DIGITAL PROFILING IN THE ONLINE GAMBLING INDUSTRY

A report on marketing and risk surveillance by the UK gambling firm Sky Betting and Gaming, TransUnion, Adobe, Google, Facebook, Microsoft and other data companies.

A REPORT BY CRACKED LABS, COMMISSIONED BY CLEAN UP GAMBLING

January 2022

Author: Wolfie Christl
Digital Profiling in the Online Gambling Industry

A report on marketing and risk surveillance by the UK gambling firm Sky Betting and Gaming, TransUnion, Adobe, Google, Facebook, Microsoft and other data companies.

A report by Cracked Labs commissioned and published by Clean Up Gambling, January 2022

© 2022

Every effort has been made to ensure the accuracy of the texts in this report. Clean Up Gambling, Cracked Labs and the authors accept no liability in the case of eventual errors.

Clean Up Gambling
11 Horseshoe Crescent, Southend on Sea, Essex, SS3 9WL, UK
https://cleanupgambling.com/

Cracked Labs – Institute for Critical Digital Culture
Gumpendorfer Straße 63b, 1060 Vienna, Austria
https://crackedlabs.org

Author: Wolfie Christl
3.2.10 Personal data processing by Microsoft/Bing ................................................................................................................. 58
  3.2.10.1 Observations on personal data processing from technical tests ................................................................................. 58
  3.2.10.2 SAR information is incomplete ................................................................................................................................. 58
  3.2.10.3 Discussion ....................................................................................................................................................................... 58

3.2.11 Personal data processing by Xandr .................................................................................................................................. 59
  3.2.11.1 Observations on personal data processing from technical tests ................................................................................. 59
  3.2.11.2 SAR information is incomplete ................................................................................................................................. 60
  3.2.11.3 Discussion ....................................................................................................................................................................... 60
Executive Summary

Clean Up Gambling has commissioned Cracked Labs to carry out the most detailed investigation into data flows in the online gambling industry to date.

This investigation lays out the scale and depth of behavioural surveillance and data practices used by online gambling operators. It provides extensive information about the scope of the data flows and the web of third-party companies that receive that data to build detailed and intimate profiles of individuals, often without their knowledge. Such profiles include indicators of personal vulnerability and addictive behaviours, which can then be used to target the most vulnerable. Such targeted messaging needs to be seen in the context of the human impact in online gambling, where:

*The gambling industry spends £1.5 billion a year on advertising, and 60% of its profits come from the 5% who are already problem gamblers, or are at risk of becoming so.*

In particular, the investigation shows:

1. **The online gambling industry processes vast quantities of personal data of a highly sensitive nature** – The investigation shows that gambling platforms do not operate in a silo. Rather, gambling platforms operate in conjunction with a wider network of third parties. The investigation shows that even limited browsing of 37 visits to gambling websites led to 2,154 data transmissions to 83 domains controlled by 44 different companies that range from well-known platforms like Facebook and Google to lesser-known surveillance technology companies like Signal and Iovation, enabling these actors to embed imperceptible monitoring software during a user's browsing experience. The investigation further shows that a number of these third-party companies receive behavioural data from gambling platforms in real-time, including information on how often individuals gambled, how much they were spending, and their value to the company if they returned to gambling after lapsing.

2. **Lack of transparency** – Both online gambling operators and third parties were asked to provide access to the data they were processing on individual consumers, in order to understand how that information was being used. The investigation lays out how the companies responded to those requests, finding that (i) the companies were not transparent about what data would be collected and (ii) did not disclose all data being processed. That lack of transparency makes it difficult for individuals to know what is happening with information being held about them and damages the ability of individuals to exercise their rights.

3. **Potential to exploit vulnerable individuals through behavioural profiling** – Gambling disorders are characterised by repetitive traits that signal a form of addictive behaviour. The potential to exploit such traits is extremely lucrative to gambling platforms. Being able to know what individuals are playing and how to ensure continued engagement has become a reality through behavioural profiling. The investigation shows that such behavioural profiles are being created by the industry. For example, a request for access to personal information was made to Signal, a profiling company owned by the credit reporting giant TransUnion. In response, Signal disclosed detailed personal profiles revealing intimate gambling behaviour. The files contained 186 separate attributes for a single individual. Those 186 attributes painted a detailed and personal portrait of the individual's gambling behaviour, including

---

their propensity to gamble, their favourite games, and their susceptibility to marketing. The profiles also included metrics as to how much they are worth financially to the gambling companies and categorised individuals on their inferred “value” to operators. Additionally, the investigation found that these data profiles were able to determine whether individuals have self-excluded from gambling or not.

