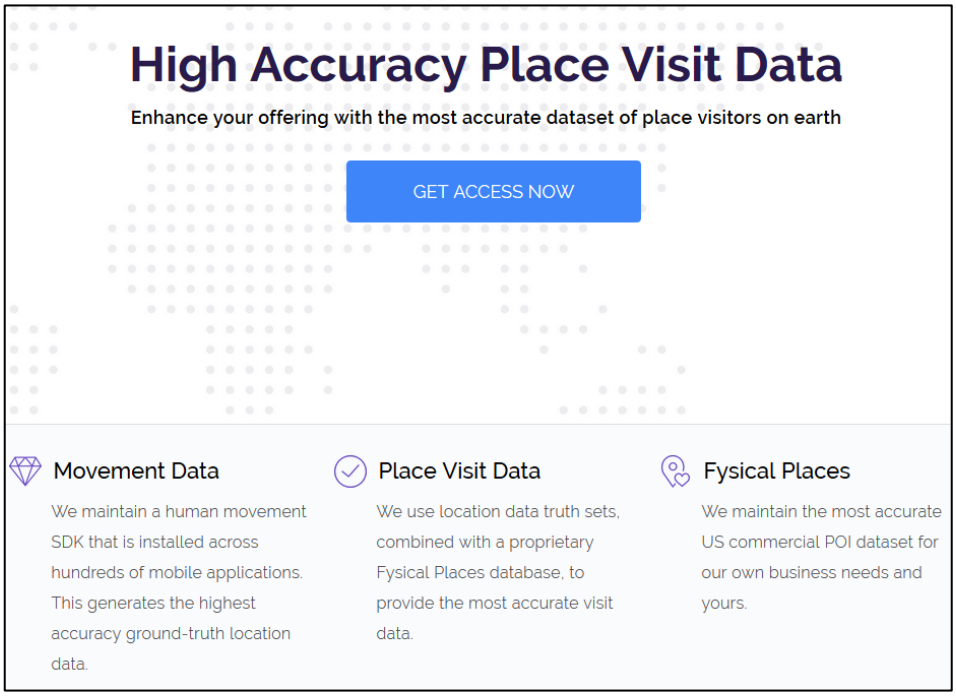
> *"Fysical Labs makes it easy for you to add a revenue stream from your mobile users without affecting the user experience [...] We have two core services that are organized around generating location data and making you money"*[212]

[209] Mnemonic, "Review of communications from apps", chapter 3.3.2 https://www.forbrukerradet.no/out-of-control/

[210] Fysical [accessed December 11, 2019] https://fysical.com/.

[211] Beaconsinspace [archived February 14, 2019] https://web.archive.org/web/20190214192040/https://beaconsinspace.com/

[212] "Monetize with the BeaconsInSpace SDK by Fysical Labs", Fysical [archived September 9, 2019] https://web.archive.org/web/20190909105115/https://mobile-sdk-docs.fysical.com/




*19 Source: https://fysical.com/ [accessed December 11, 2019]*

In its privacy policy, Fysical describes what kind of data it may receive, which includes Advertising ID, other unique identifiers, location data from Bluetooth and GPS, and a lot of device data including the IP address.

> *"Relying on this app-specific, or device-specific advertising ID (IDFA, ADID), we collect:*
>
> *An app-specific identifier or device specific identifier that is used to identify a unique app user or device user which can be tied to a specific mobile device or Customer app;*
>
> *All location meta data when a user is within range of a beacon, or when a periodic location coordinate (ie GPS) is taken, including location data (latitude/longitude coordinates including, street address, establishment name, touch point);*
>
> *Times of end user location detection;*
>
> *Device information, such as the device type, model and operating system version, device language, mobile carrier, device name, device processes, device battery state, device speed, and current IP address."*[213]

Amongst other things, Fysical uses this data for "facilitating or enabling the delivery of content, ads, offers or other marketing solutions that may be of interest to end users". It claims to delete or de-identify data 7 years after collection.

[213] Fysical privacy policy (last updated September 27, 2019) https://fysical.com/privacypolicy/enduser/index.html

The privacy policy goes on to claim that Fysical is an “opt-in only service”, and only receives data based on consent. According to Fysical, the app provider is responsible for collecting consent before transmitting personal data to Fysical.

> *“As part of our Terms of Service, Fysical requires that its Customers: (i) inform end users about our purposes for the collection of their data; (ii) receive consent from end users prior to the commencement of the processing of the End User Data; and (iii) notify end users about how their consent can be revoked.”*

However, the privacy policy also states that if users do not want to be identified by Fysical, they can either delete the app, or use the device-level settings to opt out.

> *“If end users do not want Fysical to identify their mobile device, they can: (a) delete the Customer app or adjust the in-app settings of the Customer app if the app makes that option available (this will limit data collection from this app alone); or (b) opt-out of sharing your mobile advertiser ID by limiting ad tracking on the device. For iOS, navigate to your Settings > Select Privacy > Select Advertising > Enable the "Limit Ad Tracking" setting. For Android, open your Google Settings app > Ads > Enable "Opt out of interest-based advertising".”*

In addition to processing data on behalf of Perfect365, Fysical appears to be using location data for its own commercial purposes. If Fysical uses this personal data for its own purposes, it is a controller. This means that Fysical is responsible for making sure that the data it is processing was collected in a legally compliant manner.

As noted in chapter 5, Perfect365 does not present the user with a sufficient opt in consent choice. Furthermore, asking users to use the system-level settings to opt out of data sharing is clearly not an opt-in choice. Consequently, Fysical do not appear to have a valid legal basis for processing the personal data that it was observed receiving.

### 6.1.2 Safegraph

Safegraph is a San Francisco-based location data broker specializing in insights about “foot traffic”, which can be used to show companies where consumers move and congregate. Based on data gathered from different sources, it provides data about “Places” by mapping different segments of points of interests to GPS coordinates. The company also provides information on foot

traffic across these points of interests, based on analysing data from different sources, including mobile apps, which it calls "Places patterns".[214]

Through the technical testing, Safegraph was observed receiving GPS-coordinates, Android Advertising ID, and Wi-Fi access point data (SSID and BSSID) from Perfect365.[215] The latter can be used to triangulate location even in places with low GPS reception, and is normally used to pinpoint locations inside buildings.

According to its public documentation, Safegraph uses GPS coordinates to recognize which type of place a consumer visits, including places such as "Religious Organizations", "Child Day Care Services", "Beer, Wine, and Liquor Stores", and "Funeral Homes and Funeral Services".[216]

Safegraph claims to receive GPS coordinates from about 35 million devices every month, although it says that this is based on consumers opting in, and that this is anonymous data because it does not include names or email addresses.

> *"We partner with mobile applications that obtain opt-in consent from its users to collect anonymous location data. From the data provided by these partners, we see about 35 million unique anonymous devices over the course of each month. This data is not associated with any name or email address. This data includes the latitude and longitude of a device at a given point in time. We take this latitude/longitude information and determine visits to points of interest. We then aggregate these anonymous visits to create our Patterns product."*[217]

Safegraph maintains a "movement panel" database, which in 2017 consisted of "super-accurate, anonymized location data on over 5 % of all mobile phones in the U.S.", for example to help adtech companies with extracting and validating location data from bid requests in real-time bidding.[218]

---

[214] "Places Schema", Safegraph [accessed December 11, 2019] https://docs.safegraph.com/docs/places-schema#section-patterns

[215] Mnemonic, "Review of communications from apps", chapter 3.3.2 https://www.forbrukerradet.no/out-of-control/

[216] According to Safegraph, this is only done in the US. The list of place categories is available online. [accessed December 11, 2019] https://docs.safegraph.com/docs/places-summary-statistics#section-category-statistics

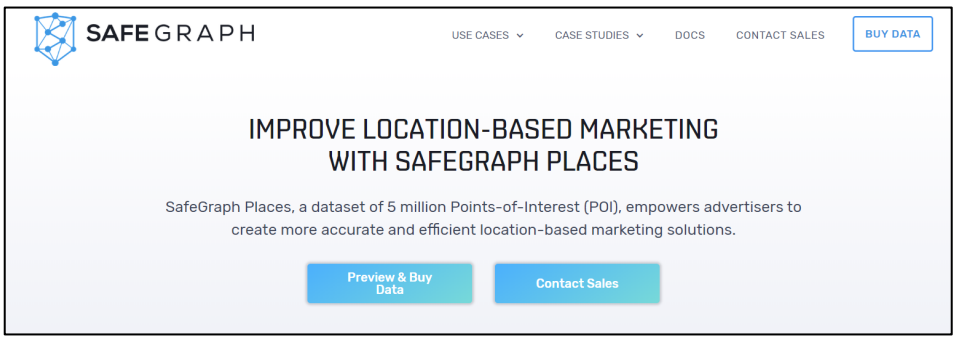
[217] "FAQs", Safegraph [accessed December 11, 2019] https://docs.safegraph.com/docs/faqs

[218] "Less than 10% of bid-stream location data is high-quality — and we know how to find it", Natasha Whitney [accessed December 11, 2019]

When tracking movement data during Thanksgiving 2016, Safegraph collected 17 trillion location markers from 10 million smartphones in the US just during the holidays. Researchers used this data set to identify the homes of individuals who were tracked through their phones.[219]

Safegraph also helps advertisers with attribution, to see whether online advertising spurred consumers to physically visit their stores. Combined with what it calls "precise building footprints", Safegraph allows advertisers to combine data for "visit attribution".

> *"[…] combine location data with SafeGraph Places to understand whether data falls inside a particular store, brand, or category of place (visit attribution). This derived location-context helps advertisers do better location-based marketing."*[220]




*20 Source: https://www.safegraph.com/advertising [accessed December 11, 2019]*

In its privacy policy, Safegraph states that it collects Advertising ID and precise GPS coordinates, in addition to various other data that allows for cross-device tracking of location.

> *"Mobile ad identifiers, primarily Apple iOS IDFAs or Google Android IDs;*
>
> *The precise geographic location of a device at a certain time, usually expressed in latitude/longitude coordinates along with a timestamp"*[221]

https://blog.safegraph.com/less-than-10-of-bid-stream-location-data-is-high-quality-and-we-know-how-to-find-it-3a2c0df35475

[219] "Politics really is ruining Thanksgiving, according to data from 10 million cellphones", Christopher Ingraham https://www.washingtonpost.com/news/wonk/wp/2017/11/15/politics-really-is-ruining-thanksgiving-according-to-data-from-10-million-cellphones/

[220] "Improve Location-Based Marketing with Safegraph Places", Safegraph [accessed December 11, 2019] https://www.safegraph.com/advertising

[221] Safegraph privacy policy (last updated May 16, 2018) https://www.safegraph.com/privacy-policy

Safegraph claims to aggregate this data and sell it to other companies, who may use it for targeted advertising. It also uses the data for its own marketing purposes, indicating that it is a controller.

> *"SafeGraph aggregates the Information collected from these mobile apps, i.e., our data partners, and provides the Information to our customers. Our customers – a variety of companies and organizations – in turn use the Information for a variety of commercial and research purposes, including ad targeting (for instance, building models of inferred audience preferences), [...]*
>
> *SafeGraph may also use the Information for our internal and operational purposes, such as to consider or make internal service improvements or quality checking, or for our own sales and marketing purposes, and more generally to operate, maintain and improve the services we offer."*[222]

According to Safegraph's privacy policy, the data it collects may also be used to target users across devices.

> *"Sometimes the Information is used to build models that connect different devices. For instance, some of our customers may create "cross device" capabilities to enable marketers to target specific sets of users across various channels and devices."*[223]

In its privacy policy, Safegraph claims not to intentionally collect data from or target users within EU and EEA countries, and states that it will delete data that it receives from individuals in Europe on a timed basis. Consequently, Safegraph does not state what legal basis it is using for processing personal data, as this is only a requirement where the GDPR applies.

Although the technical tests cannot show whether or not Safegraph actually uses the personal data it receives from European users of Perfect365, the fact that it receives the data constitutes a processing operation. This indicates that the GDPR does in fact apply to some of the processing operations of Safegraph. As Perfect365 did not collect a legally compliant consent for sharing personal data, Safegraph appears to lack a legal basis for this processing.

### 6.1.3 Fluxloop

Fluxloop is a location data broker that is based in Oslo, Norway. Its location-based advertising tool is called Pinch. According to the Fluxloop website, Pinch

[222] Ibid.
[223] Ibid.

offers app providers and advertisers *"the ability to communicate with your users when in specific locations."*[224]

During the technical testing of Perfect365, Fluxloop was observed receiving data containing a reference to another server (improbability-dot-uc-h2g2.appspot.com/unacastsdk).[225] Mnemonic cannot identify who controls this server, but there are indications. The term "unacastsdk" points to the location data company Unacast. Furthermore, until recently the Perfect365 privacy policy referenced Unacast as a "Perfect365 partner".[226] However, data transmitted to this unknown server also contains several references back to Fluxloop.

Mnemonic observed this server receiving the Advertising ID, GPS-coordinates, battery level,[227] battery charging status, and Wi-Fi access point information. Personal data flowing to this server may be mainly controlled either by Fluxloop or by Unacast, but we cannot definitely answer this based on Mnemonic's data flow analysis. Based on the references and terms mentioned in the data transmission, it may be assumed that both companies control this process to some extent. Unacast's services are described in the next section.

Publishers and third party vendors can use Pinch/Fluxloop to tailor advertising based on location, which creates *"the opportunity to post customized communication based on the recipient's interest, location and previous location."* Fluxloop combines location tracking through apps with physical beacons that can track consumers as they move around, and also use "behaviour data" to enrich its segments. Fluxloop claims to have data on more than 1 500 000 "end users".

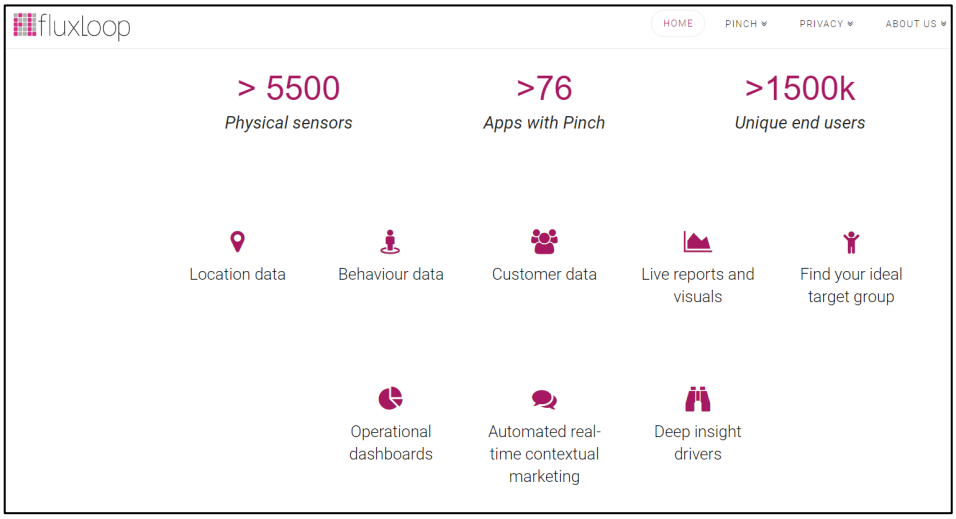
---

[224] "Pinch", Fluxloop [archived May 19, 2019]
https://web.archive.org/web/20190519212734/http://fluxloop.com/pinch/

[225] Mnemonic, "Review of communications from apps", chapter 3.3.5
https://www.forbrukerradet.no/out-of-control/

[226] Perfect 365 privacy policy (last updated April 25, 2019) [archived June 8, 2019]
https://web.archive.org/web/20190608081442/https://www.perfect365.com/about/privacy-policy/#

[227] Battery status can be valuable information when performing behavioural tracking, as user behaviour changes when they are stressed due to low battery levels. For example, Uber have been accused of using consumers' battery levels to dynamically change ride fares. "Does Uber charge more if your battery is lower?", Jessica Lindsay"
https://metro.co.uk/2019/09/27/uber-charge-battery-lower-10778303/




*21 https://fluxloop.com/pinch/ [archived at https://web.archive.org/web/20190414234826/https://fluxloop.com/pinch/]*

According to its privacy policy, Fluxloop uses its Pinch technology for location-based targeting based on GPS coordinates and other sensor technology.

> *"Pinch™ enables advertisers and publishers to gain customer insight, target marketing and offer value added services based on sensors and mobile applications, enabling real-time registration of the physical location of the users of the application."*[228]

Fluxloop goes on to claim that it only collects location data from consumers if the consumer has given in-app consent. This includes collecting location data also when the app is not in use.

> *"When you use an app using Pinch™, fluxLoop will register the mobile device's location. Registration of location will only take place when you have:*
>
> *1. Accepted location based services in the mobile device's operating system (only iOS);*
>
> *2. Given your consent in the application to registration of localisation even when the application is not active."*

Fluxloop also combines data collected across any apps using Pinch.

> *"If you have several applications which uses Pinch™, fluxLoop may compile personal data collected from all those apps to make information, services and advertisement even more relevant to you."*

[228] Fluxloop privacy policy (not dated, accessed October 16, 2019) https://fluxloop.com/privacy-policy

In its privacy policy, Fluxloop also claims to use "de-identified" personal data tied to a hashed unique identifier to provide targeted advertising.

> *"fluxLoop may use de-identified personal data extracted from data sets collected from applications utilizing the Pinch™ technology to target a specific audience on behalf of a customer."*[229]

Fluxloop goes on to claim that it processes personal data based on explicit consent. If the data is "de-identified", however, it relies on legitimate interests. If the consumer does not want Fluxloop to collect personal data, they have to opt out through device settings or uninstall the app that is transmitting data to Fluxloop.

> *"Processing of personal data administered by Pinch™ for the purpose of providing you with relevant information in the app (ref. A above) is based on your informed and explicit consent. You may at any time withdraw your consent by disabling Bluetooth, disabling location based services in the operating system (iOS), disabling Pinch™ in the application settings or by uninstalling the application."*[230]

Perfect365 did not provide users with enough information to give informed consent to processing and sharing of personal data. If personal data that was observed being sent to the unidentified server is mainly controlled by Fluxloop, the company appears to lack a valid legal basis to process the personal data it was observed receiving. Additionally, asking users to disable location based services and Bluetooth to opt out does not fulfil the GDPR condition of explicit consent.

### 6.1.4 Unacast

Unacast is a location data broker that used to be situated in Oslo, Norway, but is now headquartered in New York.[231] Its investors includes the venture investment company Investinor, which is funded by the Norwegian government, and the major telecom provider Telia.[232] It uses location data collected from apps to "enable clients to leverage location and proximity data for retargeting and attribution", which means that it connects digital behaviour

[229] Fluxloop privacy policy (not dated, accessed October 16, 2019) https://fluxloop.com/privacy-policy
[230] Ibid.
[231] "Unacast bags $17.5M to do more with location data", Natasha Lomas https://techcrunch.com/2018/02/13/unacast-bags-17-5m-to-do-more-with-location-data/
[232] "About Unacast", Unacast https://www.unacast.com/about#investors [accessed December 12, 2019]

to physical movement data. In 2018, Uncast claimed to receive daily data from more than 50 million consumers across six continents.[233]

As described in the previous section, certain personal data observed being sent from Perfect365 was transmitted to a server controlled either by Fluxloop or Unacast, or by both of them. These transmissions included a number of different types of data, including GPS coordinates, Advertising ID, Wi-Fi information, and phone metadata including battery levels.[234] As mentioned above, Unacast was referenced as a "Perfect365 partner" in the Perfect 365 privacy policy, although this reference was removed at some point between June and November 2019.[235]

Unacast allows its customers to access location data from a variety of sources, including its SDK and from real-time bidding bidstreams.[236] According to a 2018 interview with their CEO, Unacast aims to be a major provider of location data to other marketers and adtech companies.

> *"[Google and Facebook] have their proprietary location data sets. However they never, ever sell that data. That is theirs. So, for the rest of the industry or multiple industries that are looking to understand where people move around, where they live, where they work, where they shop, where they dine and how they commute, they need to get access to this data from another party in a structured and suitable manner. And that is the company that Unacast is striking to become."*[237]

---

[233] "Unacast Exceeds 50 Million Daily Average Users Across Six Continents, Leading Global Location Data Market in Quality and Quantity", Unacast https://www.globenewswire.com/news-release/2018/11/05/1645250/0/en/Unacast-Exceeds-50-Million-Daily-Average-Users-Across-Six-Continents-Leading-Global-Location-Data-Market-in-Quality-and-Quantity.html

[234] Mnemonic, "Review of communications from apps", chapter 3.3.5 https://www.forbrukerradet.no/out-of-control/

[235] Perfect 365 privacy policy (last updated April 25, 2019) (archived June 8, 2019) https://web.archive.org/web/20190608081442/https://www.perfect365.com/about/privacy-policy/#

[236] "Data Sources Pros and Cons: How do SDK, Bid Stream & Beacon Compare?", Amy Fox [accessed December 11, 2019] https://www.unacast.com/post/data-sources-pros-and-cons-how-do-sdk-bid-stream-beacon-compare

[237] "Unacast bags $17.5M to do more with location data", Natasha Lomas https://techcrunch.com/2018/02/13/unacast-bags-17-5m-to-do-more-with-location-data/


*22 Source: https://www.unacast.com/ [accessed October 9, 2019]*

Unacast runs a partner network, of which Fluxloop is a member, to "give retailers and brands new retargeting possibilities, in addition to providing a more complete picture of the offline behavior".[238]

According to its privacy statement, Unacast may collect a variety of data from apps where their SDK is embedded, including Android Advertising ID, precise geolocation including altitude, device metadata, IP address, sensor data, Wi-Fi data, cell network data, and more. However, it claims that none of this data can identify individuals.

> *"The data provided by our Partners and the data collected by means of the SDK does not include data that directly identifies you, such as your name, mobile phone number, or your email address."*[239]

The location data collected by Unacast, which it calls "location intelligence", can be used for a number of purposes, including targeted advertising and audience segmentation.

> *"This location intelligence can be used for advertising, audience segmentation, people-based movement analytics, improving business decision making by better understanding of customer movement patterns, assisting municipalities in urban planning by enhanced understanding of movement patterns, and similar purposes that utilize location as a tool."*[240]

Unacast may also share this data with other adtech companies, including data brokers. These partners include AdSquare, Tapad, and numerous other adtech companies.

---

[238] "Welcome to Unacast PROX Network", Unacast [accessed December 11, 2019] https://www.unacast.com/post/welcome-to-unacast-prox-network
[239] Unacast privacy statement (last updated June 3, 2019) https://www.unacast.com/privacy/statement
[240] Ibid.

> *"We may disclose the data provided by the Partners and the data collected by the SDK with third parties such as advertising networks, advertising publishers, and advertisers, research companies, data brokers, financial institutions, data analytics platforms, in accordance with the terms of the agreements, and only for the purposes of performing such agreements, that we have in place with such third parties."*[241]

In order to opt out of Unacast collecting the Android Advertising ID, consumers have to email the company.

> *"You can email Unacast at privacy@unacast.com, including the Advertising ID in your email, and request the blocking of the Advertising ID from further use or disclosure by Unacast. If we have that Advertising ID, once we have blocked the Advertising ID, you will receive a confirmation email from us. Please bear in mind that the blocking of the Advertising ID by Unacast following your request to that effect will not have an impact on any uses or disclosures that have already taken place."*[242]

Unacast claims to normally process personal data based on its legitimate interests to provide location-based services, and in some cases relies on consent collected by app providers.

> *"We process the data provided by the Partners and the data collected by the SDK based on our legitimate interest of providing, improving, and analyzing our location-based products and services and, where appropriate or as required by law, based on your consent that you have provided to our Partners."*[243]

Although Unacast claims that it does not process data that "directly identifies" the user, this is contradicted by the GDPR, as unique identifiers and precise geolocation is identifiable information. In other words, the data that Unacast was observed receiving from Perfect365 is clearly personal data under the GDPR. As will discussed in chapter 8, Unacast's legitimate interests to provide location based products to its customers is unlikely to outweigh the fundamental rights and freedoms of the data subjects.

### 6.1.5 Placer

The Israeli data broker and data company Placer offers retailers and other clients "unprecedented visibility info consumer foot-traffic". It provides or sells its clients insights about physical store visits, based on location data collected from millions of smartphones. According to the company, this includes data

[241] Ibid.
[242] Ibid.
[243] Ibid.

about popular locations, “store intelligence” from over 13 million venues in the US, and audience insights such as customer demographics and interests. Placer boasts of having data on more than 1.5 billion “monthly visitors” and from over 20 million “active devices”.[244]

Placer were observed to receive GPS coordinates, sensor data (altitude, course, speed), Wi-Fi access point data, cell tower data, and Bluetooth properties from MyDays.[245] All of these data points can be used to pinpoint location indoors, down to the floor of the building the consumer is situated on. Placer were not observed to receive the Android Advertising ID, but instead uses its own proprietary user ID. Although MyDays details some of their data sharing partners, their privacy policy does not mention Placer.

According to one press article from 2018, Placer claimed to be able to “track the movements of 60 percent of Android users and 40 percent of iOS smartphone users in the United States”.[246] The company also claims to provide services that “Reveal in-depth insights into tenant visitors”, based on “Foot-Traffic Insights for Brokerage Firms”. [247] Additionally, it professes to harness data from a large number of devices for purposes such as “behavioural predictions”.

> *“Now, anyone can make data-driven decisions with access to precise human movement analytics and a deeper understanding of audiences and competition. By harnessing mobile data from tens of millions of devices, Placer.ai applies the latest in AI, machine learning, and big data analytics to generate accurate insights and behavioral predictions for any location, store, or geographic area.”*[248]

According to an 2018 article on Placer, it collects data from 100 apps that have embedded the Placer SDK. Although it claims to “accurately track” the location of 60 % of Android users in the USA, Placer also claims that this is anonymous data.

> *“The company said it obtains its data through the 100 popular smartphone apps that use its SDK and that it can anonymously but*

---

[244] Placer https://placer.ai/ [accessed December 11, 2019]

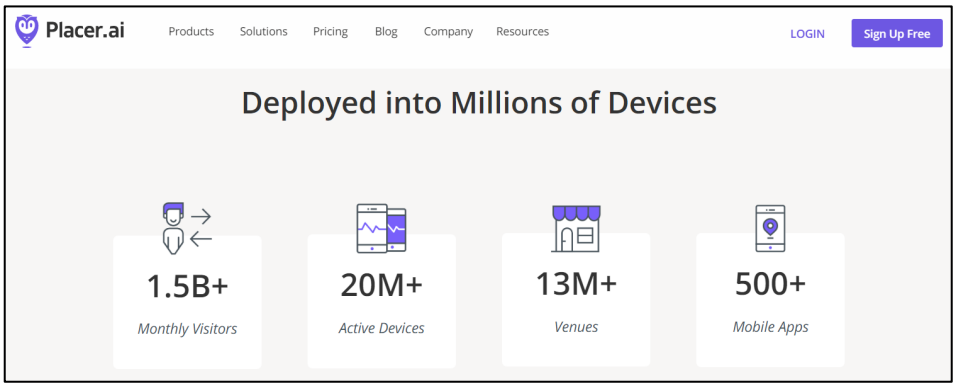
[245] Mnemonic, “Review of communications from apps”, chapter 2.4.3 https://www.forbrukerradet.no/out-of-control/

[246] “Placer.ai raises $4 million to use AI to track foot traffic”, Khari Johnson https://venturebeat.com/2018/10/24/placer-ai-raises-4-million-to-use-ai-to-track-foot-traffic/

[247] “Foot-Traffic Insights for Brokerage Firms”, Placer [accessed December 11, 2019] https://placer.ai/solutions/brokerage-firms

[248] “Placer.ai Raises $4M to Bring Unprecedented Visibility into Consumer Behavior and Foot Traffic in the Physical World”, Placer [accessed December 11, 2019] https://blog.placer.ai/launch-announcement/

> *accurately track the movements of 60 percent of Android users and 40 percent of iOS smartphone users in the United States … Placer.ai aims to tell users not just who visits a business but where they came from and where they go after they leave"*[249]




*23 Source: https://placer.ai/ [accessed December 11, 2019]*

The major adtech company LiveRamp lists Placer as a partner.[250] LiveRamp claims to have data on "more than 250 million consumers represented in the U.S., and many more worldwide".[251]

In its privacy policy, Placer describes that it may collect GPS coordinates, IP address, and unique identifiers, but claims that this is generally not identifiable information.

> *"If you are a Consumer, we may collect information such as geolocation and proximity data (if you have enabled your device to share location information), IP address, unique device identifiers for advertising (Google Advertiser ID or IDFA) and/or a pixel identifier, event information about your device (such as crashes, system activity, and hardware settings), system configuration information, time and date information, and dwell time near points of interest, as determined through beacon, Wi-Fi, and other signals per our proprietary systems. Generally, the information we collect is not information that identifies you personally."*[252]

[249] "Placer.ai raises $4 million to use AI to track foot traffic", Khari Johnson https://venturebeat.com/2018/10/24/placer-ai-raises-4-million-to-use-ai-to-track-foot-traffic/
[250] "Our Partnership with Placer", LiveRamp [accessed December 11, 2019] https://liveramp.com/partners/placer/
[251] "Identity Graph: Connecting Data for Better Customer Relationships", LiveRamp [accessed December 11, 2019] https://liveramp.com/our-platform/identity-graph/
[252] Placer privacy policy (last updated September 27, 2018) https://placer.ai/privacy-policy

Placer claims that it scrubs "personally identifiable information" from the personal data sets it uses and analyse.

> *"Placer's technology is deployed, via integration of our SDK, in thousands of mobile apps and millions of devices. Placer's technology collects data, such as geolocation data, which is scrubbed of any personally identifiable information to protect the privacy of Consumers. Using the aggregated and anonymized data, Placer provides data analytics and actionable insights to Placer Customers. Such data analytics and actionable insights may include foot traffic patterns and Consumer preferences, among many other examples."*[253]

In its privacy policy, Placer states that it relies on the app provider to collect consent for collecting and sharing personal data. It also says that consumers can opt out by using their device settings.

> *"We rely upon the developer and operator of these mobile apps to enable your connection to our Services to provide or withdraw consent with respect to the collection and use of your information. You may also control your mobile device directly by enabling or disabling the applicable settings, such as your location settings."*[254]

For consumers situated in the EU and the EEA, Placer claim to rely on a variety of legal bases for processing personal data, without going into detail about when each legal basis applies.

> *"Placer will only collect and process Personal Data when we have lawful bases for doing so. These lawful bases include when you provide consent, when we have a contractual obligation to collect or process your Personal Data, and when we have a legitimate interest in processing your Personal Data."*[255]

As Placer operates with the US definition of personally identifiable information, it does not consider unique identifiers and location data to be personal data. However, under the GDPR this is clearly personal data, and thus needs a valid legal basis for being processed. Since Placer uses the data it collects for its own commercial purposes, it can be considered a controller. Thus Placer need to make sure that it processes personal data based on a valid legal basis.

As MyDays does not collect a valid consent for processing personal data on behalf of Placer, it is possible that Placer relies on legitimate interests as a fallback option, which is problematic in itself. In any case, the legitimate interest

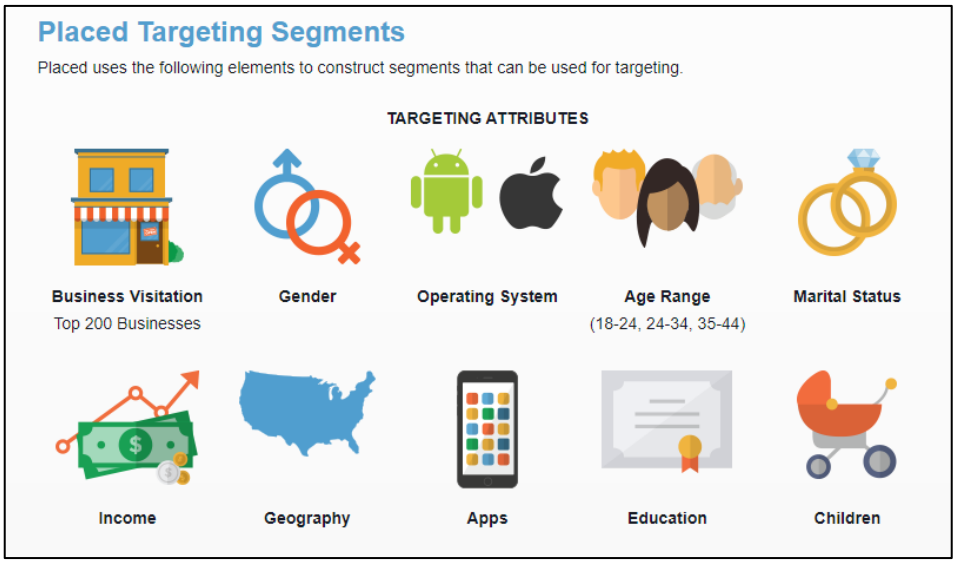
[253] Ibid.
[254] Ibid.
[255] Ibid.

of Placer to provide location-based products and services is unlikely to outweigh the fundamental rights and freedoms of the data subject. Therefore, Placer appears to lack a valid legal basis for processing the personal data that it was observed receiving.

### 6.1.6 Placed/Foursquare

Placed is a US-based location data broker that specializes in delivering audience insights and targeting based on consumer location. According to its website, Placed has recorded 2.8 billion real-world store visits since 2011, and is *"trusted by 350+ publishers, networks, and platforms, and 500+ advertisers and agencies to measure advertising's impact on store visits"*.[256]

The technical testing showed Placed receiving the Android Advertising ID, GPS coordinates, and a list of all apps installed on the device from MyDays. During Mnemonic's testing, Placed received GPS coordinates more than 250 times.[257] According to the MyDays privacy policy, it shares data with Placed to "understand User behaviour and deliver a better Advertisement Experience".




*24 https://www.placed.com/targeting [accessed December 11, 2019]*

In May 2019, Placed were sold by its previous parent company Snapchat, to the location data company Foursquare, a move which resulted in having a "measured audience" of over 100 million unique devices in the US alone, and a

[256] Placed https://www.placed.com/ [accessed December 11, 2019]
[257] Mnemonic, "Review of communications from apps", chapter 2.4.2 https://www.forbrukerradet.no/out-of-control/

registry of over 13 billion user-confirmed visits.[258] This means that consumer location data that previously was part of Snapchat was transferred to Foursquare and combined with Foursquare's data.

> *"By leveraging one of the world's largest location platforms, billions of directly measured locations, and patent-pending statistical models, Placed is able to turn complex location data into actionable insights for our clients."*[259]

Placed offers a number of different attributes that advertisers can use to target consumers, including Business Visitation, Gender, Operating System, Age Range, Marital Status, Income, Geography, Apps, Education, and Children.[260] It is listed as a third party data provider by the major data and marketing company Salesforce.[261]

According to the MyDays privacy policy, Placed collects a large variety of data from MyDays through the Placed SDK, including precise geolocation, IP address, device sensor data, identifiers, lists of installed apps, and different device metadata.

> *"The Placed SDK collects location information, for example precise location using GPS, wireless networks, cell towers, Wi-Fi access points, IP address, and other sensors, such as gyroscopes, accelerometers, and compasses, and device information, such as hardware model, operating system and version, sensor activity, device identifiers (including advertising identifiers assigned to end users' devices), wireless carrier headers, mobile device name, mobile apps installed, and mobile network information."*[262]

According to the Foursquare privacy policy, which covers both Foursquare and Placed, app developers may use the Foursquare SDK to identify where consumers are located and how often they visit specific places, in order to personalize content and to better understand the consumer.

> *"App developers partner with us to use our SDK, which they integrate into their own apps to help them identify when Partner End-Users are near*

---

[258] "Last Letter as CEO of Placed, First Letter as President of Foursquare", David Schim [accessed December 11, 2019] https://blog.placed.com/placed-powered-by-foursquare/

[259] "How it works", Placed [accessed December 11, 2019] https://www.placed.com/how-it-works

[260] "How it works", Placed https://www.placed.com/targeting

[261] "Third-Party Data Marketplace", Salesforce [accessed December 11, 2019] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace

[262] MyDays privacy policy (last updated November 26 2019) https://mydays.club/info/privacy-policy/

> *interesting places of relevance to their service (e.g. a nearby store with respect to which they can offer a coupon), personalize content or information alerts for their locale, identify accurate venue data (such as the geo-coordinates of a restaurant or store) or to better understand their end users by identifying how often their end users have visited a specific venue or chain store ("Visit Data").*"[263]

In some cases, Foursquare retains this data and combines it with its own data sets, and uses the data for its own purposes. Foursquare may also share unique identifiers with other third parties.

> *"When partners use our SDK, we receive certain Partner End-User Data back (e.g. wifi end points, Visit Data, and other Data) if our Partner has contractually agreed to allow us to retain and use such Partner End-User Data. We incorporate such Partner End-User Data into our Enterprise Services, and if contractually permitted, license such Partner End-User Data to business partners. In some cases, if contractually permitted, we share IDs such as an advertising IDs or other pseudonymized data. [...] In the event that a Partner End-User is also a Foursquare User, we combine all data about the user into a single profile."*[264]

Placed/Foursquare states in its privacy policy that it may use several legal bases for processing personal data, including legitimate interests and consent. It operates with a mix of the European concept of personal data and the US concept of personally identifiable information.

> *"Where GDPR applies to the processing of your PII, we rely on several legal bases. These include:*
>
> *When the processing is necessary for our legitimate business interests (or those of our Enterprise Customers), including but not limited to, improving the Consumer Services, or understanding how users are using our Apps and Sites, providing our Enterprise Services and other services to businesses, marketing new features and other services that may be of interest to you;*
>
> *When you have given us your consent, including as described in this Privacy Policy. You may withdraw your consent to processing at any time using the settings on your device or in your account;"*[265]

Because Placed/FourSquare operates with a mix of the European and US concepts of PII/personal data in its privacy policy, it is difficult to know what the

[263] Foursquare privacy policy (last updated September 30, 2019) https://foursquare.com/legal/privacy
[264] Ibid.
[265] Ibid.

company considers to be personal data. [266] However, the technical tests clearly demonstrate that the company is processing personal data as defined in the GDPR. Since FourSquare may combine this data with its own data sets, and use this data for its own purposes, FourSquare is clearly a controller.

Since MyDays did not collect a legally valid consent to the sharing of personal data, it is possible that Placed/FourSquare is relying on legitimate interests. However, the legitimate interest to improve its services and conduct targeted advertising is unlikely to outweigh the fundamental rights and freedoms of the data subject. Therefore, Placed/FourSquare appears to be lacking a valid legal basis for processing the personal data that it was observed receiving.

## 6.2 Behavioural personalization and targeting

Once data on the consumer has been collected, there are a number of ways to make this information actionable. There are a large number of third party vendors in the adtech industry whose main business is collecting data about individual consumers, and use this information to create detailed profiles and user segments. As described in chapter 2, these profiles can be used to make sure that the right message reaches the consumer at the most receptive moment.

The practice of tailoring messaging based on real-time and/or historical behavioural data is called behavioural targeting. With the amount of data being transmitted to third party advertisers through smartphones, this can be done in real time, continuously adapting the personalization techniques. This technology works on the assumption that the more you know about an individual, the better you are equipped to influence them by displaying your message at the right moment and in the perfect context.[267]

Below, we describe a number of companies that were observed to receive personal data during the technical tests. These companies are all involved in some form of behavioural targeting and personalisation, which may explain why they were observed receiving data that could be used to create and enrich consumer behavioural profiles.

---

[266] In a US setting, "personally identifiable information" is the equivalent of the EU concept of personal data. However, the concept of PII is more narrow than personal data as defined in the GDPR. For example, the EU concept of personal data includes information such as cookies and IP addresses, which are not considered PII. See "What Is PII, non-PII, and Personal Data?", Piwik https://piwik.pro/blog/what-is-pii-personal-data/

[267] "Behavioural targeting: be more efficient", Lucy Tesseras https://www.marketingweek.com/behavioural-targeting-be-more-efficient/

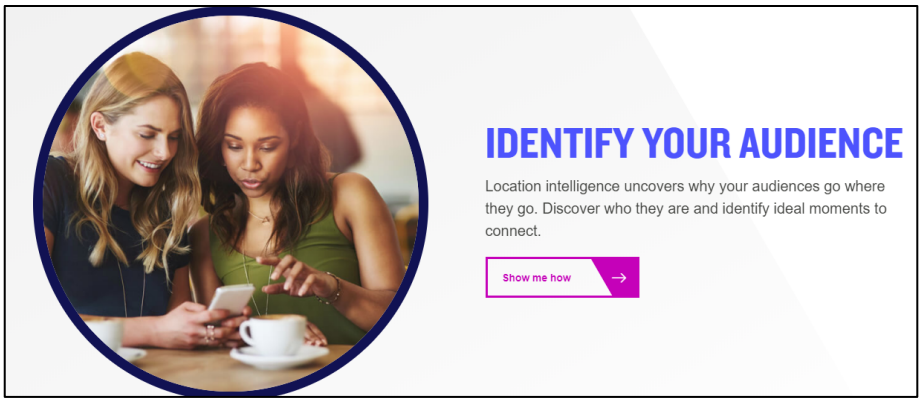
### 6.2.1 Receptiv/Verve

Receptiv (formerly Mediabrix) is a part of the California-based adtech company Verve, which supplies advertisers with different ways to reach users of mobile apps. Before it became a part of Verve, Receptiv specialized in what it called "High impact emotional moment targeting", running a Data Management Platform based on data from 150 million mobile devices.[268]

During the technical testing, Mnemonic observed Receptiv receiving the Android Advertising ID and GPS coordinates from Perfect365. Some of these transmissions were unencrypted, which means that other parties could quite easily intercept the transmission.[269] Unencrypted transmissions of location data is considered a security risk.

In addition to providing behavioural advertising, Receptiv offers advertisers a solution it calls "Location intelligence", which uses geolocation to optimize ad targeting. According to the Verve website, the use of location intelligence allows advertisers to reach consumers at the most receptive moments.

> *"Location intelligence helps you discover their habits and passions, sparking genuine connections at the perfect time."*[270]




*25 Source: https://www.verve.com/solutions/advertisers/ [accessed December 11, 2019]*

[268] Receptiv [archived January 3, 2019] https://web.archive.org/web/20190103100603/https://www.receptiv.com/

[269] Mnemonic, "Review of communications from apps", chapter 3.3.4 https://www.forbrukerradet.no/out-of-control/

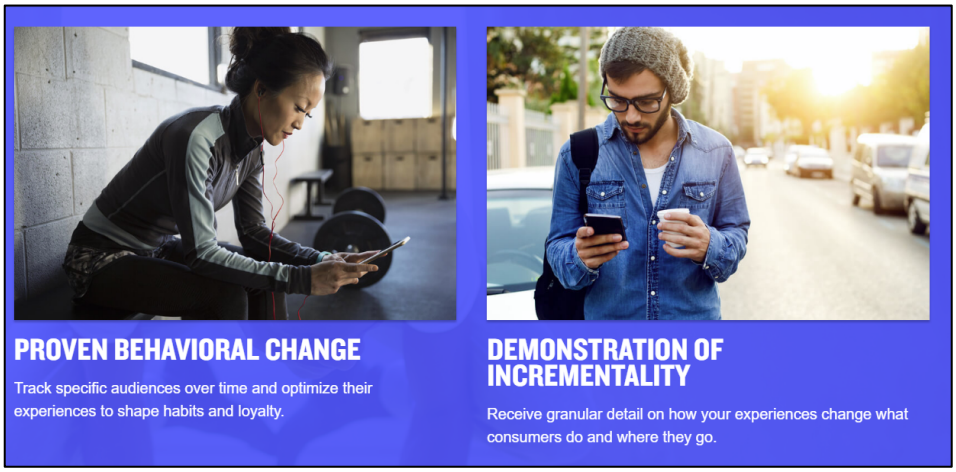
[270] "Maximize your mobile marketing", Verve [accessed December 11, 2019] https://www.verve.com/solutions/advertisers/

Verve focuses on location data for its targeting, but also offers targeting based on audience segments, which it appears to compile based on all the data that it collects from apps and devices. This is described in Receptiv's documentation.

> *"Receptiv DMP leverages proprietary in-app behavioral analytics and advanced machine learning models based on more than 150 million mobile devices. Receptiv DMP uses predictive modeling algorithms to turn 80+ terabytes of raw, disparate data into targetable and actionable audience segments, powering the next generation of intelligent mobile advertising."*[271]

By tracking consumer location, Verve claims to be able to both influence behaviour in real-time, and continuously revise its system by monitoring the effects of their targeting.

> *"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. It's something Verve calls Movement Science™ and we use it to create the best mobile marketing experiences possible."*[272]




*26 https://www.verve.com/products/momentum/ [accessed December 11, 2019]*

In its privacy policy, Verve describes how it uses location data for serving ads, which it may supplement with a variety of device sensor data. According to Verve, consumers can opt out of the collection of location data through their

[271] Receptiv [archived January 3, 2019] https://web.archive.org/web/20190103100603/https://www.receptiv.com/
[272] Verve [accessed December 11, 2019] https://www.verve.com/

device-level settings, although Verve will still use other sources such as IP addresses to determine location.

> *"Location data that you provide to an app or web site may be provided to Verve for ad serving or reporting purposes. In addition, supplemental information may also be used such as a device's speed of movement and positioning, proximity of nearby devices, or similar information available from an operating system. You can opt-out of the use of precise data for location-based tracking by using the settings available on your mobile device. Ads will continue to be selected for you based on more general information, such as location that can be inferred from Internet Protocol (IP) addresses or other data."*[273]

Verve operates with the US definition of Personally Identifiable Information (PII). Therefore it does not regard data such as IP addresses to be identifiable. Its privacy policy states that Verve may share all such non-identifiable information with other third parties such as ad networks and other adtech companies. Users have to use their device settings if they want to opt out of this sharing.

> *"Verve may disclose Non-Personal Information to vendors, such as analytics companies and to advertisers, ad networks, other partners, and third parties. To opt-out of sharing by Verve of individual level information with additional parties, you can use the "Limit Ad Tracking" settings on your mobile device."*

Since Verve operates with the American definitions of PII, it is unclear whether it is trying to comply with the GDPR, although the technical testing shows that Verve is processing personal data on individuals situated in Europe. This means that it has to treat IP addresses and location data as personal data. Verve's use of personal data for its own purposes, including sharing data with further adtech companies, means that it is a controller.

As Perfect365 did not obtain consent in a legally compliant way, and Verve operates on an opt-out basis where users have to use device settings to opt out of their location data being shared with further third parties, Verve does not fulfil the GDPR conditions for consent. Thus Verve seems to be lacking a valid legal basis for processing the personal data that it was observed receiving. Additionally, the transmission of unencrypted personal data is a violation of the GDPR provision stating that controllers and processors must use appropriate technical security measures for the processing of personal data.[274]

---

[273] Verve privacy policy (last updated November 15, 2019) https://www.verve.com/privacy-policy/

[274] GDPR Art. 32(1)

### 6.2.2 Neura

The California-based digital marketing company Neura specializes in using real-time behavioural data in order to deliver personalized messaging, in what it calls "moment-based engagement". According to its website, "Neura was built to create mobile experiences that adapt to each user's real-world behavior, helping you segment each and every user based on who they are and what they are doing."[275]

The traffic analysis of MyDays showed the app transmitting GPS coordinates, a list of Wi-Fi access points, some "behavioural events", and battery level to Neura.[276] Instead of using the Google Advertising ID, Neura employs its own unique ID, which it claims can be used by its customers but not by Neura itself.[277]

The company profiles consumers based on data collected from apps, which is used to tailor messages such as notifications based on factors such as geolocation, mental state, and life events, in what Neura refers to as "Neura True Personas":

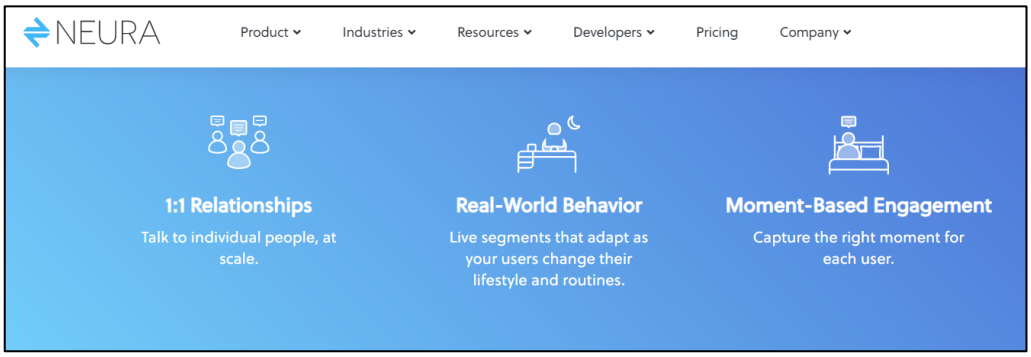
> *"Every user has a distinct lifestyle—a morning commuter, a workaholic, an avid runner, a student, a stay-at-home-parent—and you need to provide dynamic, personalized experiences that adapt to meet their needs and preferences.*
>
> *Neura intelligently segments your audience based on each user's unique lifestyle and behavioral traits. Send gaming notifications to "Morning Commuters" as they get on the train and tailor specific campaigns to Fitness Enthusiasts, Hard Workers, and users that are Sleep Deprived. Because web traffic, age, gender, and location are only part of the story."*[278]

Neura has a partnership with MyDays, which is used as a success-story on the Neura website, where it is claimed that by using behavioural data from Neura, MyDays boosted its average revenue per user by 150 %.[279] This partnership is

[275] Neura [accessed December 11, 2019] https://www.theneura.com/
[276] Mnemonic, "Review of communications from apps", chapter 3.4.3 https://www.forbrukerradet.no/out-of-control/
[277] "Explaining Neura to Your Legal Team", Jared Fleitman [accessed December 11, 2019] https://www.theneura.com/blog/explaining-neura-to-your-legal-team/
[278] "Knowledge is Power", Neura [accessed December 11, 2019] https://www.theneura.com/neura-insights
[279] "MyDays Increases ARPU by 150%", Neura [accessed December 11, 2019] https://www.theneura.com/case-studies/mydays

also mentioned in the MyDays privacy policy.

> *"Neura's system is able to analyze the raw data gathered and identify real time situations and moments, predict future moments and compose behavioral profiles and user personas."*[280]




*27 Source: https://www.theneura.com/ [accessed December 11, 2019]*

In Neura's privacy policy, it states that it collects a variety of data through its SDK, including "Device ID, Location data, Wifi MAC address, and sensory data". Neura uses the data it collects to create behavioural profiles.

> *"Our system is able to analyze the raw data gathered and identify real-time situations and moments, predict future moments, and compose behavioral profiles and user personas. Personas are machine learning generated user profiles that represent each user's real-world behavioral traits."*[281]

These profiles are shared with Neura's customers, who may subscribe to being notified about events in the consumer's life.

> *"Information that is generated by Neura after the processing of the raw data will be shared with third parties that are Neura's Customers in order to provide End Users with enhanced personalized experiences. Neura Customers will be notified regarding specific situations and moments in the End User's life, or behavioral profiles of the End Users according to the services they have subscribed to."*[282]

[280] MyDays privacy policy (last updated 2 July 2019) https://mydays.club/info/privacy-policy/
[281] Neura privacy policy (last updated March 25 2019) https://www.theneura.com/privacy-policy/
[282] Ibid.

According to Neura's privacy policy, it only receives data based on the explicit consent of the user. Although it claims not to use data for its own purposes, Neura identifies itself as a controller.

> *"Neura as a data controller, processes data on the legal basis of consent. Therefore, we require our customers who are subject to the GDPR to enable Neura to obtain the user's consent in a manner that is compliant with the GDPR principles while demonstrating the value user receives in exchange.*
>
> *Users are required to provide consent to the activation of Neura SDK in their Neura-enabled product. Consenting to the activation of the Neura SDK will indicate that the User agrees to the terms set forth in Neura's Privacy Policy."*[283]

Consumers who want to withdraw their consent or otherwise opt out of Neura collecting their data, are asked to send the company an email.

Although Neura is referenced in the privacy policy of MyDays, the app does not inform users clearly about this upon registration, and users cannot choose to use MyDays without data being shared with Neura. As a controller and a partner of MyDays, Neura has a responsibility to ensure that there is a valid consent for the processing of personal data. Since users are not given a legally valid consent request for this data sharing and processing, Neura seems to be lacking a valid legal basis to process the personal data that it was observed receiving.

### 6.2.3 Braze

Braze is a New York-based company that delivers a variety of services to app-providers, including analytics and personalized messaging. During the technical testing, Mnemonic observed Braze receiving personal data from both OkCupid and Grindr, including data related to sexual preferences, drug use, and more.

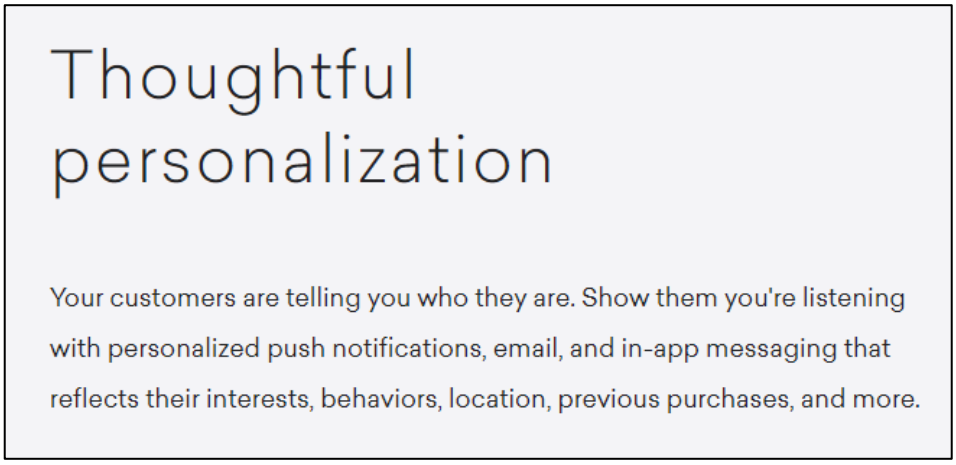
Braze offers to help its clients "create live views of their customers that stream and process historical, in-the-moment, and predictive data in an interactive feedback loop" so that its clients can use "relevant messaging across mobile and web".[284] In other words, to influence consumer behaviour based on real-time data analytics. The company states that it uses customer data to help clients "segment, personalize, and optimize messaging" and recommends its publisher partners to share as much data as possible.

---

[283] Neura GDPR policy (last updated June 26, 2018) https://www.theneura.com/gdpr/
[284] Braze [accessed December 11, 2019] https://www.braze.com/

> *"Your customer profiles should inform your entire approach. Age, gender, location, purchases, likes, and other key characteristics are included in each. Braze uses your customer profiles to help you segment, personalize, and optimize messaging as you go. The more you know, the better."*[285]

Braze claims to process data on "1 billion monthly active users",[286] and allow its "clients" to obtain and share data on its users with many other companies for purposes such as data augmentation, location services and fraud protection.[287]

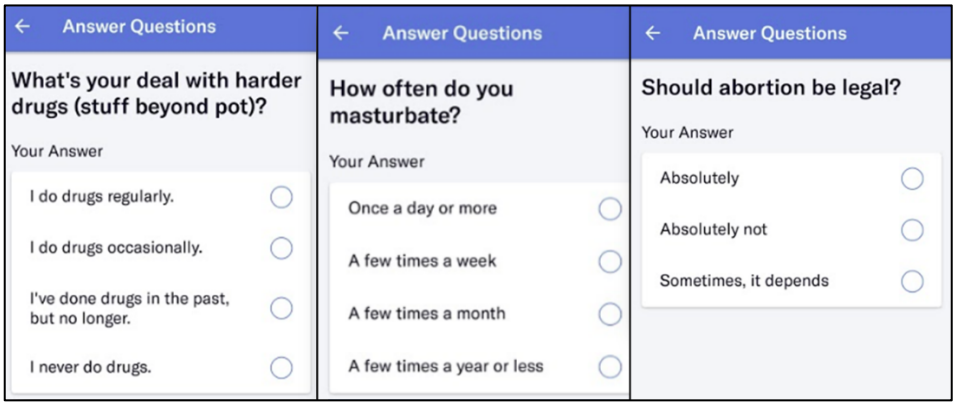



*28 Source: https://www.braze.com/product/cross-channel-personalization/ [accessed December 11, 2019]*

The technical testing showed Braze receiving very sensitive personal data from OkCupid. When first opening an OkCupid account, the user is asked to answer a series of questions about themselves. These can be innocuous questions about what movies the user likes, but also include very intimate questions about sexual desires, drug and alcohol use, political views, and more. These questions and answers were transmitted to Braze. Braze were also observed receiving data about ethnicity and GPS coordinates from OkCupid.[288] This means that Braze has the possibility to identify exceedingly personal details about individuals.

---

[285] "Optimization & AI", Braze [accessed December 11, 2019] https://www.braze.com/product/optimization-ai/
[286] Braze [accessed December 11, 2019] https://www.braze.com/
[287] "Partners", Braze [accessed December 11, 2019] https://www.braze.com/product/alloys/partners
[288] Mnemonic, "Review of communications from apps", chapter 3.5.2 https://www.forbrukerradet.no/out-of-control/




*29 Questions OkCupid users may be asked to answer.*

On its website, Braze describes how OkCupid uses the Braze platform:

> *"OkCupid keeps a pulse on its metrics from the Braze dashboard. They identify any friction points and take action to their increase their impact in real time."*[289]

In its privacy policy, Braze describes that it may process a variety of personal data on behalf of its customers.

> *"Braze processes a variety of personal information, such as email addresses, device data, ID data, personal life data (eg date of birth, hobbies, location), with regards to our prospects, customers, business partners and vendors (who are natural persons), their respective employees, agents, advisors, freelancers or contact persons, along with data of our Customer's Users authorized by Customer to use the Braze Services or Customer's End-Users using our Customers' Applications and submitting such personal data to the Customer Application, which in turn may be sent to the Braze Platform."*

In addition to receiving very revealing data from OkCupid, Braze was also observed receiving personal data from Grindr. This included GPS coordinates and data stating what the user was "looking for", indicating sexual preferences.[290]

According to Grindr's privacy policy, it uses Braze for analytics purposes:

> *"Another partner, Braze, provides us with the technology to allow us to collect certain information and reports on usage trends without identifying individual visitors (e.g., daily active users, monthly active users,*

[289] "Customers – OkCupid", Braze [accessed December 11, 2019] https://www.braze.com/customers/okcupid/
[290] Mnemonic, "Review of communications from apps", chapter 3.2.5 https://www.forbrukerradet.no/out-of-control/

> *time in app, etc.) and tools which allow us to communicate with users [via an interstitial] within the Grindr App or out of app (e.g. via push notifications or email). Such user communication allows us to message users based on certain criteria, such as location, certain profile data, and/or user behavior in the Grindr App."*[291]

In its privacy policy, Braze specifies how it may collect location data and other information from customers when it acts as processors on the customers' behalf.

> *Our Customers may ask us to track your activity and certain performance metrics in connection with your use of a Customer Application or other digital properties, for example if you have abandoned a shopping cart or if the Customer Application is a game, when you have completed a certain level of that game. Our Customers may send us information about your previous actions in their Customer Application or other digital properties, for example, information about how many times you have purchased items through their Customer Application, digital properties, stores, or elsewhere.*[292]

However, the Braze privacy policy also states that it may share data with its customers under various circumstances.

> *"We may share and disclose information about our Customers and you to the following types of third parties and for the following purposes:*
>
> *To Customers – we may disclose information to our Customers in the form of aggregated, anonymous data about the way the Services have been used [...] to further and enhance our role as a thought leader in the industry.*
>
> *[…] We may use the information we collect from our Customers for a variety of reasons, including:*
>
> *[…] to analyze our Customers' use of the Services for trend monitoring, marketing and advertising purposes;*
>
> *[...]For any other purposes about which we notify our Customers."*[293]

On its website, Braze lists all kinds of partners, including "data augmentation" companies such as FourSquare, Gimbal and NeuraFactual.[294]

---

[291] Grindr privacy policy (last updated December 3, 2018) https://www.grindr.com/privacy-policy/#share_EN

[292] Braze privacy policy (last updated October 2019) https://www.braze.com/privacy/

[293] Ibid.

[294] "Partners", Braze [accessed December 11, 2019] https://www.braze.com/product/alloys/partners

Consumers who wish to opt out of Braze collecting their data, have to fill out an online form.

As is elaborated upon in chapter 8, processors are acting on behalf of a controller in order to provide services, and as a general rule do not use the data they process for their own purposes. This would mean that Grindr and OkCupid are the controllers responsible for the transmission of special category personal data to Braze.

Although this data may be shared with Braze purely for analytics purposes, it is unclear whether Braze may share it with other customers. It is particularly problematic that Braze receives very sensitive personal data if this could be shared with other third parties.

### 6.2.4 LeanPlum

The US-based adtech company LeanPlum specializes in marketing and boosting user engagement in apps, with a focus on real-time engagement and personalization.

During the technical tests, Mnemonic observed LeanPlum receiving the user's GPS coordinates, age, gender, and "gender filter" from Tinder.[295] "Gender filter" describes which potential romantic partners the user is looking for, and therefore indicates sexual orientation, which is special category data.

In 2016, LeanPlum expected to be tracking 12 billion events per day by the end of the year.[296]

> *"Capture a complete picture of your customers by turning real-time behaviors into a deep understanding of their needs and wants. Mobile personalization helps you deliver campaigns tailored to each person to drive conversions, loyalty, and retention — at scale."*[297]

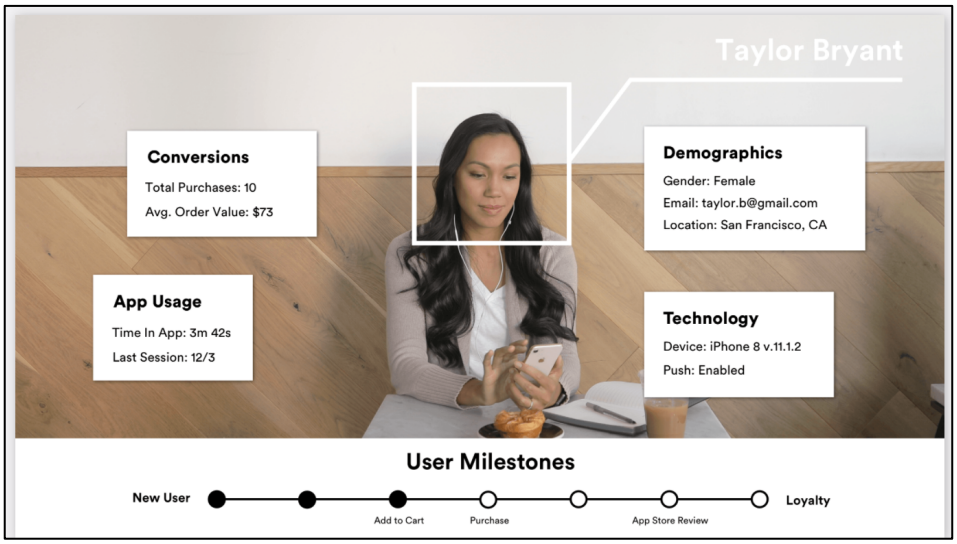
[295] Mnemonic, "Review of communications from apps", chapter 3.8.2 https://www.forbrukerradet.no/out-of-control/

[296] "Leanplum raises $29M Series C round for its mobile marketing platform", Frederic Lardinois https://techcrunch.com/2016/10/19/leanplum-raises-29m-series-c-round-for-its-mobile-marketing-platform/

[297] "Mobile personalization", LeanPlum [accessed December 11, 2019] https://www.leanplum.com/mobile-personalization/

This focus on personalized and targeted content entails collecting user data from apps in order to deliver the right message at the right time, which is meant to maximize how service providers and advertisers influence consumers.

> *"Target based on behavior*
>
> *Mobile is the most personal of devices, always with us and checked hundreds of times a day. As a result, mobile provides a window into our behaviors and preferences. Leanplum leverages those interactions so you can identify intent and effectively deliver the right personalized content in each micro-moment."*[298]




*30 Source: https://www.leanplum.com/mobile-personalization/ [accessed December 11, 2019]*

Through its targeting platform, LeanPlum lets customers browse and segment consumers based on parameters such as user attributes, device data, persistent device identifiers, and app usage.[299]

In September 2019, LeanPlum announced a strategic partnership with the data management platform Tealium, in order to *"enhance marketers' ability to create sophisticated personalized campaigns using holistic first-party data"*.[300] Tealium provides a platform to connect user data from more than 1000 integrated vendors.[301]

---

[298] Ibid.

[299] "Look up and filter user information", LeanPlum [accessed December 11, 2019] https://docs.leanplum.com/docs/look-up-and-filter-user-information

[300] "Tealium and Leanplum Form Strategic Partnership to Unify Data and Campaign Orchestration", LeanPlum https://www.prnewswire.com/news-releases/tealium-and-leanplum-form-strategic-partnership-to-unify-data-and-campaign-orchestration-300927199.html

[301] Tealium [accessed December 11, 2019] https://tealium.com/

In its privacy policy, LeanPlum states that it may use any information it collects for a number of purposes, including for targeted advertising.

> *"We also use your Personal Information to enhance, improve, operate, analyze and maintain our Service and other systems (e.g., to troubleshoot problems); [...] to tailor advertisements, content, and other aspects of your experience on and in connection with the Service"*[302]

According to its privacy policy, the use of an app with a LeanPlum SDK integration is regarded as consent to LeanPlum collecting, using and disclosing personal data. In other words, if a consumer installs an app that uses services from LeanPlum, then LeanPlum considers this as consenting to LeanPlum processing personal data collected from that app.

> *This privacy policy (this "Policy") describes the collection of personal information by Leanplum, Inc., a Delaware corporation ("Leanplum," "we," or "us") from users of our website at www.leanplum.com (the "Website"), as well as all software and other services provided by us via the Website or third party distributors (collectively, together with the Website, our "Service"). [...]By using our Service, you consent to the collection, use, and disclosure of personal information in accordance with this Policy.*[303]

Partners of LeanPlum have to agree to LeanPlum using the data it receives for its own separate purposes, indicating that LeanPlum is a data controller in its own right:

> *For any data that you collect or store via the Service, you grant us and our subsidiaries, affiliates, and successors a worldwide, non-exclusive, perpetual, royalty-free, fully-paid, transferable, and fully sublicensable right to use that data for the purpose of providing you the Service, for Leanplum's internal business purposes, and to disclose aggregated data to third parties. Aggregated data is information that we collect about a group or category of products, services, or users from which individual identities are removed or that otherwise is not personally identifiable.*
>
> *You may modify or remove your data via your Leanplum account, but Leanplum may, in accordance with Leanplum's Privacy Policy, retain in its systems and use non-personally identifiable data that is derived from your data.*[304]

---

[302] LeanPlum privacy policy (last updated August 21, 2018)
https://www.leanplum.com/privacy/
[303] Ibid.
[304] LeanPlum terms of service (last updated December 3, 2017)
https://www.leanplum.com/tos/

If consumers wish to opt out of LeanPlum collecting data, consumers are asked to send the company an email.

> *Leanplum provides you with the opportunity to choose (opt out) whether your personal information is to be disclosed to a third party or to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized. You may exercise your choice by contacting Leanplum at: privacy@leanplum.com.*[305]

That LeanPlum considers to have consent to data sharing based on the consumer using of a service where the LeanPlum SDK is integrated, is not compliant with the GDPR definition of consent. As a controller, LeanPlum cannot rely on implied consent from the data subject. Thus LeanPlum appears to lack a valid legal basis to process the personal data that it was observed receiving from Tinder.

## 6.3 Systemic oversharing

The sheer number of third parties receiving data about individual consumers, along with persistent identifiers, indicates a systemic issue of over-collecting and oversharing throughout the adtech industry.

By collecting information about the apps we use, when and how we use them, what other apps we have installed, when we uninstall apps,[306] and more, our digital realities are mapped out in extensive detail. When this metadata is combined and enriched with sensitive information about our sexuality, health, and identities, our digital profiles are reflections of ourselves that we have no control over, as they are collected, aggregated, and shared as often and as with as many third parties as possible.

During the technical testing of just 10 apps, Mnemonic observed a large number of data transmissions to at least 135 different related third parties that are involved in advertising. Although not all of these transmissions contained excessive personal data such as GPS location, the combination of all this data and different unique identifiers can create quite detailed pictures of individuals, and could also potentially be used to fingerprint devices.

---

[305] LeanPlum privacy policy (last updated August 21, 2018) https://www.leanplum.com/privacy/

[306] "Now Apps Can Track You Even After You Uninstall Them", Gerrit De Vynck https://www.bloomberg.com/news/articles/2018-10-22/now-apps-can-track-you-even-after-you-uninstall-them



The number of third parties also illustrates how data-hungry the app environment is. Although there may be legitimate reasons for transmitting some of this data, in other cases there seems to be a bloated amount of data with no immediately discernible and/or relevant use case for the consumer, but is used by third parties to aggregate and profile users at scale. This is a systemic issue that could potentially be the subject of another investigation.

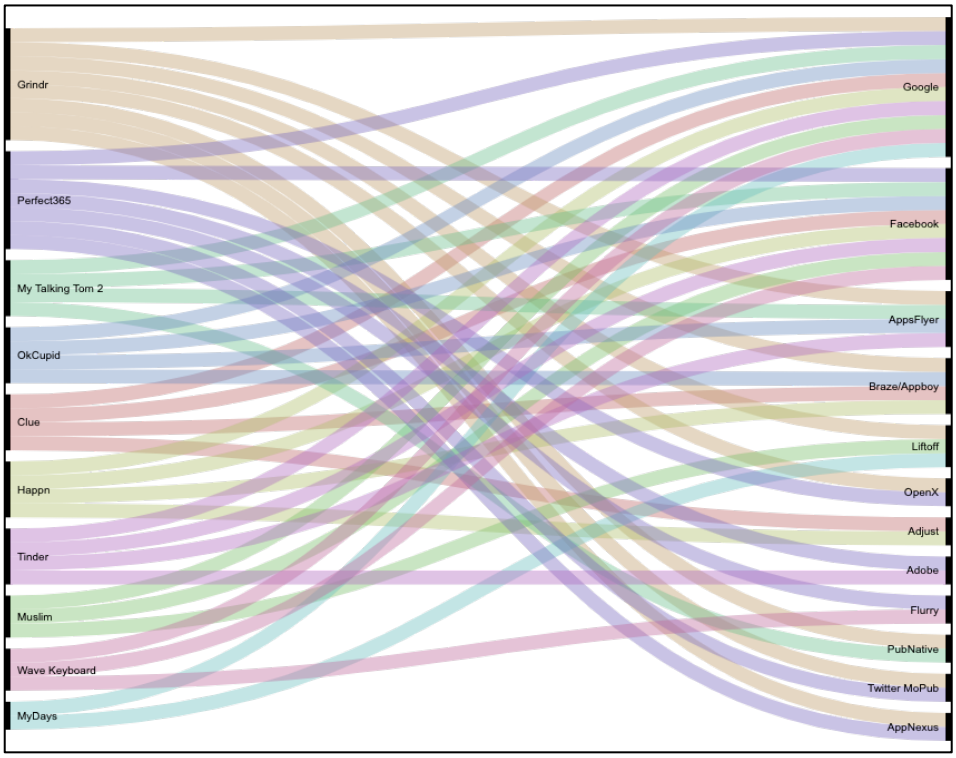
In Mnemonic's testing, many third party companies were observed receiving different other data about the user. Many third parties received data about the consumer's age and/or gender. The current country of the consumer, zip code and system language was also transmitted to numerous companies. A lot of device information and metadata was also shared liberally by the apps that were tested. Additionally, the phone model, current battery level, screen resolution and screen metadata, and information about the consumer's mobile carrier was frequently shared.[307] Such metadata can be used for device fingerprinting.[308]

Other metadata can also be used to infer quite sensitive information about an individual. For example, data about the fact that someone uses Grindr suggests that the individual is most likely gay, bisexual, trans or queer. Frequent usage of period trackers can reveal whether the user is either interested in avoiding a pregnancy or attempting to become pregnant. Other data may be used to decide between these two possibilities. As soon as this data is tied to an identifier, such as the Advertising ID, the consumer is identifiable to third party advertisers and across services. This is tied together with information about the consumers' sexual orientation, or that they are trying to become pregnant.

Many third parties were observed to receive data from several apps during the technical testing. When combined with a unique identifier, this allows the third party to add different data points to the profile they have on the user, which can become very detailed. A list of every app on your phone, combined with how often and how long you use each of them, can already be very revealing. Some third parties also track the day and time when apps are installed and uninstalled, which can signify or help corroborate important events in an individual's life. Cross-referenced with thousands of other data points, metadata can easily become personal data.

[307] Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/

[308] "Fingerprinting mobile devices: A short analysis", Alejandro Gómez-Boix, Pierre Laperdrix, and Benoit Baudry, https://hal.inria.fr/hal-01611101/file/FP_mobile_devices_A_short_analysis%20.pdf




*31 Third parties receiving data from more than one app. Source: Mnemonic, "Review of communications from apps" https://www.forbrukerradet.no/out-of-control/*

During Mnemonic's testing, many third party vendors were observed receiving data from several of the apps. As these companies are present through their SDKs in a number of apps ranging from hundreds to millions, they have the capability to combine this data through using unique identifiers such as the Advertising ID, or perform ID synchronization through other means. The above table shows which third parties were observed receiving data from more than one app during the technical tests.

### 6.3.1 AppsFlyer

The marketing and analytics company AppsFlyer is a very large actor in the global app environment. It claims to leverage "insights from "8.4 billion of the world's connected devices".[309]

[309] "AppsFlyer's People-Based Attribution Provides New Insights Connecting the Consumer Journey Across Mobile and Beyond", AppsFlyer [accessed November 29, 2019] https://www.appsflyer.com/pr/appsflyers-people-based-attribution-provides-new-insights-connecting-the-consumer-journey-across-mobile-and-beyond/

When observing data flows from Tinder, Mnemonic observed AppsFlyer receiving information about the users' Advertising ID, GPS coordinates, birthday, gender, and "target gender", which is data on sexual orientation.[310]

Additionally, OkCupid, Grindr, and My Talking Tom 2 transmitted the Android Advertising ID and various metadata to AppsFlyer.[311] AppsFlyer received the Advertising ID from Grindr combined with the device's IP address, even after the user had opted out of personalised ads.[312] AppsFlyer also received detailed sensor data from the device's magnetometer, gyroscope and accelerometer from OkCupid.

According to AppsFlyer's website, its "technology is found on 98 percent of the world's smartphones".[313] The AppsFlyer SDK is integrated in over 20 billion app installs.[314] One report suggests that AppsFlyer has tracked 23 billion app installs and 45 billion app opens across over 15,000 apps.[315] The company has more than 2000 "integrated partners", including major brands, ad networks, and data brokers.[316]

The AppsFlyer SDK boasts of a variety of features, including analytics, ad retargeting, and integrated ad networks.[317] Because of its large user graph, the metadata processed by AppsFlyer could potentially be used to infer a vast spectrum of attributes about in-app behaviour.

[310] Mnemonic, "Review of communications from apps", chapter 3.8.2 https://www.forbrukerradet.no/out-of-control/

[311] Ibid. chapter 3.13.4

[312] Ibid. chapter 3.12

[313] "AppsFlyer's People-Based Attribution Provides New Insights Connecting the Consumer Journey Across Mobile and Beyond", AppsFlyer [accessed November 29, 2019] https://www.appsflyer.com/pr/appsflyers-people-based-attribution-provides-new-insights-connecting-the-consumer-journey-across-mobile-and-beyond/

[314] According to an AppsFlyer LinkedIn job posting [accessed December 11, 2019] https://il.linkedin.com/jobs/view/mobile-team-leader-at-appsflyer-247581190

[315] "Performance Index Edition IX" , AppsFlyer [accessed December 11, 2019] https://www.appsflyer.com/gatedpdfs/pdfs/performance-index_edition-ix.pdf

[316] "Partners", AppsFlyer [accessed December 11, 2019] https://www.appsflyer.com/partners/

[317] "Mobile Attribution to the Rescue", AppsFlyer [accessed December 11, 2019] https://www.appsflyer.com/product/overview/


*32 Source: [https://www.appsflyer.com/pr/appsflyers-people-based-attribution-provides-new-insights-connecting-the-consumer-journey-across-mobile-and-beyond/](https://www.appsflyer.com/pr/appsflyers-people-based-attribution-provides-new-insights-connecting-the-consumer-journey-across-mobile-and-beyond/) [accessed November 29, 2019]*

According to the AppsFlyer privacy policy, it contractually prohibits its customers from sending "personally identifiable information (PII)", but acknowledge that it may still receive and process personal data.

> *"Within the scope of the engagement between Customers and AppsFlyer, Customers are contractually prohibited from collecting PII, unless otherwise agreed by AppsFlyer. However, Customers have sole control over their properties (including their websites and Application) and configuration of the Services and thus Customers have the technical ability to configure the Services to collect PII. This includes, for example, a Customer using an End User's email address as a Customer issued user ID Technical Identifier. If a Customer has configured the Services to collect PII then we may receive and process such data."*[318]

AppsFlyer regards itself as a data processor on behalf of its customers in most cases. It claims to have a legitimate interest to process data on behalf of customers. In some cases it relies on consent, which it claims should be obtained by the customer on behalf of AppsFlyer.

> *"The lawful basis relied on by AppsFlyer to process Platform Data is its legitimate interest: (i) to provide its Customers using the Services with more accurate analysis and measurement of their marketing campaigns; and (ii) to detect and prevent fraud related to their ad campaigns. AppsFlyer may also rely, where appropriate, on consent obtained by Customers on AppsFlyer's behalf. With regards to Registration Information and Log Data, the lawful basis AppsFlyer relies on is its need to perform its obligations under the Agreement between AppsFlyer and Customer and on its legitimate interests to maintain, analyze and improve the Services."*

[318] AppsFlyer Services privacy policy (last updated March 24, 2019) https://www.appsflyer.com/services-privacy-policy

Although AppsFlyer may be operating as a processor on behalf of Tinder, it is problematic that it receives sensitive personal data such as sexual preferences. This is special category data that should generally only be processed based on explicit consent.

## 6.4 Google and Facebook

The adtech industry is packed with companies that are virtually unknown entities amongst consumers. However, by far the largest actors in the adtech industry are household names, namely Google and Facebook. Although the dominant position of Google and Facebook is outside the scope of this report, it is pertinent to outline the extent of tracking that these companies engage in throughout the mobile app environment.

In the technical testing, all of the apps except Clue and Grindr were observed interacting with Google's advertising service DoubleClick. Additionally, every app was transmitting data to various parts of the Google system, and all of them had integrated various Google SDKs, including Google Ads, Google Crashlytics, and Google Firebase. Some of the data being transmitted to Google may be due to the Android operating system being a Google service. However, it can be difficult to know where Google as a service-provider ends and where Google as an advertising service begins.

All of the apps except MyDays were observed sending the Advertising ID to Facebook's graph API.[319] Every app except Clue had integrated a Facebook SDK. This means that Facebook can potentially track consumers through these apps, even if the consumer does not have a Facebook account.[320]

[319] Mnemonic, "Review of communications from apps", chapter 2.3 https://www.forbrukerradet.no/out-of-control/

[320] For a more detailed examination of how Facebook tracks consumers through SDKs, see "How Apps on Android Share Data with Facebook", Privacy International https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report

| App | Google DoubleClick | Facebook graph API |
|---|---|---|
| Clue | | ! |
| Grindr | | ! |
| Happn | ! | ! |
| Muslim: Qibla Finder | ! | ! |
| My days | ! | |
| My Talking Tom 2 | ! | ! |
| OkCupid | ! | ! |
| Perfect365 | ! | ! |
| Tinder | ! | ! |
| Wave Keyboard | ! | ! |

### 6.4.1 Google

In the adtech industry, Google is a monolithic entity that owns both the marketplace and the distribution system. Google has been criticized by adtech rivals for stifling competition, arguing that Google's control over the supply chain gives the company an advantage that is impossible to match.[321]

Despite Google being a well-known consumer brand, the details of its advertising empire, which makes up a large majority of its income, is very non-transparent to the average user and rarely understood even by experts. By combining data from its other services, Google allows advertisers to target individual consumers on a large number of criteria, attributes, and characteristics.

According to a 2018 study of 959 000 apps available on the Google Play Store, Google trackers, including its advertising services DoubleClick, Admob, and

[321] "Explainer: Advertising executives point to five ways Google stifles business", Paresh Dave and Sheila Dang https://www.reuters.com/article/us-tech-antitrust-google-explainer/explainer-advertising-execs-point-to-five-ways-google-stifles-business-idUSKCN1VW2L9

Adsense, were present in more than 88 % of all apps,.[322] Google's advertising service DoubleClick, which has been rebranded and integrated into the Google Marketing Platform, is also active on more than 80 % of the world's top 10 000 popular websites.[323]

As described throughout this report, Google plays a significant role in cross-service and cross-platform tracking throughout the mobile adtech industry, particularly due to the Android Advertising ID. The trust-based approach of Google's mobile advertising policies appears to allow a large variety of third and fourth parties track consumers across Android-based devices.

### 6.4.2 Facebook

Facebook collects user data from a large percentage of websites and apps, which can be combined with data from its social network. This has allowed Facebook and third parties to gain significant additional insights and targeting possibilities towards Facebook users. The 2018 study on tracking in Android apps found that Facebook had trackers integrated in more than 42% of all apps available in the Google Play store.[324]

For example, a 2018 study by Privacy International of 34 popular apps showed that at least 61 % of the tested apps automatically shared user data with Facebook. This happened automatically the moment the user started the apps, even if the user did not have a Facebook account. Additionally, some of the apps were observed transmitting detailed and sensitive personal data to Facebook through the Facebook SDK.[325]

According to the Privacy International study, the Facebook SDK was pre-configured to automatically share data with Facebook, before the user was asked to consent to any data sharing in the apps. The observed data transmissions to Facebook also included the Android Advertising ID. This allows Facebook to build incredibly detailed profiles on consumers, regardless of whether the consumer has a Facebook account or not.

---

[322] "Third Party Tracking in the Mobile Ecosystem", Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt https://arxiv.org/abs/1804.03603
[323] "DoubleClick.Net Usage Statistics", BuiltWith https://trends.builtwith.com/ads/DoubleClick.Net
[324] "Third Party Tracking in the Mobile Ecosystem", Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt https://arxiv.org/abs/1804.03603
[325] "Investigating Apps interactions with Facebook on Android", Privacy International https://privacyinternational.org/appdata

# 7 Cascading data sharing through Grindr

As a part of the technical testing, our team observed a number of third party companies receiving personal data from Grindr, including users' IP addresses in combination with the Android Advertising ID and other identifiers, metadata related to sexual preferences, and precise GPS coordinates. The use of the Grindr app is in itself a strong indicator of sexual preferences, as the app is geared toward homosexual, bisexual, and trans people. This means that data transfers that indicate the use of Grindr can be a strong indicator for sexuality, even if data fields explicitly stating sexuality are not being sent.

Because of the particularly sensitive nature of Grindr, and because the data flow contained references to real-time bidding, the independent researcher Zach Edwards was commissioned to audit the app and the third parties that were observed receiving data through Grindr. Due to the complicated nature of this research, this chapter goes into significant detail to accurately capture the technical specifics of what was observed. As with any app data transfers, some transmissions happen on a server-to-server basis, and therefore cannot be observed by a data flow analysis. Whenever a particular data transmission could not be observed directly, this is noted below.

## 7.1 The advertising technology in Grindr

As a part of its free app service, Grindr displays advertising banners in the app. Grindr also lets third party advertisers collect information about its users.[326]

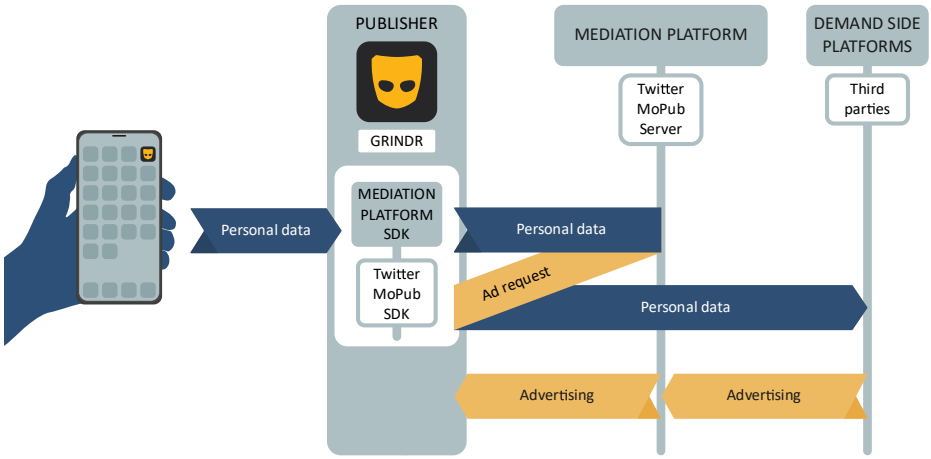
The advertising in Grindr includes targeted behavioural advertising, with some limitations on data use. Users that do not want this have to opt out through the device settings. This is described in Grindr's privacy policy.

> *"Our advertisers also use their own cookies or other tracking technology which may collect information about you within the Grindr Services. We do not control use of these tracking technologies. We prohibit them from tracking or monitoring health information (e.g., HIV status) or certain sexual group identification (e.g., Tribe).*
>
> *[...] Behavioral Advertising Within The Grindr App. If you are using the Grindr Services on an Apple iOS device, you can opt out of behavioral targeting by going into Settings > Privacy > Advertising on your iOS device, or visiting Apple's website for more information. To opt out on an Android device, open the "Google Settings," click on "Ads" and enable "Opt out of interest based ads.""*[327]

[326] Grindr Ads [accessed December 11, 2019] https://www.grindrads.com/index.html
[327] Grindr privacy policy (last updated December 3, 2018) https://www.grindr.com/privacy-policy/

As a part of its advertising system, the Grindr app includes integrated SDKs from a number of adtech companies, including Twitter's MoPub, AdColony, AppsFlyer, Braze, OpenX, Smaato and Vungle. Additionally, the companies AppNexus, Bucksense, and PubNative were observed receiving personal data through Twitter MoPub.[328]

As described in its privacy policy, Grindr uses Twitter's MoPub as an advertising mediation platform. This means that MoPub plays a major role in processing ad transactions that involve other third party companies.

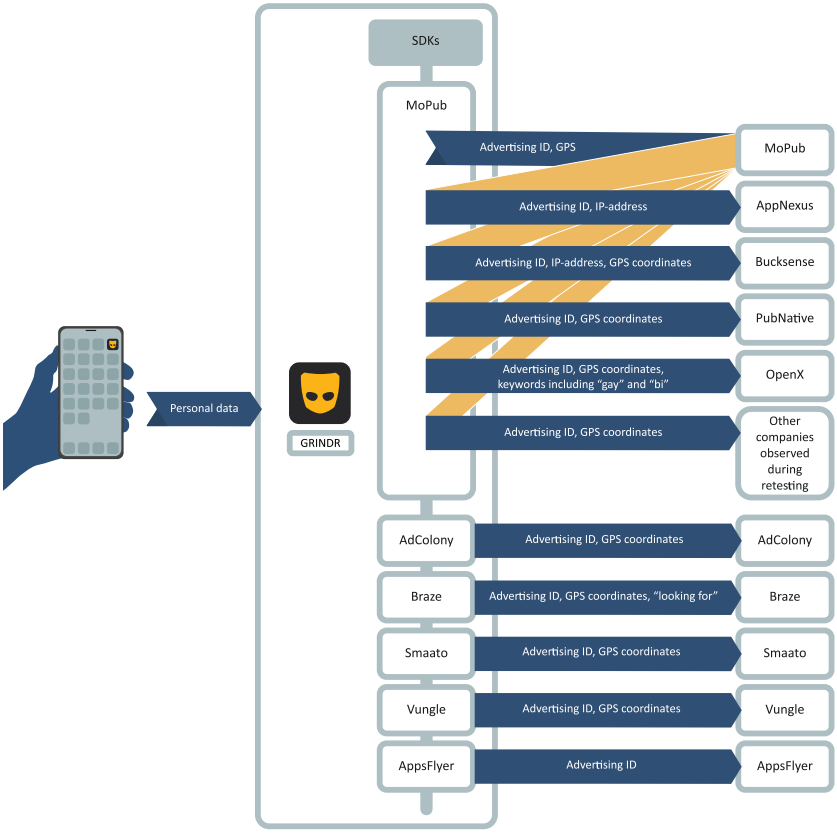



*33 Twitter's MoPub acts as an advertising mediation platform in the Grindr app.*

The technical testing showed MoPub mediating data transmissions to several such third parties. Some of these transmissions included personal data and combinations of persistent unique identifiers. Simultaneously, a number of other third parties were observed receiving personal data directly through their SDK integrations in the Grindr app. These transmissions and the relevant third parties are described below, followed by a problematization of how this system is set up to facilitate the broadcasting of personal data with few or no safeguards.

The below table provides an overview of what data was observed being transmitted to which third parties.

[328] Mnemonic, "Review of communications from apps", chapter 3.2 https://www.forbrukerradet.no/out-of-control/




*34 Overview of sharing of personal data in the Grindr app.*

### 7.1.1 Twitter's MoPub

Twitter's MoPub is a large supply side platform that helps app publishers make money through behavioural advertising. MoPub also acts as a mediation platform that "allows publishers to make ad requests to multiple ad networks".[329] Additionally, MoPub provides "advanced bidding" to increase the app publishers' profits by letting multiple demand side platforms compete with each other.[330]

In 2013, MoPub was acquired by the social media company Twitter. As one of the larger mobile-based marketing platforms, Twitter's MoPub has access to a

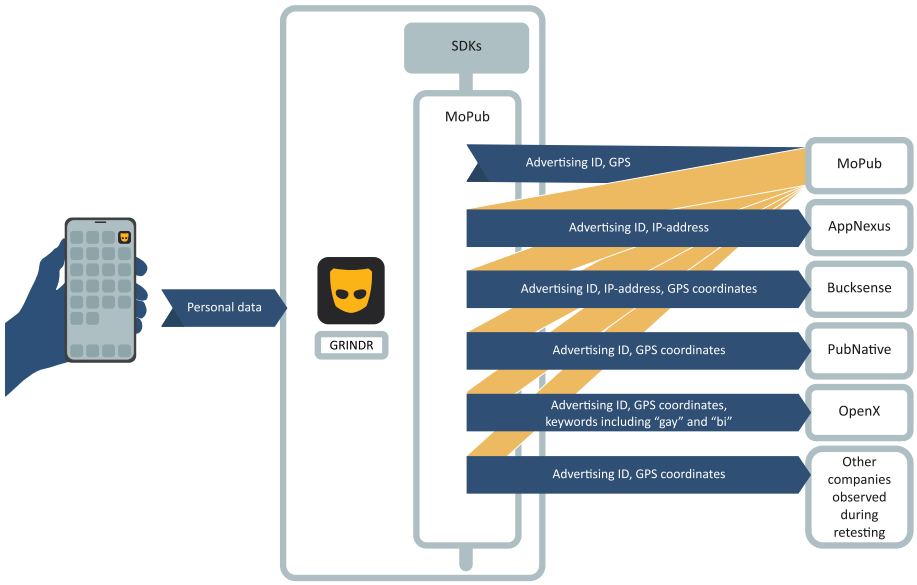
[329] "MoPub Network Mediation", MoPub [accessed December 11, 2019] https://developers.mopub.com/publishers/mediation/mopub-network-mediation/
[330] "MoPub Advanced Bidding", MoPub [accessed December 11, 2019] https://media.mopub.com/media/filer_public/00/a5/00a55497-1774-49d0-ac62-d894477c3b4b/mopubadvancedbidding_pubs.pdf

vast amount of consumers through its marketplace. This data may also be combined with data collected through the Twitter platform.[331]

> *"MoPub Marketplace brings together more than 49,000 apps and 180 DSPs globally, servicing 450 billion monthly app advertisement requests and reaching over 1.5 billion unique devices."*[332]

As a part of its in-app behavioural advertising, Grindr uses Twitter's MoPub as an advertising mediation platform. This means that MoPub is responsible for mediating data transmissions with other third parties, in order to show targeted ads in the app.

During the technical testing of Grindr, Mnemonic observed the Advertising ID, precise GPS coordinates, app name, and age being transmitted to MoPub through MoPub's SDK in the Grindr app. According to the "http referrers" Mnemonic observed, MoPub also triggered a number of requests containing personal data to other third parties , including AppNexus, Bucksense, PubNative, and OpenX.[333]

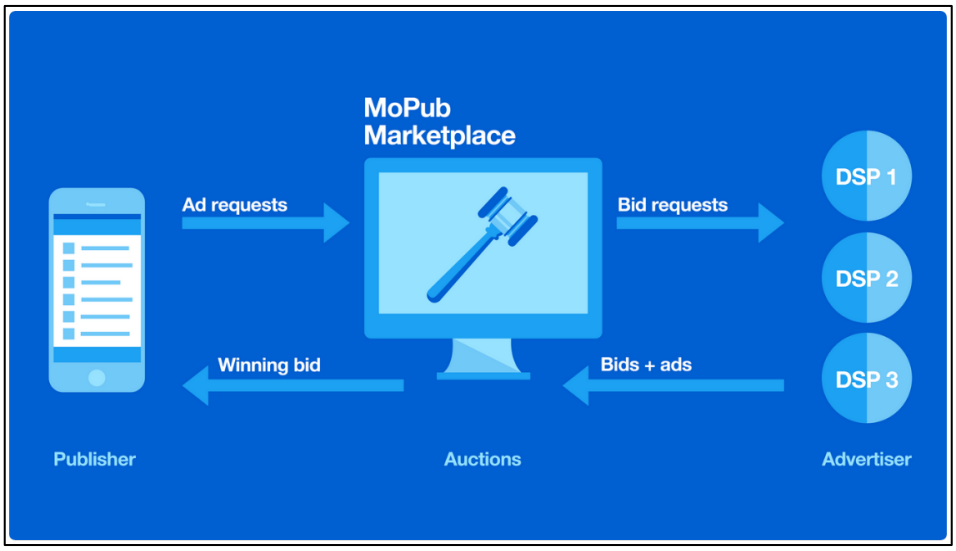



*35 Third parties receiving personal data through Twitter's MoPub mediation.*

[331] "MoPub Is Testing Ways To Do More With Twitter Data", Allison Schiff https://adexchanger.com/mobile/mopub-testing-ways-twitter-data/
[332] "Our History", MoPub [accessed December 11, 2019] https://www.mopub.com/company/history/
[333] The process is described in detail in Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/

Through its role as an advertising mediation party, Twitter's MoPub's SDK sends an ad request to the MoPub server whenever an ad should be placed in the app. Subsequently, MoPub sends data to other advertising third parties.[334] These mediation referrals include information such as Advertising IDs and other identifiers, demographic data such as age and gender, and precise GPS coordinates.

Subsequently, other adtech companies such as AppNexus or OpenX – or MoPub itself – may broadcast this data in the form of bid requests to advertisers and demand side platforms, on a server-to-server basis. The winning bidder displays an ad in the Grindr app, which is loaded in the background or cached for later.




*36 Source: https://www.mopub.com/marketers/marketplace/ [accessed December 11, 2019]*

According to its SDK user documentation, MoPub has set up its SDK to pseudonymize/truncate the IP addresses of EU and EEA-based end users, to protect user privacy in compliance with the GDPR.[335] However, as the technical testing shows, the MoPub SDK was transmitting the full IP address to AppNexus and Bucksense.

Mnemonic was not able to observe from where MoPub gets the phone's IP address. However, the implications of MoPub broadcasting the IP address

[334] The details on how this works is described throughout MoPub's developer documentation. "Maximize revenue for every ad impression.", MoPub [accessed December 11, 2019] https://developers.mopub.com/
[335] "GDPR Publisher Integration Guide", MoPub [accessed December 11, 2019] https://developers.mopub.com/publishers/best-practices/gdpr-guide/

together with the Advertising ID to AppNexus and Bucksense, is that these companies can use the data for cross-device tracking. This is described in detail in chapter 7.2.

In its privacy policy, MoPub states that it collects a lot of different data from apps, including IP address, Advertising ID, GPS coordinates, demographic information, device metadata, and app usage data.

> *"When you use an app that has integrated the MoPub Services, we collect personal data about you. The MoPub Services are designed to avoid collecting information such as your name, address, or email address, but the personal data we collect does enable us to recognize your device over time and across apps. Depending on where you live and your privacy choices, the personal data we collect includes:*
>
> *Device identifiers such as your IP address, iOS Identifier for Advertising (IDFA), Android Advertising ID, or a MoPub-specific identifier.*
>
> *Your precise geo-location, when location services have been enabled for an app on your device that has integrated the MoPub Services. Note that when location services have not been enabled in any of your apps that have integrated the MoPub Services, we will still infer data about your location based on your IP address.*
>
> *Information that a Publisher Partner has collected about you and shared with MoPub, such as demographic information (e.g., your age or gender) or information about your interests, to help make the ads served to you more relevant.*
>
> *Information about your device, such as the type and model, manufacturer, operating system (e.g. iOS or Android), carrier name, mobile browser (e.g., Chrome, Safari), and screen size.*
>
> *Information about your app usage, including the apps on your device that use the MoPub Services and the version of such apps, the app on your device that is requesting an ad, the start/stop time of your app session, your current time zone, and your network connection type (e.g., WiFi, cellular).*
>
> *Information about ads served, viewed, or clicked on, such as the type of ad, where the ad was served, whether you clicked on it, and whether you visited the advertiser's website or downloaded the advertiser's app."*[336]

In Grindr's privacy policy, Grindr states that it shares data with Twitter's MoPub, including the Android Advertising ID, parts of the profile information, "distance information", and demographic information.

> *"We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of*

[336] MoPub privacy policy (last updated August 9, 2018)
https://www.mopub.com/legal/privacy/

> *your demographic information with our advertising partners. These third parties may also collect information directly from you as described in this Privacy Policy through technology such as cookies. The privacy policy of these third party companies applies to their collection, use and disclosure of your information. One of these advertising partners is MoPub that helps Grindr deliver personalized advertising."*[337]

According to MoPub's privacy policy, as a part of its advertising network, it may share user data with *"Data Partners and Advertising Demand Partners to infer what you may be interested in and to serve ads to you based on these inferred interests."* MoPub's list of partners includes more than 160 demand side platforms and/or mediation partners, who are all part of MoPub's partner network.[338] MoPub may share personal data with all of these partners as a part of this system.

> *"We share personal data with Advertising Demand Partners so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you on our mobile advertising exchange and across the broader advertising ecosystem."*[339]

MoPub encourages consumers to read the privacy policies of its more than 160 partners, in order to understand how these may use their personal data. Although MoPub claims to rely on consent in order to process personal data, its partners do not necessarily use consent as a legal basis. This means that if the consumer wants to withdraw their consent from MoPub, the partners may choose not to respect this withdrawal.

> *"MoPub Partners may also have separate legal bases for collecting, using, retaining, and sharing your personal data. For example, some Publisher Partners and Supported Advertising Mediation Partners may mutually agree to process your personal data for personalized advertising purposes on the basis of legitimate interests."*[340]

Mnemonic did not observe transmissions to all of the listed MoPub partners during their testing. However, as described above, the way that advertising mediation works in mobile apps is dynamic. This means that depending on different contexts, such as location of the device and how the app is used, further unique data flow partners could have been triggered.

---

[337] Grindr privacy policy (last updated December 3, 2018) https://www.grindr.com/privacy-policy/
[338] "MoPub partners", MoPub [accessed December 11, 2019] https://www.mopub.com/legal/partners/
[339] MoPub privacy policy (last updated August 9, 2018) https://www.mopub.com/legal/privacy/
[340] Ibid.

The dynamic nature of mobile advertising is illustrated by a number of subsequent findings during Mnemonic's re-testing of Grindr. Mnemonic observed additional data flows to the adtech companies Aarki, Adtelligent, InMobi, InnerActive, Mars Video, and Mobfox during the retesting. These transmissions included the Advertising ID, and both Adtelligent and Mars Video were also observed receiving the IP address. Because these findings occurred late in the testing phase, they are not discussed further in this report.[341]

In its user documentation and privacy policy, MoPub states that it will only process personal data on EU and EEA users on the basis of consent.

> *"If you are located in the European Economic Area, the United Kingdom, or Switzerland, Publisher Partners who would like us to serve you personalized ads must first obtain your consent so that MoPub and our partners can process your personal data for this purpose. Some Publisher Partners may choose to obtain your consent for this purpose even if you are located outside of these regions. If you provide your consent, we will collect, use, share, and otherwise process all of the personal data described above for the purpose of serving you personalized advertising that MoPub and our partners believe is most relevant to you."*[342]

MoPub relies on publishers to obtain consent from the user. This may be implemented by the publisher in a number of different ways.[343] However, if for some reason the consent status of the user is unknown, certain publishers and mediation partners, including Vungle and AdColony, may rely upon legitimate interests to process personal data.[344]

If consumers wish to withdraw their consent, or otherwise stop MoPub from collecting their personal data, they are asked to use their device-level opt out settings.

MoPub reserves the right to share the data that it collects with its partners. Since MoPub has its own purposes for further processing and sharing of the personal data that it collects, it is clearly a controller.

---

[341] Mnemonic, "Review of communications from apps", chapter 3.2.1
https://www.forbrukerradet.no/out-of-control/

[342] MoPub privacy policy (last updated August 9, 2018)
https://www.mopub.com/legal/privacy/

[343] "GDPR Publisher Integration Guide", MoPub [accessed December 11, 2019]
https://developers.mopub.com/publishers/best-practices/gdpr-guide/

[344] "Supported Mediation Partners", MoPub [accessed December 11, 2019]
https://developers.mopub.com/publishers/mediation/supported-mediation-partners/

As shown in chapter 5, Grindr does not give users sufficient information about how data may be shared during the registration process in the app. Furthermore, users are not given any options in the app to limit data sharing. As we will discuss in chapter 8, a controller cannot rely on legitimate interests as a fallback option if it did not have a valid consent. Thus Twitter's MoPub appears to lack a valid legal basis for processing the personal data that it was observed receiving.

### 7.1.2 AppNexus (AT&T)

AppNexus is a major adtech player that was acquired by the US telecom company AT&T in 2018.[345] Before the acquisition, AppNexus claimed to process 6 million queries per second, with more than 11 billion impressions transacted per day.[346] AppNexus, which is part of AT&T's adtech division Xandr, runs both a supply side platform and a demand side platform, meaning that it facilitates parts of the RTB system for a large number of adtech players. The major Norwegian media house Schibsted has been a partner of AppNexus since 2015.[347]

During the technical testing of Grindr, AT&T's AppNexus was observed receiving both the unique Advertising ID and the IP address, and the app name through a mediation referral from MoPub.[348]

As a part of its acquisition of AppNexus, and as a major telecom and TV provider, AT&T can potentially use data collected through AppNexus to sell and target ads to users' IP addresses and Advertising IDs. For example, AT&T can use the data from the online tracking industry in combination with first-party data from its TV boxes, in order further to refine its targeted advertising.[349]

For example, a consumer in the USA might subscribe to AT&T's mobile services, and have an AT&T set-top TV-box that is connected to their home network.

---

[345] "AT&T to Acquire AppNexus", BusinessWire
https://www.businesswire.com/news/home/20180625005372/en/ATT-Acquire-AppNexus

[346] "About AppNexus", AppNexus [accessed December 11, 2019]
https://www.appnexus.com/about

[347] "Schibsted Media Group and AppNexus announce global partnership"
https://schibsted.com/news/schibsted-media-group-and-appnexus-announce-global-partnership/

[348] Mnemonic, "Review of communications from apps", chapter 3.2.1
https://www.forbrukerradet.no/out-of-control/

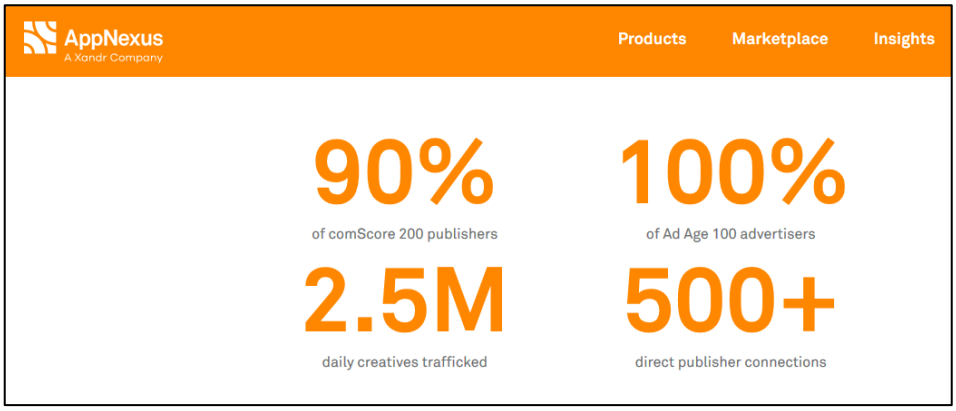
[349] "Turner Using Xandr Data for Targeted Ad Products", Jon Lafayette
https://www.broadcastingcable.com/news/turner-using-xandr-data-for-targeted-ad-products

Through ID syncing, AT&T can merge the information collected through its advertising network AppNexus with the customer data it already has access to through its subscription services and mobile network. This gives both AppNexus and AT&T access to more sophisticated profiles that can be used to target consumers across channels and devices.

> *"[AT&T's adtech division] Xandr has already used AT&T's data to create 30 custom audience segments for advertisers to target audiences on [AT&T's owner] Turner's digital properties. Now it will use those audience segments to target viewers across Community and is in the process of building hundreds more. Additionally, AT&T is able to map all of the devices in a given household in order to target the members of that household with ads running across those various devices.*
>
> *"AT&T's data is really interesting, valuable and differentiating. What you buy (Amazon) and where you go (AT&T) are some of the best signals, and we look forward to leveraging them across Xandr's inventory".*[350]

According to its privacy policy, AppNexus' platform allows buyers and sellers to engage in various forms of targeted and behavioural advertising, and to buy and sell data on consumers.

> *"[...] buyers and sellers and their partners use our Platform to engage in a variety of techniques, including interest-based advertising, real-time (or programmatic) advertising, contextual, and location-based advertising.*
>
> *[...] Buyers, sellers, and other companies may also use our Platform to buy and sell data to help make the ads that end users see more relevant."*[351]




*37 Source: https://www.appnexus.com/marketplace [accessed December 11, 2019]*

[350] "With video ad marketplace Community, AT&T's Xandr expands inventory", Tim Peterson https://digiday.com/marketing/video-ad-marketplace-community-atts-xandr-expands-inventory/

[351] AppNexus privacy policy (last updated October 24, 2019) https://www.appnexus.com/platform-privacy-policy#infocollect

AppNexus explains that it collects a number of different data points, including GPS coordinates, IP addresses, Advertising ID, other identifiers, activity data, interest data, and more. However, it claims that this cannot identify an individual in the "real world", because it does not include a name or email address.

> *""Personal Data" is defined as any data relating to a living individual who can be identified directly from that data, or indirectly in conjunction with other information. It can take the form of a name or address, and can extend to unique identifiers, IP addresses and other identifiers which do not tell us who an Internet user is in the "real world" but may, when combined with other information, allow the identification of a living individual.*
>
> *We do not collect personal data that identifies you as an individual in the "real world." When you (an Internet user) visit a Digital Property that has integrated our technology or that use technology that integrates with our Platform, we do not know your name or email address or other information that directly identifies you. We take care to ensure that we do not collect any information that tells us who you are."*[352]

Its privacy policy also states that AppNexus may, upon instructions from its clients, share data with third party providers.

> *"[…] so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you using their data and our and our partners' technology", "so that certain of them can create demographic and interest profiles to help our clients choose the best ad for you using our and our partners' technology", and "so that they can improve their products and services for use by us and others across the broader online advertising ecosystem".*[353]

AppNexus' list of third party providers includes more than 4000 companies. This list includes bidders, real time data providers, and other third party providers.[354]

The AppNexus privacy policy goes on to state that it uses data collected through its platform both as an independent controller and as a processor. It claims to have a legitimate interest to process personal data in most cases.

> *"We normally rely on our legitimate interests to collect and use personal data, except where our interests are overridden by your data protection interests or fundamental rights and freedoms. Our legitimate interests are*

[352] Ibid.
[353] Ibid.
[354] "Third Party Providers", AppNexus [accessed 12 November, 2019] https://www.appnexus.com/third-party-providers

> *described in more detail below (see "How do we use the information we collect") and include the operation of our Platform and business and the provision of our online advertising technology services to our clients as required by our agreements with them. In some cases, we may rely on your consent which is obtained for us by the operator of the Digital Properties that use our technology or use technology that interacts with our Platform."*[355]

According to AppNexus' privacy policy, consumers may opt out of location data tracking by changing their device settings or by not giving apps access to location data. However, AppNexus will still infer location based on IP address if the consumer disables location services.

> *"Most mobile devices offer you the ability to stop the collection of location information at any time by changing the preferences on your device. You may also be able to stop the collection of location information by particular apps by adjusting the settings for individual apps or following the standard uninstall process to remove specific mobile apps from your device. Note when location services have not been enabled in any of your apps, we will still infer data about your location based on your IP address."*[356]

If a Grindr user wants to opt out of AppNexus' collecting their personal data, they would first have to go through MoPub's list of 160+ partners. Then they would have to guess that AppNexus was one of those partners actually receiving personal data. Then they could opt out of certain tracking from AppNexus, but as AppNexus own partners may have different legal bases for processing personal data, this means that those partners may choose not to respect an opt out choice. Thus the consumer would have to track down each of those partners, and so on. This is clearly an impossible task for anyone, illustrating the lack of consumer control when data is being shared widely across the adtech industry.

Because AppNexus uses the data that it collects for its own purposes, such as sharing the data with other third party providers, it can be considered a controller. As established above, the Advertising ID and IP address are both personal data, and allows for persistent tracking of individuals over time. Although AppNexus uses a distinction between personal data and "real world" data, as we have shown in this report, this is not a meaningful distinction, because unique device identifiers can be tied to real individuals.

---

[355] AppNexus privacy policy (last updated October 24, 2019) https://www.appnexus.com/platform-privacy-policy

[356] Ibid.

As demonstrated in chapter 5, Grindr did not obtain a valid consent for sharing data with third parties. AppNexus' persistent tracking of users across devices and services means that its legitimate interest to provide targeted advertising is unlikely to outweigh the fundamental rights and freedoms of the data subject. Thus AppNexus appears to lack a legal basis for processing the personal data that it was observed receiving.

### 7.1.3 Bucksense

Bucksense is an adtech company that provides a white label advertising service for publishers. Bucksense is owned by the Heritage Group (75 %) and the Italian telecommunications company Acotel Group (25 %).[357] It claims to be the "programmatic ad platform of choice" for more than 350 brands worldwide, including Adidas, Visa, Disney, and Huawei.

Bucksense owns the advertising platform Directopub, which it claims offers "access to 1.8+ billion daily users" and allows marketers to "target 5,000+ data audiences".[358] The Directopub platform allows marketers to target campaigns at specific audience segments. Its promise is *"It is a known fact that no matter how good your ad is, it will be ineffective if placed in the wrong context. Our platform allows you to cherry pick where, to whom, and when show your ad to perform at its best."*[359]

The technical test of Grindr showed Bucksense receiving the app name, the Advertising ID, IP address, and GPS coordinates through a mediation referral from MoPub.[360]

Bucksense has an official partnership with Grindr, with the latter using the Bucksense platform Directopub as its white label platform solution to provide a direct ad buying and real-time bidding interface for the app.[361]

---

[357] "Heritage Group invests in Programmatic and acquires 75% of the shares in Bucksense", Andrea Di Domenico (machine translated from Italian) https://translate.google.com/translate?hl=&sl=it&tl=en&u=https%3A%2F%2Fwww.programmatic-italia.com%2Fheritage-group-acquisisce-75-bucksense%2F

[358] "The RTB Platform for Agile Marketers", Bucksense [accessed December 11, 2019] https://www.bucksense.com/landing/lp5/?kw=rtb

[359] "From ordinary to extraordinary ads with enhanced features and effective placements.", Bucksense [accessed December 11, 2019] https://www.directopub.com/formats/

[360] Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/

[361] "The RTB Platform for Agile Marketers", Bucksense [accessed December 11, 2019] https://www.bucksense.com/landing/lp5/?kw=rtb

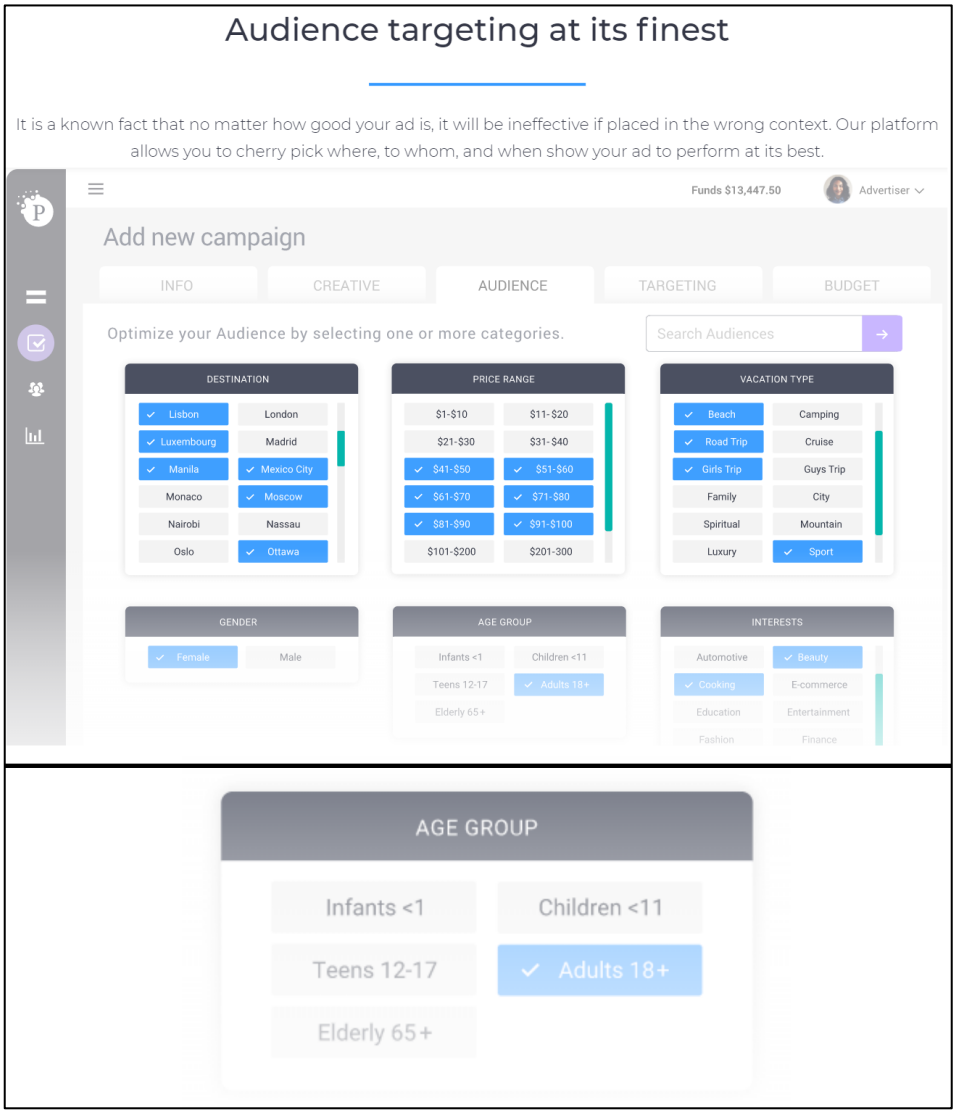
According to a press release, Grindr uses the Bucksense Directopub platform to provide "advertisers direct access to the enormous spending power of the LGBTQ+ community" and to "enable small, LGBTQ-owned businesses with limited budgets to directly reach their community".[362]

MoPub is one of the advertising networks that advertisers can add through the Bucksense Directopub platform.[363] This works by Grindr advertising partners uploading banner ads into Grindr's Bucksense-powered self-service page for advertisers.[364] These ads then flow through MoPub when the self-service bids were either chosen to win, or had the highest bid for a user.

On MoPub's website, Bucksense is listed as an Advertising Demand Partner, meaning *"companies that advertisers work with to bid on ad inventory through the MoPub advertising exchange and to serve the ad that is most relevant to you"*.[365]

The Bucksense Directopub platform allows ad targeting to any age group, likely with full control given to the publisher. As shown below, a screenshot from the company shows targeting possibilities towards children and infants. Its "teens" age group includes 12 year olds.[366] As we do not have access to the Directopub platform, we cannot confirm how this targeting works in practice.

[362] "Grindr, in Partnership with Bucksense, Launches Self-Service Advertising Product", Bucksense https://www.businesswire.com/news/home/20180829005147/en/Grindr-Partnership-Bucksense-Launches-Self-Service-Advertising-Product
[363] "How to add a campaign", Bucksense [accessed December 11, 2019] https://howto.bucksense.com/how-to-add-a-campaign/
[364] "Self Service", Grindr [accessed December 11, 2019] https://selfservice.grindr.com/login
[365] "MoPub Partners", MoPub [accessed December 11, 2019] https://www.mopub.com/legal/partners/
[366] In the US, children under 13 are protected by COPPA. In the EU, children are afforded special protections under the GDPR.




*38 Source: https://directopub.com/platform/ [accessed 29 November, 2019]*

In its end user privacy policy, Bucksense describes how it receives data when a consumer receives or clicks an ad, either from the consumer's device, from ad exchanges, from other third parties, or from publishers.

> *"Bucksense serves advertisements to end users of various publishers (such as website operators or mobile app developers), via real-time marketplace platforms exchanges ("Exchanges") and/or such publishers. Those ads are provided by advertisers, who use Platform to serve their ads and manage the overall performance of their ad campaigns, including by using third party services that integrate with our Platform. When an end user receives or clicks on an ad, we might receive or collect some or all of the data provided below, whether from the end user's device, from the relevant Exchange/s, from third parties and/or publishers ("Data").*"[367]

[367] "Bucksense Ad Platform Privacy Policy", Bucksense (not dated, last accessed November 22, 2019) https://www.bucksense.com/platform-privacy-policy/

According to the Bucksense privacy policy, it collects personal data, including the IP addresses, Advertising ID, and GPS coordinates, from a variety of sources in order to deliver behavioural advertising. All this information may be shared with clients, vendors, and "other companies". Bucksense also collects data from multiple sources and combine them, in order to create audience segments.

> *"The Bucksense Services collect information about your device and the ads that we deliver onto your device. This data, which is collected passively using various technologies may come from such sources as your web browser or the apps that you use. We also may obtain the precise location (e.g., lat/long coordinates) of your device and may use that information to deliver targeted ads. We may also combine the information collected across multiple sites and mobile apps in order to create interest segments that help us target future advertisements based upon those inferred interests. This practice is sometimes referred to as behavioral advertising or interest-based advertising*
>
> *[...] We may share this information with clients, vendors, and other companies that we conduct business with as permitted by law.*
>
> *When we present an ad on your device we might receive or collect some or all of the following:*
>
> *Which application will present the ad*
>
> *If you clicked the ad and when*
>
> *IP address*
>
> *User Agent*
>
> *Carrier where applicable*
>
> *General location (i.e. city or zipcode)*
>
> *Android advertising ID or Apple advertising ID (IDFA) as applicable""*[368]

However, Bucksense says that it does not collect personal information, because it does not receive information such as addresses or telephone numbers.

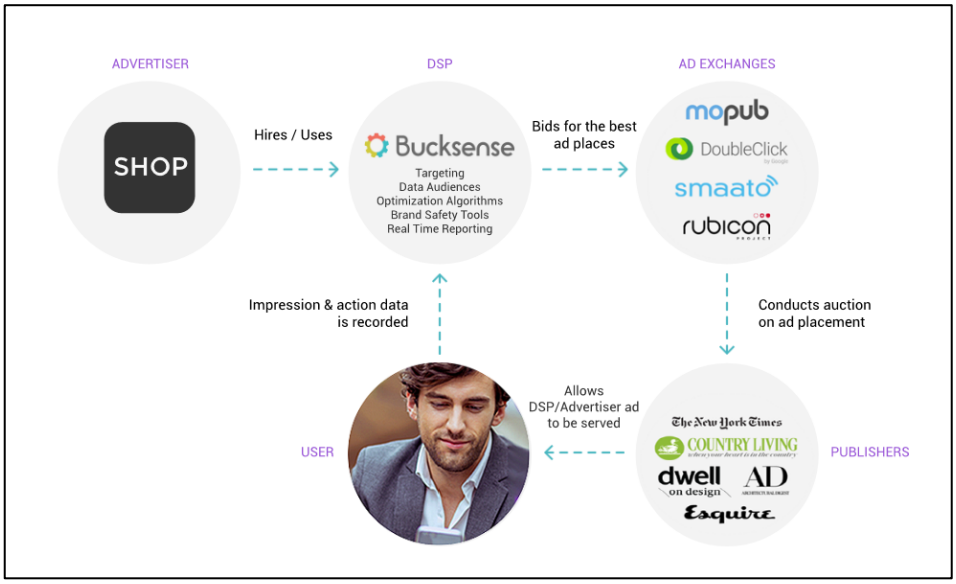
> *"We generally do not collect or use personal information about individual users through the Bucksense Service. When we say "Personal Information", we mean individually identifiable information that would allow us to determine the actual identity of and/or directly contact a specific living person, such as an email address or telephone number."*[369]

[368] Ibid.
[369] Ibid.

Bucskense goes on to state that its clients and partners may use the data it collects, including unique identifiers in combination with IP addresses, to track consumers across devices and services.

> *"Our clients or partners may use the above technologies (sometimes, in combination with each other or other data such as IP addresses or hashed or de-identified data files) to coordinate identifiers across platforms, browsers, or devices, in order to more efficiently analyze or target advertising."*[370]

On its website, Bucksense lists more than 70 *"supply, data, and tracking partners"* who *"provide our clients with access to 2+ Billion potential customers daily."*[371] This list includes MoPub, OpenX, PubNative, and Smaato. Bucksense also provides access to data from a number of data brokers.[372]




*39 Source: https://www.bucksense.com/marketplaces/#openRTB [accessed December 11, 2019]*

It is not clear from its privacy policy which legal basis Bucksense uses for processing personal data, but it is implied that it relies on consent.

> *"Our use of such information is governed by this privacy policy, and the end users' consent and preferences as conveyed to us by such end users, by publishers and by other third parties."*[373]

[370] Ibid.
[371] Bucksense Partners", Bucksense [accessed December 11, 2019] https://www.bucksense.com/about-us/#ourPartners
[372] "About us", Bucksense [accessed December 11, 2019] https://www.bucksense.com/about-us/
[373] "Bucksense Ad Platform Privacy Policy", Bucksense (not dated, last accessed November 22, 2019) https://www.bucksense.com/platform-privacy-policy/

Although Bucksense claims not to collect personal information, the definition of personal information that it is operating with is not consistent with the legal definition provided by the GDPR. As Bucksense clearly is processing personal data, and using data for its own purposes by sharing data with other partners, it is a controller. Therefore, it must have a valid legal basis for processing the personal data.

As demonstrated in chapter 5, Grindr did not collect a legally valid consent from the user upon registration. Bucksense's own version of consent seems to be based on the possibility to opt out through device settings, which is not compliant with the GDPR. Therefore, Bucksense appears to be lacking a valid legal basis to process the personal data that it was observed receiving.

### 7.1.4 OpenX

The California-based adtech company OpenX is mainly a supply side platform[374] and ad exchange.[375] It claims to reach more than 240 million consumers in the US alone on a monthly basis, and record 4.5 trillion "data events" every day. It also boasts of having more than 2500 supply partners, and works with more than 30 000 advertisers.[376]

During the technical testing of Grindr, OpenX was observed receiving the Advertising ID, GPS coordinates, app name, and a number of keywords including "gay" and "bi" through a mediation referral from Twitter MoPub. OpenX was also observed receiving data via its own SDK, which was directly integrated into the Grindr app.[377]

Beyond the fact that OpenX receives personal data on users of the Grindr app, keywords such as "gay" and "bi" are can be appended to user profiles owned by OpenX. OpenX may then identify those users in other apps and websites, and allow its partners to bid on these in ad campaigns.

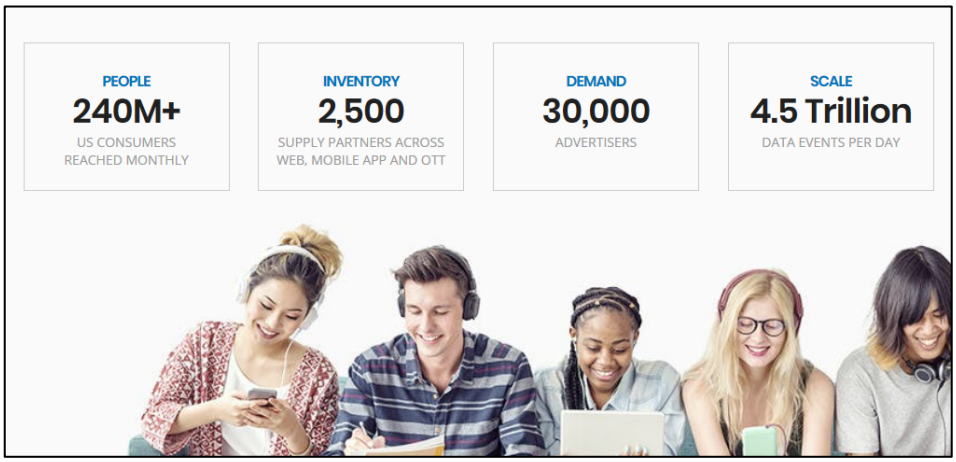
These data transmissions were accompanied by a user data request referring to the OpenRTB system.[378] Such user data requests are used to negotiate bid

[374] "SSPs like OpenX are eyeing direct ties to advertisers", Seb Joseph https://digiday.com/marketing/ssps-like-openx-eyeing-direct-ties-advertisers/
[375] "Driving Superior Monetization", OpenX [accessed December 11, 2019] https://www.openx.com/publishers/
[376] OpenX [accessed December 11, 2019] https://www.openx.com/uk_en
[377] Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/
[378] The observed user data request was similar to mobile ad requests shown in OpenX's own RTB documentation. "OpenRTB ad request parameters", OpenX [accessed

prices, which allows advertisers and DSPs to set the price to showing an ad to a particular individual in a particular context. In other words, this shows that OpenX is telling marketers how much the individual is worth. In addition to the ad bidding process, this data may be used for future OpenRTB advertising optimizations and for data collection for other purposes. However, OpenX's actual real-time bidding processes happen out of the scope of what Mnemonic was able to observe in the data flow analysis.

According to a 2016 OpenX whitepaper on its partnership with Grindr, OpenX provided more than 1 billion ad impressions in Grindr during 2015-2016.[379]

Through its ad exchange, OpenX has direct relationships with more than 50 000 apps, which it facilitates real-time bidding for in order to allow advertisers to show targeted ads.[380] Through this system, OpenX claims to facilitate more than 60 billion bids per day.




*40 Source: https://www.openx.com/ [accessed December 11, 2019]*

According to its own documentation of its OpenRTB implementation, OpenX recommends app vendors to transmit the Advertising ID, GPS coordinates, gender, and a lot of other data as a part of the RTB process.[381] The personal

December 11, 2019]
https://docs.openx.com/Content/developers/ad_request_api/openrtb_parameters.html

[379] "Grindr Leverages OpenX to Increase Competition for their Inventory and Drive Value", OpenX [accessed December 11, 2019] http://welcome.openx.com/rs/745-BUQ-779/images/OpenXCaseStudy_Grindr.pdf

[380] "OpenX Ad Exchange", OpenX [accessed December 11, 2019] https://www.openx.com/uk_en/demand-partners/adexchange/

[381] "OpenRTB ad request parameters", OpenX [accessed December 11, 2019] https://docs.openx.com/Content/developers/ad_request_api/openrtb_parameters.html

data OpenX was observed to receive through its Grindr and MoPub integrations may be appended to existing user profiles and used for future targeting, although this could not be observed through Mnemonic's data flow analysis.

According to its privacy policy, OpenX may collect a number of different data points about consumers, including demographic data, device data, unique identifiers, geolocation, inferred interests and behaviour, and data gathered from cross-device tracking.

> *"'Free form' demographic information (e.g. age, gender, marital status)*
>
> *Browser information (e.g. URL, browser type, 'click through' data)*
>
> *Ad reporting or delivery data (e.g. size/type of ad, ad impressions, location/format of ad, data about interactions with the ad)*
>
> *Device-type information (e.g. screen dimensions, device brand and model)*
>
> *Unique identification numbers (e.g. IP address and mobile/cell phone device ID)*
>
> *Location data (as derived from IP address or GPS (for mobile))*
>
> *Interest segments (i.e. inferred information on the behavior or likely interests associated with a device)*
>
> *Retargeting data (i.e. data revealing previous interest in a product or website)*
>
> *Information about the possible relationships among different browsers and devices*
>
> *Information about your activities on our website and Services"*[382]

Even if the consumer opts out of OpenX tracking and collecting personal data, other third party advertisers and ad networks that are part of OpenX's ad exchange may use different legal bases for processing personal data. Therefore, OpenX recommends that the consumer reads the privacy policies of all these third parties, without specifying who the third parties are.

> *"Third-party advertisers and ad networks that participate in the OpenX Ad Exchange may also use their own cookies and other ad service technologies to display and track their ads. We do not control and are not responsible for such third-party advertisers' and ad networks' information practices or their use of cookies and other ad service technologies. To learn more about the practices of these companies, please read their privacy policies."*

[382] OpenX privacy policy (last updated May 25, 2018)
https://www.openx.com/legal/privacy-policy/

Although we were not able to locate a list of OpenX's third party partners online, OpenX claims on its website that its RTB marketplace includes more than 1200 publishers, 34 000 advertisers, and more than 400 buyers, generating more than 60 billion bids every day.

> *"OpenX pioneered the Real Time Bidding Advertiser Marketplace and currently provide 1,200+ publishers and 900+ premium mobile publishers access to the budgets from 34K+ advertisers and 400+ Buyers. The OpenX Ad Exchange generates 60B+ bids per day across 190 countries."*[383]

The OpenX privacy policy goes on to state that its data collection is sometimes reliant on consent, but it also claims to have a legitimate interest for its processing of personal data. It does not specify when which legal basis applies.

> *"On certain occasions, OpenX relies on the consent of the individual to process personal information (for example, when the user inputs personal information into the OpenX website). On other occasions, OpenX may process personal information when OpenX needs to do this to fulfill a contract or where OpenX is required to do so by law.*
>
> *OpenX may also process data when it is in OpenX's or its customer's legitimate interests to do this and when these interests are not overridden by the individual's data protection rights (which may vary based on an individual's jurisdiction). Those legitimate interests include improving OpenX's Services."*[384]

Furthermore, OpenX states that it may act as both a controller and data processor regarding the personal data that it collects.

> *"For EEA individuals, the data controller in respect of your personal information is OpenX Ltd.*
>
> *As set out above, Publishers may use the Services to process data that they collect for their own purposes. In this respect we act as data processor for the Publisher, which may have its own Privacy Policy, which explains how it uses personal information."*[385]

If consumers wish to opt out of this collection and use of data, they have to download an app or use their device settings to restrict data sharing. As OpenX tracks users across different devices and browsers, the consumer has to do this on every device if they truly wish to opt out.

> *"Opting Out for Mobile Application Data: To opt out of OpenX's collection, use, and transfer of data for interest-based advertising on mobile apps,*

[383] "OpenX Ad Exchange", OpenX [accessed December 11, 2019] https://www.openx.com/publishers/adexchange/
[384] OpenX privacy policy (last updated May 25, 2018) https://www.openx.com/legal/privacy-policy/
[385] Ibid.

> *you may download the DAA's AppChoices application from the Android or iOS app store on your mobile device. Users outside the United States may not have access to this application; instead, you can use "Limit Ad Tracking" in your iOS settings or "Opt out of interest-based ads" in your Android settings to limit OpenX's collection of data for interest-based advertising.*
>
> *Opting Out for Location Data: You may opt out of our collection, use, and transfer of precise location data by using the location services controls in your mobile device's settings.*
>
> *Effect of Opting Out: If you use a different device or browser, or erase cookies from your browser, you will need to renew your opt-out choice."*[386]

As documented in chapter 5, Grindr does not provide information or valid consent mechanisms that would give OpenX a valid legal consent to process personal data. Furthermore, the extensive sharing and cross-device tracking that OpenX describes, and the vague description of its legitimate interests, indicates that the data subject's fundamental rights and freedoms will outweigh the legitimate interests of OpenX to provide targeted advertising, share data with other third parties, and improving its services. Consequently, it seems like OpenX lacks a valid legal basis to process the personal data that it was observed receiving.

### 7.1.5 PubNative

The German adtech company PubNative is a mobile supply side platform and ad exchange. It helps publishers market ad space in apps and facilitate targeted advertising.[387]

During the technical testing of Grindr, PubNative was observed receiving the Advertising ID, GPS coordinates and appname through a mediation referral from MoPub.[388]

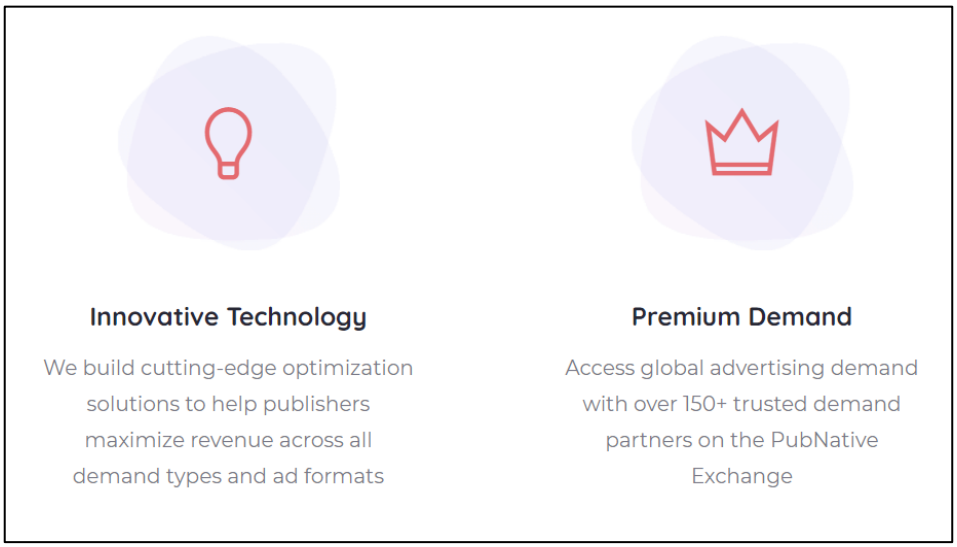
On its website, PubNative describes how its ad exchange HyBid lets demand partners access every ad impression in apps. Although it does not list its partners on its website, PubNative claims to work with more than 150 demand partners.

---

[386] Ibid.
[387] "Leading Mobile SSP PubNative Acquired by Major Media and Gaming Investment Firm – MGI", PubNative [accessed December 11, 2019] https://pubnative.net/blog/pubnative-acquired-by-mgi/
[388] Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/

> *"HyBid allows publishers to increase revenue and reach more potential buyers by making each impression available to multiple demand partners – including direct demand, simultaneously. Our low-latency S2S integration requires minimal development resources and provides a lightweight solution to eliminate latency and improve user experience."*[389]

Other than this, PubNative does not provide much information about its practices on its website, asking potential clients to request an invitation to receive more information.[390]




*41 Source: https://pubnative.net/#home [accessed November 29, 2019]*

In its privacy policy, PubNative explains that it may receive various types of data from publishers, including Advertising IDs, user interactions within apps, device metadata, and user information including gender, age and interests.

> *"Data we receive from Publishers differ. We typically receive: mobile identifiers such as the ID for Advertising for iOS (IDFA), Google Advertising ID device information (device model, platform, operating system version, browser details). However, from time to time the Publishers may also provide data to us, which typically relates to the behavior of users inside the Publisher's apps and may include: user interactions within an app (e.g. in-app purchases, registration) user information such as age, gender, interests."*

[389] PubNative [accessed December 11, 2019] https://pubnative.net/#home
[390] However, they provide documentation for developers, including how to integrate PubNative as a custom ad network through MoPub. "Documentation", PubNative [accessed December 11, 2019] https://developers.pubnative.net/

The PubNative privacy policy goes on to state that the company may share personal data with further third parties, although these third parties are not named.

> *"In the context of the serving of ads, data are exchanged between PubNative and partner advertisers on the bid request level (to get an ad) or in aggregated form for reporting and fraud analysis. This might include the following information on the bid request level:*
>
> *· device information (device model, platform, operating system version, browser details)*
>
> *· targeting information (county, city, hyperlocation when allowed to be collected)*
>
> *· user information (such as device ID, hashed device ID, age, gender and interests, when allowed to be collected)."*

According to PubNative's privacy policy, it only processes personal data based on consent, which is collected by its customers (in this case Grindr). This means that PubNative claims to be a data processor on behalf of the publisher.

> *"We process the data received from Publishers on behalf of the Publishers*
>
> *[…] The collection and processing of usage data by the mobile app Publishers are controlled by and the exclusive responsibility of the respective Publishers. PubNative processes these data for and on behalf of the Publishers in the first place."*[391]

PubNative lists its purposes for processing data in its privacy policy.

> *"Our processing activities include the following:*
>
> *Serving ads to the users*
>
> *Serving ads to the users taking into account their approximate location when permitted by the user's device*
>
> *Serving ads to the users taking into account their age, gender, keywords or interests when provided by the user in the host mobile app on the user's device. Race, religion, politics, sex life, or health are unavailable targeting criterions in PubNative's Technology"*[392]

PubNative also seems to use the data it collects to optimize its own technologies.

> *"The data processing described in this privacy policy serves to market ad space for targeted in-app advertising and targeting campaigns and implement ad campaigns for the customers of PubNative. As such, data*

[391] PubNative privacy policy (last updated July 2018) https://pubnative.net/privacy-notice/
[392] Ibid.

> *are only processed on the basis of users' consent as part of customer instructions. Insofar as data from PubNative are processed for purposes of billing, abuse monitoring or fraud prevention, error correction and for optimizing PubNative's Technology, this is done on the basis of PubNative's legitimate interests. The legal basis in this respect is Art. 6 (1) (f) GDPR. The interests of users are protected by the exclusively pseudonymous processing and the opt-out option described below."*[393]

Although PubNative claims to be a processor on behalf of the publisher, its privacy policy seems to indicate that it may also use the data for its own purposes. Therefore, PubNative may be considered controllers in its own right, which means that it has a responsibility to make sure that it has a legal basis for processing personal data.

As the Grindr app does not collect consent from the user in a legally compliant way, PubNative needs to obtain consent in another way. In one use case, we observed a PubNative consent popup in Grindr. However, this popup was not observed by other testers using different devices, indicating that this consent prompt is not universal.[394] In its privacy policy, PubNative states that users can opt out through their device settings.

There is no way for the Grindr user to know that PubNative is receiving their personal data, nor to know that PubNative may be sharing this data with further third parties. This makes it questionable whether PubNative has a valid legal basis for processing the personal data that it was observed receiving.

### 7.1.6 Vungle

Vungle is a San Francisco-based third party vendor specializing in mobile advertising. It runs a mobile supply side platform that helps 60 000 apps to make money through advertising, and provides demand side functionalities for marketers. In July 2019, Vungle was acquired by the private equity firm Blackstone for $750 million.[395] Vungle also runs its own advertising network, promising *"we'll show your users the right ads at the right time, increasing conversions and earning more for every ad."*[396]

---

[393] Ibid.

[394] The popup was observed on an Android device in Austria in November 2019. It was not observed on any of the Norwegian devices used for testing.

[395] "Sources: Blackstone will buy mobile video ad firm Vungle for $750 million; founder lawsuit settled", Dean Takahashi https://venturebeat.com/2019/07/15/sources-blackstone-will-buy-mobile-video-ad-firm-vungle-for-750-million-lawsuit-settled-with-founder/

[396] "Monetize", Vungle [accessed December 11, 2019] https://vungle.com/monetize/

The company also runs advertising campaigns for brands, which are mostly data-driven. This includes showing "data-optimized ads" on more than 1 billion unique devices.[397]

> *"Make your money work harder and connect with the users that matter to minimize waste and maximize returns.*
>
> *Our powerful platform is packed with tracking features that keep you in the loop and ahead of the game."*[398]

During the technical tests, Mnemonic observed Vungle receiving GPS coordinates from both Perfect365 and Grindr. Vungle also received the Advertising ID and various device configuration parameters from Grindr, through their SDK integration. [399] In the transmissions from Perfect365, Vungle appeared to show that it did not necessarily have consent to collect this information, as the data transmission included the line "consent_status=unknown".[400]


*42 https://vungle.com/creative-labs/ [accessed December 11, 2019]*

[397] "Blackstone Closes Acquisition of Vungle, a Leading Mobile Performance Marketing Platform", Blackstone https://www.blackstone.com/media/press-releases/article/blackstone-closes-acquisition-of-vungle-a-leading-mobile-performance-marketing-platform

[398] "Advertise", Vungle [accessed December 11, 2019] https://vungle.com/advertise/

[399] Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/

[400] Mnemonic, "Review of communications from apps", chapter 3.2.1 https://www.forbrukerradet.no/out-of-control/

Vungle's privacy policy describes how it collects a significant amount of personal data from apps where the Vungle SDK is integrated, including IP addresses and unique identifiers. However, Vungle claims that none of this can directly identify end users.

> *"When you visit an app that uses Vungle technology, we use and deploy "tracking technologies" (see Section 2.3, below) to automatically collect certain information about your device. Some of this information (including for example, your IP address and certain unique identifiers), may identify a particular computer or device and may be "personal data" in some jurisdictions, including the EU. We collect this information the first time Vungle's SDK is initialized on a Publisher Client's app. Note, however, that Vungle's Ad Services do not collect any information that that enables us to identify End Users personally (such as your name, address, or email address)."*[401]

Vungle also combines the personal data it collects from apps with data from other publishers and third parties. It uses this data to perform ID syncing, to match user identifiers in order to combine profiles across companies to combine profiles and identifiers across services.

> *"We may also combine, merge, and/or enhance the information we collect about your device, including the personal data, with information we may collect about your interactions with other Publisher Client's Apps and ads served through Vungle's Platform, or with information collected from our Clients and third parties (such as data providers). This may include, for example, mobile device IDs, demographic or interest data, and content viewed or actions taken on an app to help make the ads served to you more relevant while limiting your exposure to less relevant ads. We (or our third party partners) may also use this additional information to undertake "user matching," which means that in addition to the ID an End User has been assigned in our system, we may also receive a list of unique IDs our external partners or Clients have assigned to an End User."*[402]

The privacy policy goes on to state that Vungle may share the personal data it collects with a number of different categories of third parties, including advertisers, attribution partners, third party vendors, Vungle affiliates, and website advertising partners.

If Vungle wants to share personal data with third parties *outside of these categories*, it claims that it will ask for consent. Vungle does not provide an extensive list of who these third parties are, but its Partner-page lists AppsFlyer,

---

[401] Vungle privacy policy (last updated July 26, 2018) https://vungle.com/privacy/
[402] Ibid.

Adjust, Branch, Kochava, Singular, and Tenjin as "mobile attribution and analytics" partners.[403]

In its privacy policy, Vungle claims to use legitimate interests as the legal basis for most of its processing:

> *"we normally rely on our legitimate interest to collect personal information from you, except where such interests are overridden by your data protection interests or fundamental rights and freedoms."* [404]

Vungle also relies on consent for processing personal data in some cases.

> *"In some cases, we may rely on our consent or have a legal obligation to collect personal information from you, or may otherwise need the personal information to protect your vital interests or those of another person. If we rely on consent to collect and/or process your personal information, we will obtain such consent in compliance with applicable laws."*[405]

According to its own SDK user documentation on GDPR implementation, Vungle recommends that publishers (e.g. app providers) use their own consent mechanisms and pass the users' choice on to Vungle, rather than having Vungle ask the user for consent.

> *"Option 1 (recommended): Publisher controls the GDPR consent process at the user level, then communicates the user's choice to Vungle. To do this, developers can collect the user's consent using their own mechanism, and then use Vungle APIs to update or query the user's consent status. Refer to the GDPR Recommended Implementation Instructions section for details.*
>
> *Option 2: Allow Vungle to handle the requirements. Vungle will display a consent dialog before playing an ad for a European user, and will remember the user's consent or rejection for subsequent ads."* [406]

Since Vungle appears to use the data it collects for its own purposes, it may be considered a controller. Therefore, Vungle is responsible for making sure that the personal data it processes was collected in a legally compliant manner. As Grindr did not collect consent in a compliant way, Vungle seems to be lacking a valid legal basis for processing the personal data that it was observed receiving.

---

[403] "Partners", Vungle [accessed December 11, 2019] https://vungle.com/partners/
[404] Vungle privacy policy (last updated July 26, 2018) https://vungle.com/privacy/
[405] Ibid.
[406] "GDPR Recommended Implementation Instructions", Vungle [accessed December 11, 2019] https://support.vungle.com/hc/en-us/articles/360002925791#gdpr-recommended-implementation-instructions-0-27

In addition to Vungle receiving personal data directly from Grindr, its support documentation shows that the company encourages a number of questionable practices that allow for additional data sharing and collection.

In order to restrict the collection of unwanted data, third party vendors can set up filters that prevents certain data fields from being passed. For example, an adtech company may decide to filter out any data about consumers' sexual orientation, because it considers sensitive personal data a liability. As noted above, MoPub claims to truncate IP addresses as part of its GDPR implementation. However, the technical testing seems to contradict this, as MoPub was still transmitting complete IP addresses to AppNexus and Bucksense through mediation referrals.

Attempts to filter certain categories or fields of data are not watertight. There are ways for companies to get around restrictions on what data can be sent or received. For example, Google's AdMob provides a framework that allows partners to send additional data to third parties through custom data fields, a feature Google calls "network extras". If a data receiver has set up a filter to block certain fields of data, the use of custom fields may be used to circumvent this filter.

In Google AdMob's public documentation for developers, Vungle is the only listed example of a partner with access to network extras.

> *"Certain mediated networks, such as Vungle, require or have the option to provide a custom network extras object to provide additional information to requests to their network."*[407]

This means that Google AdMob provides Vungle with access to extra features that allows Vungle to bypass data filters, and thus send more data to its partners than what would ordinarily be possible through Google's regular advertising tools.[408]

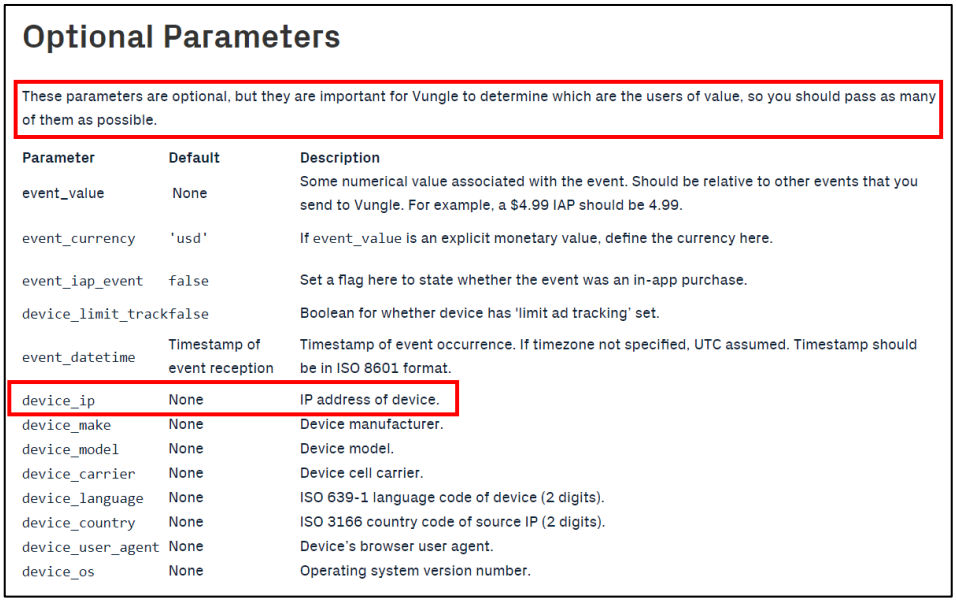
[407] "Configuring ad requests with network extras (optional)", Google AdMob [accessed December 11, 2019] https://developers.google.com/admob/ios/mediation-test-suite#configuring_ad_requests_with_network_extras_optional

[408] The integration of Vungle and AdMob is described further in Google's documentation. "Integrating Vungle with Mediation", Google AdMob https://developers.google.com/admob/android/mediation/vungle

Since its inception, Vungle has received venture funding at several points, with Google being a major investor in the Seed Round, Series A and Series B.[409] The fact that Vungle, a company Google has invested in, is the only partner mentioned to have access to special features, raises concerns.

Through its own documentation for app developers, Vungle instructs its publisher partners to set up the Vungle SDK to use these custom fields to send a lot of optional data, including IP addresses.

> *"These parameters are optional, but they are important for Vungle to determine which are the users of value, so you should pass as many of them as possible.*
>
> *[…] IP address of the device."*[410]



## Optional Parameters

These parameters are optional, but they are important for Vungle to determine which are the users of value, so you should pass as many of them as possible.

| Parameter | Default | Description |
|---|---|---|
| event_value | None | Some numerical value associated with the event. Should be relative to other events that you send to Vungle. For example, a $4.99 IAP should be 4.99. |
| event_currency | 'usd' | If event_value is an explicit monetary value, define the currency here. |
| event_iap_event | false | Set a flag here to state whether the event was an in-app purchase. |
| device_limit_track | false | Boolean for whether device has 'limit ad tracking' set. |
| event_datetime | Timestamp of event reception | Timestamp of event occurrence. If timezone not specified, UTC assumed. Timestamp should be in ISO 8601 format. |
| device_ip | None | IP address of device. |
| device_make | None | Device manufacturer. |
| device_model | None | Device model. |
| device_carrier | None | Device cell carrier. |
| device_language | None | ISO 639-1 language code of device (2 digits). |
| device_country | None | ISO 3166 country code of source IP (2 digits). |
| device_user_agent | None | Device's browser user agent. |
| device_os | None | Operating system version number. |

*43 Source: https://support.vungle.com/hc/en-us/articles/115004827347-Post-Install-Postback-API-Documentation [accessed December 11, 2019]*

[409] Google Ventures invested in Vungle in 2011, 2013, and 2014. "Don't Try This At Home: How Vungle Broke In To Silicon Valley", Tomio Geron https://www.forbes.com/sites/tomiogeron/2012/06/25/dont-try-this-at-home-how-vungle-broke-in-to-silicon-valley/#1a4502501884
"Vungle Raises $6.5M For A Growing In-App Mobile Video Advertising Business", Kim-Mai Cutler https://techcrunch.com/2013/08/15/vungle-series-a/
"Video ad startup Vungle raises $17M from Google, AOL, & others", Tom Cheredar https://venturebeat.com/2014/02/06/video-ads-startup-vungle-raises-17m-from-google-aol-others/

[410] "Post-Install Postback API Documentation", Vungle Support [accessed December 11, 2019] https://support.vungle.com/hc/en-us/articles/115004827347-Post-Install-Postback-API-Documentation

Vungle and Twitter MoPub are integrated partners. In the developer documentation, Vungle describes how to integrate the Vungle SDK with MoPub's advertising mediation platform.[411]

Although Vungle is a part of Google's self-certification program, it is actively encouraging app developers to send full IP addresses as advertising targeting criteria. When this is sent together with the Advertising ID, this allows third party vendors to track users across devices.

As Vungle is integrated into the Grindr app and encourages publishers to provide the IP address it is a possible source for the initial transmission of the IP address to other parties. However, this could not be observed during Mnemonic's technical testing.

### 7.1.7 AdColony

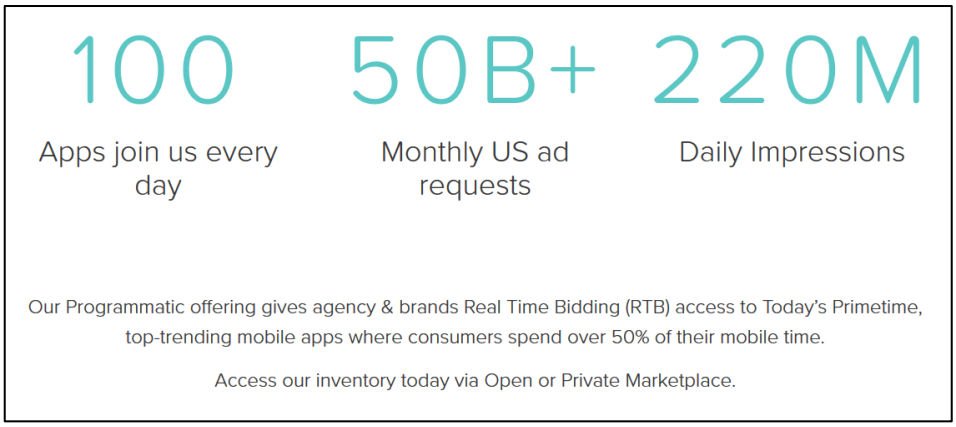
AdColony is a mobile supply side platform that helps app publishers make money through ads.[412] It also provides demand side technology that enables marketers to advertise brands and mobile apps.[413] AdColony is a subsidiary of the Norwegian holding company Otello, which used to be part of the company Opera.[414]

AdColony claims that its advertising platform has a reach of over 2 billion unique devices, and a "market leading SDK footprint in the top 1000 apps".[415] The company also runs a programmatic advertising service to give brands *"Real Time Bidding (RTB) access to Today's Primetime, top-trending mobile apps"*.[416]

During the technical testing of Grindr, AdColony was observed receiving the Advertising ID, GPS coordinates, age, app name, and the configurations, and the

[411] "Integrating MoPub + Vungle SDK v.6 (Android)", Vungle [accessed December 11, 2019] https://support.vungle.com/hc/en-us/articles/360003491192#set-up-vungle-as-an-sdk-network-0-0
[412] "Grow With Us", AdColony [accessed December 11, 2019] https://www.adcolony.com/publishers/
[413] "Highest Quality Mobile Experiences", AdColony [accessed December 11, 2019] https://www.adcolony.com/advertisers/
[414] "Opera Software ASA Becomes Otello Corporation ASA", Otello [accessed December 11, 2019] https://www.otellocorp.com/
[415] "Subsidiaries – AdColony", Otello [accessed December 11, 2019] https://www.otellocorp.com/subsidiaries/ad-colony
[416] "Programmatic", AdColony [accessed December 11, 2019] https://www.adcolony.com/technology/programmatic/

Grindr user ID. Adcolony received this data directly from Grindr through the AdColony SDK integration.[417]




*44 Source: https://www.adcolony.com/technology/programmatic/ [accessed December 11, 2019]*

Its privacy policy outlines what data AdColony collects about consumers. This includes IP addresses, Advertising IDs, and precise geocoordinates.

> *"Our technology Platform collects and uses personal data, including but not limited to: the name of the Publishers on which the advertisement is served, the IP address used to access the Internet, device advertising identifiers (Google Advertising ID, Apple Identifier for Advertisers), [...]*
>
> *Our technology Platform also collects and uses precise location data about a device from mobile applications and advertising exchanges and may match the device location to certain residential or commercial points of interest such as a "neighborhood", "coffee shop" or "Sports arena" for interest-based advertising, ad targeting, analytics and market research purposes."*[418]

Additionally, AdColony states that it collects data from other third parties to construct profiles on consumers.

> *"We sometimes work with third-party data partners and advertising exchanges to enhance our advertising and targeting capabilities on the Platform. As determined by our partners' business and privacy policies, we may also receive and retain information from partners' Publishers including but not limited to: the current location of the device, third-party applications on the device or in use at the time of our advertising transaction with the device, the Users age, gender or other demographic indicator, and we may use or derive data obtained from third parties such*

[417] Mnemonic, "Review of communications from apps", chapter 3.2.2 https://www.forbrukerradet.no/out-of-control/

[418] AdColony privacy policy (last updated May 24, 2019) https://www.adcolony.com/privacy-policy/

> *as approximate location based on IP address to help match data sets, although such data is processed outside of our Platform."*[419]

Although its website does include an extensive list of partners, AdColony provides an overview of some of these partners. This includes MoPub, Google DoubleClick, PubNative, Smaato, AppsFlyer, Kochava, and many more.[420]

According to its privacy policy, AdColony considers itself controllers for most processing activities related to its advertising services.

> *"Where AdColony is a controller of data (e.g., via most of our advertising Services), the legal basis will be both legitimate interest (Art. 6 (1) f) GDPR) and consent (Art. 6 (1) a) GDPR) depending on the type of information subject to processing and the information we receive from upstream partners. We may also process data for the performance of a contract with you (Art. 6 (1) b) GDPR)."*[421]

AdColony claims to have legitimate interests under the GDPR to process most of the personal data it receives. Unlike the other adtech companies described in this chapter, AdColony describes its reasoning for having a legitimate interest to process personal data. This includes the interest of publishers to monetize their audience, that it secures the data it processes, and that consumers are aware that this type of collection and sharing of personal data is taking place when they use the internet.

> *"AdColony has assessed that it has legitimate interest in the collection of this information pursuant to 6(1)(f) of General Data Protection Regulation (GDPR). In our assessment, we believe that all data processing currently engaged upon via the AdColony Marketplace falls under the "legitimate interest" legal basis. A summary of our rationale is as follows:*
>
> *· Pre-internet, digital publishers were able to monetize their audience subscription lists for direct marketing purposes utilizing legitimate interest, and advertisers were able to use that data for direct marketing purposes on the same basis. Data subjects typically had to pay subscription fees to access content.*
>
> *· In the digital age, publishers still need to monetize their audiences in order to continue to provide free content and Advertisers continue to need to reach their desired audiences. Data subjects have become increasingly reluctant to pay cash for digital content from Web sites and mobile apps.*

[419] Ibid.
[420] "Performance", AdColony [accessed December 11, 2019] https://www.adcolony.com/performance/
[421] AdColony privacy policy (last updated May 24, 2019) https://www.adcolony.com/privacy-policy/

> · *The types of data segments utilized by AdColony (e.g., pseudonymous personal data) and the profiling activities are not generally considered high risk per the guidance of the A29WP.*
>
> · *Users are increasingly savvy about the types of data being collected about them via Web sites for digital advertising. Moreover, transparency tools which explain the data collection practices of companies such as AdColony are increasingly ubiquitous.*
>
> · *AdColony adopts reasonable controls to ensure that the data collected is secured and won't fall into the hands of an entity that might be in position to harm the human rights of data subjects.*
>
> · *Thus, the balance of interests leans towards the benefits generated for data subjects, publishers and advertisers, and those benefits outweigh the risks to the fundamental human rights of data subjects.*
>
> · *Accordingly, AdColony feels confident that the processing activities engaged upon via the AdColony marketplace fall under the legal basis of legitimate interest."*

Although AdColony claims to respect device level opt out settings, it "strongly discourages" using the settings.

> *"We honor Apple "Limit Ad Tracking" and Google Opt out of "Ads Personalization" device settings, but we strongly discourage their use. AdColony works very hard to respect privacy and personal data and sees these global tools as having a damaging effect on your experience with advertising. There will always be advertising, so we believe that the best world is one where that ads are relevant to your interests and where you have granular control over which ad networks you trust with your personal data, not a tracking block for all ad networks."*

During the technical testing, after Mnemonic had enabled the device level opt out settings, AdColony was still observed receiving a significant amount of data including the Advertising ID.[422] As discussed further in chapter 2.5, this is highly problematic as it indicates that even if the consumer is aware of the data sharing and actively tries to opt out, this still does not ensure that their data is not shared with third parties.

As will be discussed in detail in chapter 8, AdColony's reasoning for having a legitimate interest in tracking and collecting consumers' personal data through more than 2 billion devices is unlikely to outweigh the data subject's fundamental rights and freedoms. If this is the case, AdColony lacks a legal basis to process the personal data that it was observed receiving.

[422] Mnemonic, "Review of communications from apps", chapter 3.12 https://www.forbrukerradet.no/out-of-control/

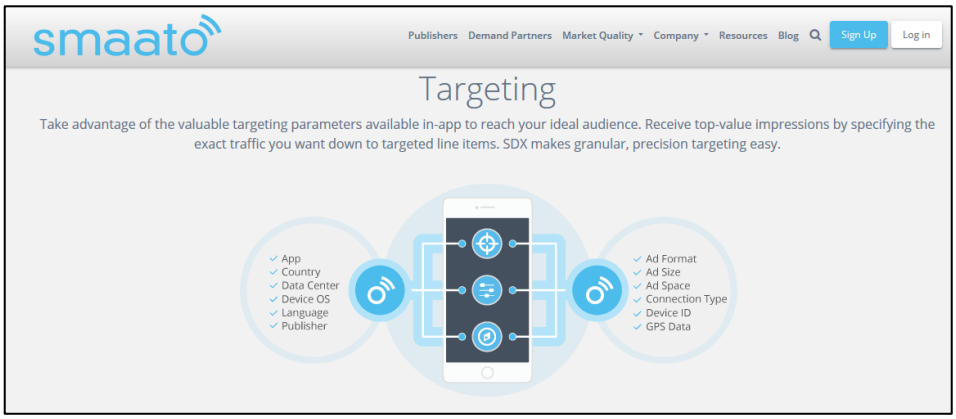
### 7.1.8 Smaato

Smaato is a San Francisco-based mobile adtech company that provides a mobile supply side platform. It also runs an ad exchange and provide ad server functionality to help app publishers monetize their apps. Additionally, Smaato runs a demand side platform that allows marketers to run mobile ad campaigns.[423]

According to its website, Smaato partners with more than 90 000 mobile publishers and app developers, and has more than 450 demand partners.[424]

> *"Our platform reaches over one billion unique mobile users and processes 500+ billion monthly ad requests globally. On top of our extensive reach, we deliver in-depth local expertise to key markets around the world with offices in China, Germany, Singapore, and the US."*[425]

Through its SDK integration in the Grindr app, Smaato was observed to receive the Advertising ID, GPS coordinates, the user's age, and the app name. Smaato were observed receiving more data transmissions from Grindr than any of the other third parties.[426]

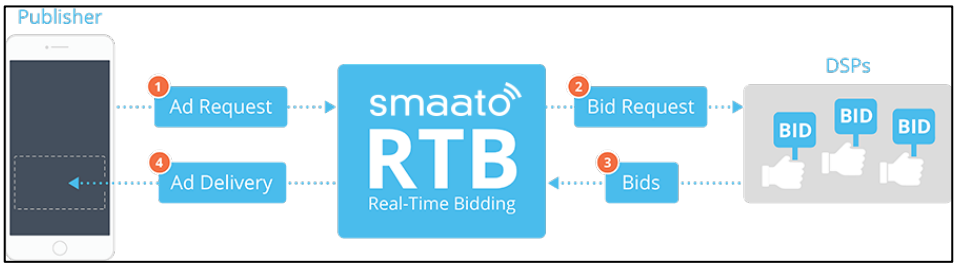



*45 Source: https://www.smaato.com/advertisers/ [accessed December 11, 2019]*

On its website, Smaato describes how a partnership with Grindr provided Grindr with access to more than 337 ad networks and DSPs:

[423] Smaato [accessed December 11, 2019] https://www.smaato.com/
[424] "About Smaato", Smaato [accessed December 11, 2019] https://www.smaato.com/company/
[425] Ibid.
[426] Mnemonic, "Review of communications from apps", chapter 3.2.2 https://www.forbrukerradet.no/out-of-control/

> *"Smaato was able to deliver much higher eCPMs to Grindr because of the massive scale it brings with 337+ ad networks and DSPs connected globally to its platform, and the granular controls it gave to the developers in setting the minimum eCPM floors by geography."*[427]




*46 Source: https://www.smaato.com/real-time-bidding/ [accessed December 11, 2019]*

According to its privacy policy, Smaato may use the data it collects for a number of purposes, including profiling and audience segmentation, which may be derived from cross device tracking and by combining data from various sources.

> *"Create inferences about End Users categorized into "Audience Segments" or to help Clients do so. For example, if the information we collect indicates that an End User likes apps (or clicks on ads) about travel, we may categorize the End User of that device as someone who is interested in travel;*
>
> *Develop and use data models that try to predict End Users' potential future behavior and interests on a per-device basis or across devices;*
>
> *[…] Resolve identities across multiple devices, such as to match IP addresses to link an End User across, for example, mobile browsers, mobile devices, tablets, set top boxes, or other devices"*[428]

Smaato states that it relies on user consent in order to collect and use personal data, and claims to have a legitimate interest in using unique identifiers to provide targeted advertising. According to its privacy policy, the tailoring of marketing messaging is beneficial to end users.

> *"In order to store and gain access to information stored on your device, we rely on your consent. For this "cookie consent" (which applies not only to "cookies" but also to Mobile IDs), we rely on mobile app developers and oblige them contractually to pass on only legally obtained data. […]*
>
> *In some cases, we rely on legitimate interest as a legal basis for processing Personal Data, in order to provide our and/or other data controllers' services. Such processing goes beyond the original collection of Mobile IDs.*

[427] "Case Study: Grindr", Smaato [accessed December 11, 2019] https://www.smaato.com/resources/case-studies/success-story-grindr/
[428] Smaato privacy policy (last updated April 16, 2019) https://www.smaato.com/privacy/

> *A legitimate interest we rely on, for instance, is the tailoring of promotional communications within mobile apps and services, which is beneficial to End Users and is an integral part of the ecosystem by which freely available content is funded through advertising revenue."*

If consumers want to opt out of this tracking, Smaato states that they must use the system-level Android settings.

On its partner list, Smaato lists more than 1 000 partners that it may share data with. In order to understand how personal data may be processed, Smaato encourages consumers to read the privacy policies of all the partners.

> *"We encourage you to review the privacy policies of our Demand Partners and the TCF Vendors to ensure that you understand their privacy practices in relation to the personal data they may process."*[429]

Smaato claims to be a data processor in some cases, and a controller in other cases. It is unclear whether the data it receives through Grindr is processed by Smaato as a controller or as a processor.

> *"Smaato may act as either a data controller or a data processor in handling your Personal Data, depending on the precise circumstances. For instance, for Personal Data that we use internally and independently to create our own data tools and operate the Smaato Ad Services, and for Personal Data that we collect about our Clients, we are a data controller. But when we handle Personal Data strictly on behalf of our Clients or Partners in order to provide our services to them, we are a data processor. Thus, for instance, if you have questions about data that is used primarily by a mobile app on which our technology is embedded – or companies that serve ads that use our technology – you should contact those companies regarding questions about the Personal Data they handle and control."*

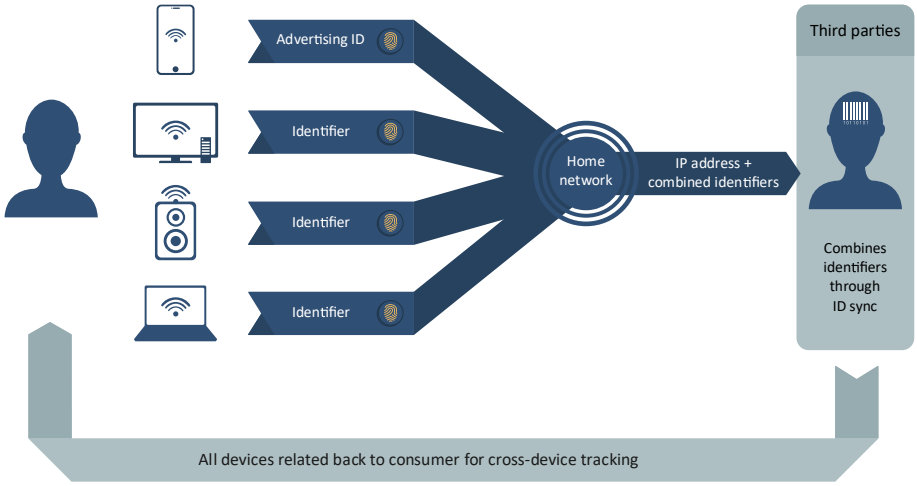
Similarly to AdColony, Smaato claims to have a legitimate interest to track and profile consumers because consumers want free content. As discussed in chapter 8, this is unlikely to outweigh the fundamental rights and freedoms of the data subject. If Smaato is sharing this data with any of its 1000 partners, it seems to be lacking a valid legal basis to process the personal data that it was observed receiving.

[429] "Partner List", Smaato [accessed December 11, 2019] https://www.smaato.com/partner-list/

## 7.2 Self-certification and cross-device tracking

When combining the Android Advertising ID with an IP address, third party vendors can identify users across the adtech system and beyond. As demonstrated below, the combination of the Advertising ID with the IP address observed in the analysis of Grindr illustrates how Google's trust-based system creates significant privacy breaches for consumers, while creating revenue opportunities for adtech companies.

For example, a data broker or other third party vendor may receive information about a Grindr user, including his Android Advertising ID and his IP address. The user then opens Grindr while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address.




*47 The IP address can be used to connect different identifiers for cross-device tracking.*

The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behaviour across devices and target the user and their devices with ads on different networks. For companies such as AT&T's AppNexus, which received the IP address and other Grindr data, this IP address could also be used to append data from apps to existing customer profiles.

In other words, third party vendors can use the IP address to push personal data collected from apps into publisher websites and digital TV ads. This data

can then be appended to profiles used for tracking consumers across devices, and be expanded exponentially to new digital marketing and adtech partners.

### 7.2.1 The problem of self-certification

Google's mobile advertising mediation platform is called AdMob, and provides app publishers access to marketers that are part of different advertising networks. AdColony, MoPub and Vungle are all part of the AdMob-supported advertising networks.[430]

As described in chapter 2, a large portion of mobile tracking for advertising purposes is built upon the Android Advertising ID. The use of this unique identifier is conditional on certain terms set forth by Google, which is part of the AdMob self-certification scheme called "Google Play self-certified ad networks program".

Ad networks sign up to this program by self-certifying that they will only use their SDKs in compliance with Google's terms for advertising networks, which includes that they must never send the Android Advertising ID together with other unique identifiers,[431] and should generally not be combined with personally identifiable information (PII).[432]

The use of "PII" instead of "personal data" in this context is confusing, as it does not make it clear whether Google prohibits the combination of the Advertising ID and IP address, since IP addresses is not considered PII in the US, but is personal data under the GDPR. However, as demonstrated above, the use of an IP address effectively prevents users from reducing tracking if they reset their Advertising ID.

A 2019 study showed that approximately 70% out of 24 000 Google Play apps were transmitting the Advertising ID alongside other identifiers. [433] This shows that the combination of the Advertising ID with other identifiers is commonplace across the adtech industry, meaning that many third party

[430] "Mediation", Google AdMob [accessed December 11, 2019] https://developers.google.com/admob/android/mediate
[431] "Monetization and Ads", Google Play Developer Policy Center [accessed December 11, 2019] https://play.google.com/about/monetization-ads/ads/#!?zippy_activeEl=ad-id#ad-id
[432] "Best practices for unique identifiers", Android Developers [accessed December 11, 2019] https://developer.android.com/training/articles/user-data-ids
[433] "Ad IDs Behaving Badly", Serge Egelman https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly/

vendors seem to completely disregard Google's terms. This demonstrates the systemic issues in Google's hands-off approach.

In other words, there seem to be no safeguards to prevent an ad network from self-certifying, then turning around and breaching the terms by appending the Advertising ID to other persistent identifiers. Google's ad network program seems to be entirely trust-based and has a significant lack of checks and balances.

The broadcasting of combinations of unique identifiers resembles observations made by Brave as part of its complaint against the Google and IAB real-time bidding systems. According to evidence filed by Brave, bid requests on websites often include IP addresses and unique tracking identifiers. This allows a large number of third party vendors to harvest personal data from websites whenever an ad is displayed.[434] This personal data may also be extracted from data brokers and other adtech companies to create or enrich user profiles.

The technical tests described above shows how a similar system is set up in the mobile app environment. The Android Advertising ID, IP address, and other unique identifiers are broadcast through advertising mediation platforms. This allows third parties to collect personal data from apps. Through ID syncing, this data can be appended to profiles collected from other services and devices. Consequently, the data collected through the RTB system on websites can easily be appended and combined with data collected from apps.

# 8 Legal analysis

In the previous chapters we have described how a large amount of third party adtech companies are receiving a variety of personal data through regular use of popular Android apps. Identifiers and personal data such as GPS-coordinates, IP addresses, and unique ID numbers such as Android Advertising IDs are transmitted together with information about app use, sexual preferences, behavioural data, and more. This information is used to make inferences about individuals and segments of consumers, which is employed to target personalized advertising at the moments when we are most receptive, and possibly for other purposes that are not related to advertising.

[434] "Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR", Johnny Ryan https://brave.com/adtech-data-breach-complaint/

The data sharing described above shows an adtech industry fuelled by collecting as much data as possible in order to combine, analyse and use it to influence behaviour. The cost of this systemic oversharing and overcollection seems to be that personal data is being broadcast at every turn, leaving consumers with little transparency or insight into what data is being collected, how it is used, and very little or no control over their personal data.

As described in chapter 3, the consequences of this widespread collection and use of personal data may stretch far beyond personalized advertising; the current system opens up for comprehensive abuse that can undermine not just our privacy, but erode our autonomy and even our democracies. This raises serious questions about whether these processing operations can be legally justified.

In this chapter, we look at some of the data transmissions and processing that were observed throughout previous chapters from a legal point of view. We use the General Data Protection Regulation (GDPR), which applies to all processing of personal data related to individuals situated in the EU and EEA, as a basis for this analysis. Additionally, the ePrivacy Directive applies to how third parties gather consent to accessing information stored on the consumers' device, but this is outside the scope of our analysis.

Because the technical testing was done in Norway, the GDPR applies to all processing of personal data described in this report. Although we do not cover every third party data recipient in detail in this chapter, the legal analysis and conclusions can be considered representative of the processing undertaken by companies in large parts of the adtech industry described throughout the report.

## 8.1 The General Data Protection Regulation

The rights to privacy and data protection are two fundamental rights enshrined in the EU Treaties and in the Charter of Fundamental Rights.[435] In the EU and the EEA countries, data protection law aims to ensure the fair processing of personal data by organisations from the public and private sectors. The General Data Protection Regulation (GDPR) grants individuals an important number of data protection rights, such as the right to access, erase, rectify, move or object to the processing of their personal data. This important piece of legislation

[435] Art. 7 and 8 of the Charter of Fundamental Rights of the European Union, Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU), Art. 1(2) and Recital 1 GDPR.

obliges controllers and processors not only to respect these rights, but also to facilitate exercising them.

Since all of the apps that were tested offer their services directly to individuals in the EU and EEA countries, the service providers and third parties who receive and process personal data fall under the scope of the Regulation and must thereby comply with its stringent requirements.[436]

The widespread transmissions of personal data observed during the technical testing leads to a number of questions regarding how these publishers and third parties are complying with the GDPR. The GDPR includes a number of data protection principles. For example, the principle of data protection by default requires technical and organizational measures to ensure that only personal data which are necessary for each specific purpose of the processing are processed.[437]

The principle of purpose limitation states that personal data must only be processed for specified, explicit, and legitimate purposes, and should not be processed in manners that are incompatible with those purposes.[438] Similarly, the principle of data minimisation means that the collection of personal data should be adequate, relevant and limited to what is necessary to fulfil the stated purposes of processing.[439]

Although these principles are all potentially important points of contention regarding the practices we have described, our scope is focused on considering the lawfulness of processing of personal data. In this chapter, we will examine whether the third parties receiving personal data have a valid legal basis for their processing operations. If there is no valid legal basis for the processing of personal data, then the processing is not compliant with the GDPR.

### 8.1.1 Data subjects, controllers, and processors

The GDPR protects the rights of any identified or identifiable natural living person, or **data subject,** whose personal data undergoes processing operations by an entity which determines the means and purposes of such processing, which is called a **controller**. Entities carrying out data processing on behalf of the controller are considered **processors**.

[436] GDPR Art. 3(2)
[437] GDPR Art. 25(2)
[438] GDPR Art. 5(1)(b)
[439] GDPR Art. 5(1)(c)

In general, all processing undertaken by a processor shall be governed by a contract or another binding legal instrument signed with the controller. When a processor also determines the purposes and means of processing of personal data it receives from the controller, it shall be considered a controller or a joint controller in its own right.

The controller is defined by whether it can "determine the purposes and means of the processing of personal data".[440] What is relevant to determine whether an entity is a controller or not is therefore to what degree it can choose how the data is processed and for what end.

In the context of adtech, controllers often set their own SDKs to collect data, and then decide how the collected data is used. Consequently, in the examples described throughout this report, the individual consumer is the data subject, the app providers are controllers, while the adtech third parties receiving personal data from the apps are either processors, separate controllers, or joint controllers, depending on how and under what terms they use the personal data.

A third party that provides basic analytics or error logging functions for the app provider may be considered a data processor if it is acting only upon the instructions of the publisher. In that case, the app provider is the controller responsible and liable for determining the purposes for the processing of personal data carried out on its behalf.

According to a 2018 European Court of Justice ruling, marketers that are involved in the purchase of targeted advertising can be considered joint controllers, even if they do not actually process personal data themselves, as long as they define the means purposes of the processing.[441] This means that, for the means and purposes of processing that the marketers have defined, the responsibility to ensure that personal data is processed on a valid legal basis extend to the marketers who are using third party adtech vendors to serve targeted advertising.

However, many of the adtech companies we have described use the data for their own purposes, or share the data with other companies, and thereby define the purposes for which they use personal data (for example, making data

[440] GDPR Art. 4(7)
[441] "Why marketers must conduct GDPR Data Protection Impact Assessments of RTB", Johnny Ryan https://brave.com/dpia/

available to their partners, or creating behavioural profiles). If a company uses the personal data it receives for its own purposes, and determines the means of such processing, this makes it a separate controller. This means that it cannot rely on the original controller (app provider) to be the only responsible party to obtain a valid legal basis for their processing operations, or to ensure compliance with other obligations under the GDPR, in particular as regards the exercise of data subjects' rights.

### 8.1.2 Definition of personal data

Article 4(1) of the GDPR contains a definition of personal data, which covers the information that can directly or indirectly identify a natural person.

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*[442]

Note that this definition includes unique identification numbers, which may include Advertising IDs, location data, and online identifiers (such as IP addresses). Most of the third parties described in this report receive personal data from the app providers, and consequently process personal data in some form. Even if the third parties delete personal data in a timely manner, they must make sure that they rely on a valid legal basis for the processing of such personal data.

Under the GDPR, the processing of special categories of personal data is as a general rule forbidden, unless certain criteria are fulfilled.

> *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*[443]

Some of the data that was observed being transmitted, particularly data concerning the use of Grindr, likely falls within the scope of special category data because it is data concerning sexual orientation.

[442] GDPR Art.4(1)
[443] GDPR Art.9(1)

## 8.2 Legal basis for processing of personal data

According to the GDPR, in order to be lawful, the processing of personal data must be based on one of six legal bases. Among others, the processing may be based on consent, the fulfilment of a contract, compliance with a legal obligation or on the legitimate interests of the controller/processor when such interest outweighs the fundamental rights and freedoms of data subjects.

As described above, the third parties that were observed receiving personal data claim to use a variety of legal bases for their processing operations. Many of these companies claim to rely on both consent and legitimate interests as a legal basis, often without a clear distinction between the categories of personal data, the purposes of processing, and the legal basis relied upon for their processing. This is problematic because it makes it difficult to understand what legal basis is used for what processing operations.

Some of third party vendors claim that they operate based on consent passed on through contractual terms with their customers, which in this case would be the app providers. However, each entity processing personal data must obtain a clear, valid, unambiguous and separate consent from data subjects when they rely on such a legal basis.[444] "Consent" packaged in terms and conditions or privacy policies and handed from controller to controller is not compliant.

In the decision from the French data protection authority CNIL against the third party vendor Vectaury, the passing on of consent was deemed to be inadequate. The CNIL stated that controllers not only have to implement a compliant consent mechanism, but also have to make sure that any personal information is collected and processed in a lawful manner. This means that when receiving personal data from a partner company, the receiving party must be able to demonstrate that the transmitting party also relied on legally compliant consent mechanisms.[445]

As shown in chapter 5, the majority of the apps that were tested did not present the user with legally compliant consent mechanisms, and this has consequences for the validity of consent for any third parties acting as controllers. This is elaborated upon this in the following sections.

[444] GDPR Art. 4(11) and Art. 7

[445] "How a small French privacy ruling could remake adtech for good", Natasha Lomas https://techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/

### 8.2.1 Consent

Under the GDPR, consent must fulfil certain conditions in order to be considered legally valid. This includes that consent is required to be freely given, specific, informed, and unambiguous. Additionally, the data subject must have given consent through a statement or by a clear affirmative action.[446]

Processing of special categories of personal data, which includes data concerning the data subject's sex life, sexual orientation, and health, is as a general rule forbidden, unless the controller has obtained explicit consent.[447]

According to the European Data Protection Board (EDPB; former Article 29 Working Party), a European body, which contributes to the consistent application of data protection rules and composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS),

> *[…] opt-in consent would almost always be required [...] for tracking and profiling for purposes of direct marketing, behavioural advertisement, location-based advertising or tracking-based digital market research.*[448]

This means that many of the adtech companies described in this report would most likely have to rely on consent as the legal basis for their processing operations.

#### *7.2.1.1 Freely given and specific*

In order to be a valid legal basis for processing, consent needs to be freely given and specific. To fulfil the requirement of being freely given, the controller should as a general rule not make access to the service dependent on user's consent to the processing of personal data for purposes beyond providing the service.[449]

---

[446] GDPR Art. 4(11) and Art. 7

[447] GDPR Art.9

[448] "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 47, Article 29 Working Party https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[449] This is described in "Guidelines on consent under Regulation 2016/679", p. 8, Article 29 Working Party https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[450]

As shown in chapter 5, none of the apps that were analysed provide any meaningful ways of giving or refusing consent to the sharing of personal data with third parties. In almost all of the apps, the only option to use the app is to agree to the sharing of personal data as described in the privacy policies. If the data subject has to choose between giving blanket consent to third party processing for profiling and behavioural advertising purposes, or uninstalling the app, the consent cannot be considered to be "freely given".

The consent to processing of personal data must also be specific for the processing activity in order to be considered legally valid. When asked to consent to processing of personal data, any processing that is not strictly necessary for the performance of the service should be presented separately. This means that consent for different processing operations of personal data outside the normal functioning of the service cannot be bundled together.

> *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.*[451]

In other words, the data subject clicking "I agree" to a blanket privacy policy, cannot be considered having given consent to their personal data being shared with third parties and used for profiling.

#### *7.2.1.2 Informed and unambiguous*

A valid consent under the GDPR must be informed and unambiguous. This means that it must fulfil certain conditions for transparency, as laid out in Article 12 of the GDPR.

> *The controller shall take appropriate measures to provide any information […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*[452]

[450] GDPR Art. 7(4)
[451] GDPR Art. 7(2)
[452] GDPR Art.12(1)

A 2019 decision by the French data protection authority CNIL deemed Google to be in breach of this principle of transparency, because information about processing operations was spread across multiple documents, and because the information on how personal data may be used was presented in a way that was vague and difficult for the user to comprehend.

> *Users are not able to fully understand the extent of the processing operations carried out by GOOGLE. But the processing operations are particularly massive and intrusive because of the number of services offered (about twenty), the amount and the nature of the data processed and combined. The restricted committee observes in particular that the purposes of processing are described in a too generic and vague manner, and so are the categories of data processed for these various purposes. Similarly, the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company. Finally, the restricted committee notices that the information about the retention period is not provided for some data.* [453]

As demonstrated in chapter 5, none of the apps that were tested provide clear information about third party data sharing when the data subject starts using the app.[454] Only Perfect365 and My Talking Tom 2 mentions up front that data is shared for advertising purposes, but without clarifying the extent of tracking and data sharing going on in the app.

For the other apps, the user would have to read the entire privacy policy, and the privacy policies of any third and/or fourth parties, in order to know the extent of data sharing. Many of the apps and third parties do not even mention the names of the companies that they are sharing personal data with. This shows that the consent is not informed, and does not fulfil the requirement of being specific and unambiguous.

#### *7.2.1.3 Explicit*

In order to be legally valid, consent with regard to the processing of personal data has to be explicit.[455] This means that the controller should obtain verbal or written confirmation about the specific processing.[456]

---

[453] "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", CNIL https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[454] Except My Talking Tom 2, if the user reports to be over 16 years old.

[455] Article 9(2)(a) GDPR.

[456] This is detailed in Recital 32 of the GDPR.

Several of the third parties analysed in the previous chapters claim to rely on consent for some of their processing operations, but they either assume that the app provider could gather valid consent on their behalf, or they consider *not having opted out* through device-level settings to be a valid form of consent.[457]

According to the Article 29 Working Party, consent cannot be based on an opt-out mechanism, as the failure to opt out is not a clear affirmative action.[458] This indicates that none of the controllers who claim that data subjects can withdraw their by default opted-in consent by turning off personalized ads through their device settings, have a valid consent to process personal data.

Due to the massive scale of data sharing outlined in this report, which is just the tip of an iceberg, it seems unlikely that the adtech industry in its current form can operate based on consent as a legal basis. The industry in its current form clearly does not seem to meet the stringent requirements of consent as set forth in the GDPR. The system is deprived of any meaningful individual choice and transparency, and personal data is transmitted to an enormous amount of actors who each operate with their own privacy policies. Meanwhile, users are not informed and not given granular choices in violation of the regulation.

### 8.2.2 Fulfilment of a contract

One of the legal bases for processing personal data under the GDPR is when "the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".[459] This generally means that in certain cases, controllers may have a legal basis to process certain personal data when this is necessary to fulfil a contract with the data subject. For example, an online retailer may need to process users' payment data in order to fulfil a transaction, and an address in order to ship items to the buyer.

According to the European Data Protection Board's guidelines, the fulfilment of a contract cannot be used as a legal basis for processing personal data for behavioural advertising purposes.

> *"As a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services.*

[457] See chapter 2.5 for more detail on these opt-out settings.
[458] "Guidelines on Consent under Regulation 2016/679 (wp259rev.01)" page 16, Article 29 Working Party https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[459] GDPR Art. 6(1)(b)

> *Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads.*
>
> *[…] Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue."*[460]

Furthermore, the EDPB notes that tracking users for audience segmentation purposes also cannot rely on the fulfilment of a contract as a valid legal basis.

> *"The EDPB also notes that tracking and profiling of users may be carried out for the purpose of identifying groups of individuals with similar characteristics, to enable targeting advertising to similar audiences. Such processing cannot be carried out on the basis of Article 6(1)(b), as it cannot be said to be objectively necessary for the performance of the contract with the user to track and compare users' characteristics and behaviour for purposes which relate to advertising to other individuals"*[461]

Consequently, it seems clear that none of the processing operations described in this report can rely on the fulfilment of a contract as a legal basis, particularly when personal data is used for advertising purposes.

### 8.2.3 Legitimate interests

In certain cases, the processing of personal data may be based on legitimate interests. The GDPR explains this as following:

> *"Processing shall be lawful only if and to the extent that at least one of the following applies: […] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*[462]

[460] "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects", p.14-15, European Data Protection Board https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[461] Ibid.

[462] GDPR Art. 6(1)(f)

Controllers who wish to use legitimate interest as a legal basis should conduct an evaluation. According to the ICO, this test can be broken down into three elements. [463]

(1) Purpose test: are you pursuing a legitimate interest?

(2) Necessity test: is the processing necessary for that purpose?

(3) Balancing test: do the individual's interests override the legitimate interest?

If a controller is relying on legitimate interests for their processing operations, it must clearly articulate their interests, and specify the purposes for the processing. To constitute a valid basis for processing of personal data, legitimate interests must be "lawful", "sufficiently clearly articulated" (transparent) and "represent a real and present interest".[464]

Certain purposes, such as fraud prevention, may constitute a controller's legitimate interests. However, the reliance on legitimate interests as a legal basis for processing requires controllers to balance their interests against the interests, rights, and freedoms of the data subject.

#### *8.2.3.1 Interests, rights, and freedoms of the data subject*

The extent and scope of personal data sharing and processing outlined throughout this report has potentially serious consequences for the data subjects' fundamental right to privacy. As noted by Amnesty International, the systemic surveillance that forms the foundation of microtargeting and behavioural advertising is also a threat to human rights such as the freedom of expression, freedom of thought, and the right to non-discrimination and equality

Few of the companies described in this report explain their legitimate interests in a clear way. In many cases, they simply state that they have legitimate business reasons to process personal data.

There is often a lack of information provided by companies about the balancing exercise between the legitimate interests of the controller and the fundamental

[463] "Legitimate interests", The Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

[464] "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" p. 25 and p. 52, Article 29 Working Party https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

rights and freedoms of the data subjects. This is particularly problematic because of the extent of invasive processing practices performed by many of the companies, and considering that the data subjects are only using an app, without awareness of the numerous third parties that are receiving and processing their personal data for various purposes.

According to Recital 47 of the GPDR, when using legitimate interests as a legal basis for processing, the controller also has to make sure that it is taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interests could exist for example where there is a relevant and appropriate relationship between the data subject and the controller, in situations such as where the data subject is a client or in the service of the controller.

At any rate, the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

In other words, the data subject must have a “reasonable expectation” that their personal data is being used by the company for a specific purpose. This expectation must exist at the time and in the context of the collection of the personal data. This particularly applies in cases where “there is a relevant and appropriate relationship between the data subject and the controller”.

It is difficult to see how consumers have a “relevant and appropriate relationship” with most of the third parties described throughout this report. There is a serious information asymmetry between the companies and the data subjects, with the former operating largely opaquely while having a lot of information on data subjects. In other words, the companies are virtually unknown to most consumers, so one can hardly consider this a relationship at all.

Although consumers may know that many “free” digital services are funded by advertising, this does not mean that most people will have a “reasonable expectation” of the amount of sharing and processing going on behind the scenes. For example, it seems very unlikely that users of a make-up or fertility app expect that their location data is continuously transmitted to location data brokers and to companies that engage in behavioural profiling. Accordingly, it

seems unlikely that the legitimate interests of the controller override or are even equal to the fundamental rights and freedoms of the data subjects in most of the cases described in this report.

#### *8.2.3.2 Interests of the controller*

In order to constitute a legitimate interest for processing personal data, the controller must be able to demonstrate that their processing operation represents a real and present interest. This should include being able to show that the processing of personal data is necessary for the purposes that the controller has defined.

Several of the third parties that were observed receiving personal data claim in their privacy policies that they have a legitimate interest to process such personal data. Many do not elaborate on their reasoning and simply state that they have an interest. Some, however, do justify the interest by explaining that targeted advertising is used to monetize and therefore support (free) online services. This may be regarded as carried out for a legitimate interest, but it is not absolute and it requires the balancing of interests.

The argument that publishers have a legitimate interest to monetize their services by showing targeted advertising is problematic. Many consumers may be averse to paying for many digital services, but this does not mean that companies can disregard data subjects' fundamental rights and freedoms just to offer services.

For such a balancing, as shown in chapter 7, AdColony provides the following argument for why it has a legitimate interests for processing personal data:

> *In our assessment, we believe that all data processing currently engaged upon via the AdColony Marketplace falls under the "legitimate interest" legal basis. A summary of our rationale is as follows:*
>
> *Pre-internet, digital publishers were able to monetize their audience subscription lists for direct marketing purposes utilizing legitimate interest, and advertisers were able to use that data for direct marketing purposes on the same basis. Data subjects typically had to pay subscription fees to access content.*
>
> *In the digital age, publishers still need to monetize their audiences in order to continue to provide free content and Advertisers continue to need to reach their desired audiences. Data subjects have become increasingly reluctant to pay cash for digital content from Web sites and mobile apps.*
>
> *The types of data segments utilized by AdColony (e.g., pseudonymous personal data) and the profiling activities are not generally considered high risk per the guidance of the A29WP.*

> *Users are increasingly savvy about the types of data being collected about them via Web sites for digital advertising. Moreover, transparency tools which explain the data collection practices of companies such as AdColony are increasingly ubiquitous.*
>
> *AdColony adopts reasonable controls to ensure that the data collected is secured and won't fall into the hands of an entity that might be in position to harm the human rights of data subjects.*
>
> *Thus, the balance of interests leans towards the benefits generated for data subjects, publishers and advertisers, and those benefits outweigh the risks to the fundamental human rights of data subjects.*
>
> *Accordingly, AdColony feels confident that the processing activities engaged upon via the AdColony marketplace fall under the legal basis of legitimate interest.*[465]

In other words, AdColony appears to be arguing that, because its role in serving targeted advertising is important for keeping online services free for users, it has a legitimate interest for its data processing. Additionally, according to AdColony, internet users are capable of understanding how their data is shared as a part of the adtech industry, and can use transparency tools to understand more about this.

As we have demonstrated throughout this report, it is next to impossible for a consumer to know which third parties are receiving and using personal data from even a single app. Regular consumers use many apps, which may all have their own third parties, and each third party may have many fourth parties. It is highly questionable that consumers can reasonably expect this data sharing and processing.

The argument that widespread collection and processing of personal data is necessary to fund online content is often repeated amongst adtech industry actors.[466] However, there are many alternative business models for funding online content, including subscription models, and importantly, advertising models that do not rely on breaching fundamental rights.

There is a key difference between "traditional" advertising-funded media and the adtech industry – the former does usually not rely on broadcasting personal data about consumers. As shown in chapter 2.3, there are alternative digital

[465] AdColony privacy policy (last updated May 24, 2019) https://www.adcolony.com/privacy-policy/

[466] "Internet Users Like Targeted Ads, Free Content", Grant Gross https://www.cio.com/article/2386057/internet-users-like-targeted-ads--free-content.html

advertising models that do not rely on the sharing and processing of personal data, including so-called contextual advertising, which relies on targeting ads based on publisher content rather than on personal data. This shows that the processing of personal data is not "necessary" to provide ad-funded services.[467]

There is a large scale erosion of responsibility in this system, where each actor may operate with their own legal basis for processing, their own opt out tools, and their own policies regulating the purposes of their processing. It is impossible to exercise your rights as a data subject when you do not even know who is processing your personal data.

Based on these observations, it does not seem right to assume that the fundamental rights and freedoms of the data subjects can be overridden by adtech companies' legitimate interests to serve ads and otherwise monetize personal data. As we have shown throughout this report, the widespread broadcasting of personal data is a threat to consumers' fundamental rights and freedoms.

In addition to undermining the right to privacy, the comprehensive surveillance many of these companies engage in poses a systemic threat to fundamental rights such as the freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination. Meanwhile, the system is so complex that consumers cannot have any reasonable expectation of this happening. It can be assumed that such a threat may significantly outweigh any perceived legitimate interest that data brokers and other adtech actors have in monetizing this data.[468]

## 8.3 Conclusion of legal analysis

As shown above, controllers need a valid legal basis for processing personal data for profiling and targeted advertising. In the cases described in this report, none of the apps or third parties appear to fulfil the legal conditions for collecting valid consent. Data subjects are not informed of how their personal data is shared and used in a clear and understandable way, and there are no granular choices regarding use of data that is not necessary for the functionality of the consumer-facing services.

---

[467] "Why the GDPR 'legitimate interest' provision will not save you", Johnny Ryan https://pagefair.com/blog/2017/gdpr-legitimate-interest/

[468] The argument that the fundamental rights of the data subject outweighs the economic interest of the controller is also supported by a Spanish court decision against Google Spain. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

Since the controllers in question fail to fulfil the conditions for consent, and the legal ground of necessary for the performance of a contract does not apply in these circumstances, the processing would need to be based on the legitimate interests of the controller. However, the data subject cannot have a reasonable expectation for the amount of data sharing and the variety of purposes their personal data is used for in these cases.

The large amount of personal data being sent to a variety of third parties, who all have their own purposes and policies for data processing, constitutes a widespread violation of data subjects' privacy. Even if advertising is necessary to provide services free of charge, these violations of privacy are not strictly necessary in order to provide digital ads. Consequently, it seems unlikely that the legitimate interests that these companies may claim to have can be demonstrated to override the fundamental rights and freedoms of the data subject.

If the majority of adtech companies described in this report can be considered controllers or joint controllers, and they can neither demonstrate that they have valid legal consent nor a legitimate interest that overrides the consumer's fundamental right to privacy, they appear to be lacking a legal basis for processing the personal data that they were observed to receive. If this is the case, a large number of third parties that collect consumer data for purposes such as behavioural profiling, targeted advertising and real-time bidding, are in breach of the General Data Protection Regulation.

# 9 What needs to be done?

In this report we have demonstrated how, whenever we use our apps, a large number of mostly unknown third party vendors are receiving very detailed personal data about us. The collection of data across services and devices allows many of these companies to construct intricate profiles about individual consumers, which can be used to target, discriminate and manipulate people. All of this depends on a complex industry of actors that operate outside of the public consciousness, and happens on a questionable legal basis.

In the complex web that is the adtech industry, consumers are being monetized through their personal data, and have few ways to avoid being made part of the transactions constantly taking place when they use online services. Hundreds or thousands of companies enable, facilitate, and participate in collecting, sharing, and selling information, monetizing consumer data in the pursuit of higher



returns on investment or conversions. Marketers and publishers are also complicit, through the enabling and financing of the broader system. Although national authorities and data protection agencies are aware of the industry, little has been done to curb this mass-exploitation of personal data. Change is overdue for the adtech industry.

## 8.1 The spread of personal data is illegal

There are very few actions consumers can take to limit or prevent the massive tracking and data sharing going on in the adtech industry. Although there are a variety of tools to prevent tracking in web browsers, there are few effective alternatives for mobile apps. In fact, ad blockers and tracker blockers are often banned from the Google Play Store. There are some industry self-regulation web portals where consumers can try to opt out of behavioural advertising, but this does not necessarily prevent the tracking.

Because of the enormous complexity of the adtech industry, and the overarching lack of transparency and control mechanisms, consumers are more or less powerless to prevent the harms that the system facilitates or makes possible. We have no direct customer relationships with any of the third parties involved, that most of us have no idea exist, and consequently there are few prospects of voting with our feet or boycotting bad actors.

The vastness of the adtech system seems to assure that any Android user will have their data hoovered up with at least one of these actors, which may share or sell the data to other actors. In short, in its current form, the adtech industry seems to make it inevitable that your personal data will end up in the databases of hundreds of companies that you have never heard of, who all have their own policies for processing and sharing this information.

Even if consumers had the time and knowledge necessary to read and understand privacy policies, these documents are excessively complicated and obtuse. Many actors attempt to relieve themselves of responsibility by pointing to their partners and contractors, and it is often impossible to understand how personal data may be used and shared, or what legal basis the service providers are using for their processing operations.

As demonstrated throughout this report, it is unreasonable to assume that consumers can give informed consent to the excessive tracking, sharing, and profiling that pervades in the adtech industry. It is therefore highly doubtful that this comprehensive system of commercial surveillance can be fixed by providing new consent mechanisms or better designed legal documents.

As described in chapter 3, most consumers do not think that having their every move and click being tracked in order to get personalized ads is a fair trade-off. The comprehensive digital surveillance happening across the adtech industry may lead to harm to both individuals, to trust in the digital economy, and to democratic institutions. It seems pertinent to question whether this corporate surveillance is a price worth paying in order to show more personalized content and advertising.[469] In any case, it seems clear that the uncontrolled spread of personal data currently pervading the adtech industry is illegal, and must be curbed.

## 8.2 Authorities must enforce the law

Direct and indirect harms such as manipulation, discrimination, chilling effects, and the propagation of misleading information are all by-products of the systems described in this report, and as a result it seems overdue that regulatory authorities take action to limit these harms as much as possible.

It is welcome that data protection authorities such as the ICO are looking at the infringements that abound in the adtech industry, but investigations also need to lead to concrete actions if the systematic violations do not cease. Although the implementation of the GDPR throughout Europe is a welcome step toward protecting consumers in the digital world, at the time of writing there has been a significant lack of enforcement actions against the major multinational companies that are systemically breaching the law.[470]

Although the workload for data protection authorities across Europe is immense in the wake of the implementation of the GDPR, regulators are still struggling with receiving adequate funding.[471] Consequently, enforcement seems to be lacking even when there is ample evidence of breaches of data protection legislation. There is an urgent need for political will to allocate the necessary resources in order to ensure that consumers and citizens are protected in the digital world.

---

[469] For more information on how the adtech industry is influencing the internet as a whole, see "Targeted Advertising Is Ruining the Internet and Breaking the World", Dr. Nathalie Maréchal https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world

[470] The German Data Ethics Commission has called this an "enforcement gap". "Opinion of the Data Ethics Commission", Daten Ethik Kommission https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.html?nn=11678512

[471] "Data Protection Commission 'disappointed' at budget allocation", Charlie Taylor https://www.irishtimes.com/business/technology/data-protection-commission-disappointed-at-budget-allocation-1.4045248?mode=amp

The transnational cooperation between enforcement authorities is necessary to enforce cross-border cases, and ensure that consumers' privacy is protected regarded of their nationality. Although the GDPR introduced a "one-stop shop" mechanism in an attempt to increase the effectiveness of cross-border enforcement, there are still issues pertaining to how specific cases are assigned. The cooperative mechanisms between national regulators therefore needs to be continuously improved upon to facilitate effective enforcement.

In addition to the GDPR, the use of on-device tracking software such as certain Software Development Kits is also regulated under the ePrivacy Directive. Amongst other things, the directive regulates how companies can access information on consumers' end devices ("terminal equipment").[472] The European Commission has proposed a modernization of the ePrivacy Directive, aiming to replace it with a Regulation on Privacy and Electronic Communications.

This Regulation may, depending on the outcome of the legislative process, add additional protection against the tracking of consumer behaviour online, including provisions mandating privacy by default by software providers, to give consumers greater control and prevent online tracking. Consequently, the adoption of a strong Regulation on Privacy and Electronic Communications, combined with effective enforcement, will particularise and complement the GDPR by protecting consumers from online tracking and profiling.[473]

It is also important that Consumer Protection Authorities are involved and up to date on advertising technology. Although it falls outside the scope of this report, the practices described in this report include a number of breaches of consumer law, and many of the practices may be deemed unfair commercial practices.

Although the adtech industry consists of thousands of companies that are virtually unknown to consumers, the market is dominated by technology giants such as Google, Facebook, and Amazon. To avoid the total dominance of the market, competition authorities must actively look at data concentration in the digital economy. This means that they must look at the market concentration of

[472] "Digital Single Market – Stronger privacy rules for electronic communications", European Commission https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_17

[473] "Open letter to EU Member States", Access Now, BEUC, EDRi, Open Society, and Privacy International https://www.beuc.eu/publications/beuc-x-2019-056_open_letter_in_support_of_the_eprivacy_regulation.pdf

personal data, and use antitrust enforcement when necessary to limit the dominance of the major players.[474]

## 8.3 Marketers and publishers must take responsibility

Due to the privacy-invasive nature of programmatic advertising, it may be an important factor in the prevalence of ad-blocking in web browsers.[475] The ad fraud happening in the digital advertising industry is also a money sink for many companies. In short, publishers and advertisers may be losing a lot of money from some of the current advertising models.[476]

Companies that rely on digital advertising to create revenue, such as brands, marketers, and many publishers, should look toward alternative solutions to the currently dominant adtech system. In order to comply with European law, and to respect the fundamental rights of consumers, the industry should look toward innovative technological solutions that do not rely on widespread broadcasting and collection of personal data.

The customers of many of the adtech companies and data brokers detailed in this report include many of the largest brands on the planet, as well as many small and medium sized businesses. By utilizing technologies that rely on tracking and profiling consumers in order to reach potential customers, these companies are funding massive breaches of fundamental rights. Consequently, brands should take care to not funnel money into an industry that seems to be systematically breaching the law.

As controllers, publishers may be held responsible for the GDPR violations perpetrated by the third and fourth parties that receive personal data through their implementations. Similarly, scandals arising from data breaches and similar cases relating to the adtech industry may blow back on the brands who rely on these companies for facilitating their advertising. This could lead to significant fines and reputational damage to both brands and publishers using these systems.[477] In other words, many of the companies involved in the adtech

[474] "A European competition policy that serves consumers in the digital era", BEUC https://www.beuc.eu/publications/european-competition-policy-serves-consumers-digital-era/html

[475] " In Germany, Use of Ad Blockers Driven by Security, Privacy Concerns", eMarketer https://www.emarketer.com/content/in-germany-use-of-ad-blockers-driven-by-security-privacy-concerns

[476] "Cost of global ad fraud could top $30bn", Christopher Tolve https://www.thedrum.com/news/2019/06/06/cost-global-ad-fraud-could-top-30bn

[477] "Why marketers must conduct GDPR Data Protection Impact Assessments of RTB", Johnny Ryan https://brave.com/dpia/

industry are at risk of their partners putting them out of compliance with the GDPR.

If the practices and processing operations described throughout this report is found to be in breach of the GDPR, the relevant companies, including marketers, publishers, and the adtech companies themselves, must purge their databases of all personal data that has been illegally acquired. This also includes deleting user graphs or profiles built using data that was obtained using illicit methods, or otherwise lacks a valid legal basis. Furthermore, these processing activities should cease until the companies in question can document that they are complying with European law. Meanwhile, marketers and publishers may want to look toward other advertising models that do not rely on the collection and processing of personal data.

Publishers in charge of websites, apps or other types of digital services that enable invasive tracking through their platforms should strongly consider revising their strategy and business models. When deciding on how to create revenue, they must undertake in-depth privacy and risk impact assessments, in accordance with the demands of the GDPR. Publishers should also limit the data they collect themselves, and the data they allow third parties to collect, in line with the data protection principles of data protection by design and by default. The sharing of personal data should in general be limited to what is strictly necessary to provide the service.

## 8.4 Conclusion

With how the adtech industry works today, personal data is being broadcast and spread with few restraints. The multitude of violations of fundamental rights are happening at a rate of billions of times per second, all in the name of profiling and targeting advertising. It is time for a serious debate about whether the surveillance-driven advertising systems that have taken over the internet, and which are economic drivers of misinformation online, is a fair trade-off for the possibility of showing slightly more relevant ads.[478]

The evidence keeps mounting against the commercial surveillance systems at the heart of online advertising. As it stands, the situation is completely out of control, harming consumers, societies, and businesses. It is overdue that change is enacted, and that the currently prevalent practices are curbed.

[478]"Targeted ads are one of the world's most destructive trends. Here's why", Arwa Mahdawi https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy

# 9 Glossary

Adtech company – Company involved in digital advertising technology. May include a large number of different companies, including data brokers, supply side platforms, demand side platforms, third party data providers, and more.

Advertising ID – Unique identifier tied to a mobile phone. Is used to track consumers across services for ad tracking.

Advertising mediation platform – A company that facilitates the display of advertising in mobile app. The equivalent to SSPs on mobile platforms, allowing the publisher to maintain several advertising networks at the same time.

Attribution – The act of measuring ad effectiveness. May involve tracking whether consumers clicked an ad, whether an ad spurred a physical store visit, and other subsequent consumer behaviour.

Audience segment – Categories of consumers with similar traits. Used to score, sort, and target consumers based on similar characteristics.

Behavioural advertising – Online advertising that is microtargeted toward individuals or segments of consumers based on their past, current and future behaviour, which is determined based on extensive tracking and profiling.

Bid request – Transaction in the RTB system where an SSP transmits data to DSPs and DMPs, signalling that there is an ad space/consumer for sale. May contain personal data.

Contextual advertising – Online advertising that is targeted at content instead of at individuals. Rather than using tracking and profiling to provide ads, contextual advertising is tailored to specific websites, news articles, or apps.

Controller – A company or organization that processes personal data, and determines the means and purposes of such processing.

Data broker – Company specializing in collecting, compiling and analysing data about consumers to create profiles and segments that can be used for various purposes. Data brokers collect data from various sources, including from online tracking, credit card transactions, public records, and more. They usually sell data and/or profiles to other companies.

Data management platform (DMP) – Data broker that compiles consumer data from different sources, and provides services to other adtech companies, including data enrichment, compiling profiles, and instructing advertisers and bidders about which consumers to target.

Data subject – An individual whose personal data is being processed.

Demand side platform (DSP) – Adtech company that bids on ad space from SSP on behalf of marketers, as part of the RTB process.

ID syncing / audience syncing/ cookie syncing – Process of combining different identifiers about an consumer to track them across different services and devices.

Major platforms – Large entities that fulfil several roles in the adtech industry, due to vertical integration and control of the supply chain. Includes actors such as Google, Facebook, and Amazon.

Marketers – Companies that want to acquire and retain valuable customers. May include brands, retailers, service providers, etc. They buy advertising spaces from publishers, either directly or through adtech intermediaries.

Measurement – The act of measuring number of ad impressions and clicks on an ad. Often a service provided by independent third party vendors. Also includes services such as fraud prevention and controlling whether ads show up in the correct places.

Processor – A company or organization that processes personal data strictly on behalf of a controller.

Profiles – Compilations of data about an individual consumer. Can consist of enormous amounts of data, and may contain extensive information about an individual's past and present behaviour, predicted future behaviour, and more. Is often used for targeting behavioural advertising. Can be described as "digital twins".

Publishers – Companies such as website- or app-providers, provide information and interactive services to users, and who reach consumers directly. Usually sells advertising space to marketers.

Real-time bidding (RTB) – The process where multiple companies place bids in real time to decide who will display an ad. The process normally consists of multiple partners such as SSPs, DSPs, and DMPs. As a part of the RTB process, personal data may be broadcast to a multitude of companies.

Software development kit (SDK) – A library of code that is used by app developers to integrate different third party functionality in apps. SDKs can also be used for commercial tracking.

Supply side platform (SSP) – Companies who work on behalf of publishers to sell advertising space to DSPs. Works like an auctioneer in the RTB system.

Third party analytics services – Companies and services that provide information to publishers about different types of user metrics, on behalf of the publisher.

Third party vendor – Companies that process data about the consumer, but does not have a direct interface or relationship with the consumer. Includes adtech companies, data analytics providers, data brokers, and more. May provide services directly to marketers or publishers, or use data for their own purposes.

Tracking – The act and technology that allows adtech companies to collect data about consumers as they move around online. Consumers are usually tracked whenever they browse a website or use an app, but tracking is also becoming common in "real life" through technology such as connected devices.

FOR MORE INFORMATION

Øyvind H. Kaldestad
Communications advisor
E-mail: ohk@forbrukerradet.no
https://www.forbrukerradet.no/out-of-control/