**Form of the report**

The findings of the investigation have been provided and analysed in the report “Digital Profiling in the Online Gambling Industry”\(^2\). It further examines data practices by the online gambling platform, Sky Betting and Gaming (‘SBG’). The report further clarifies how SBG works with other third parties, including how SBG transmits and shares data with those third-party companies and how those third parties process personal data. The report was compiled through observations of personal data flows of an individual (‘Data Subject 2’). Those observations were conducted through technical testing on their activities on the SBG websites. This observational data was then supplemented and contrasted with information received by data subjects (Data Subjects 1 and 2) following subject access requests (‘SAR’) to SBG and the third-party companies. The report also gives an overview of profiling in the gambling industry as well as of marketing and risk surveillance.

The report is accompanied by a technical report\(^3\) that presents the raw findings, including details of the responses to SARs and the technical details following the observations of data flows.

The main findings of the investigation relate to (i) the quantity and quality of data being processed, (ii) the lack of transparency over data being processed by gambling companies and the third-party companies that they send data to, and (iii) the potential for such data being used to profile and exploit vulnerable gamblers.

### I. **Quantity and quality of data**

The technical report analyses the evidence on data flows obtained through responses to SARs that were submitted by the two data subjects, as well as the technical testing on Data Subject 2’s activity on websites operated by SBG.

**Tracking by third parties.** As part of the observations of personal data flows by Data Subject 2, it was found that SBG transferred data to third-party companies. For example, 2,154 transmissions of data were made to 44 different digital surveillance companies by just 37 visits to SBG websites.\(^4\) The report shows that companies such as Adobe, Signal, Facebook, and Google received the greatest number of transmissions of data. A high number of transmissions often suggest extensive behavioural profiling but even a single request can be problematic if it transfers extensive information, as it appears occurs in the case of gambling platforms.\(^5\)

**Third-party companies received extensive behavioural data.** Several third-party companies, including Signal, MediaMath, Facebook, Google and Microsoft, received detailed behavioural data on activities by Data


\(^4\) Section 3.2 of the Report.

\(^5\) Ibid.
Moreover, the report shows that intimate information about individual gambling behaviour was being processed and passed to third parties, including an individual’s full gaming history, completed bets, as well as dates and amounts of deposits and withdrawals. Information passed to third parties was used to build profiles about behaviour on gambling platforms, from favourite games and how often individuals stayed online to the percentage of how many marketing emails were read.

**Tracking across websites operated by different companies.** The report outlines how third-party companies can track users across websites, as these companies used the same personal identifiers when visiting a gambling platform as they did when visiting websites of other companies. As a result, those behavioural tracking companies can recognise a visitor on SBG websites as the same individual who visits another website, meaning that third-party companies can profile, track and follow people across various websites. During visits to SBG websites, at least 20 third-party companies stored personal identifiers they use across websites in the user’s browser, including data brokers, such as Oracle, LiveRamp, Salesforce and

---

6 Ibid.
7 Ibid.
8 Section 3.2.1 of the Report.
9 Section 3.2. of the Report.
Tapad, a company owned by Experian. Most of them also learned that the user linked to the personal identifier visited a gambling website, and can potentially further exploit this information.\textsuperscript{10}

**Profiling.** Responses to both data subjects’ SARs show that SBG’s partner company Signal processed up to 186 profile attributes relating to their characteristics and behaviours. This extensive processing provides the framework for advanced profiling to be made on individual consumers, often without their knowing consent.\textsuperscript{11}

### II. Lack of transparency

Data subjects have a right of access to their data under Article 15 of the UK GDPR. This includes confirmation as to whether personal data is being processed by the organisation and if so, the data subject has a right of access to that data. Both Data Subject 1 and Data Subject 2 submitted SARs to SBG and its network of third parties, asking for access to all personal data processed by the various companies. However, several of the companies either initially refused to deal with the requests or returned the disclosure of the data incomplete.\textsuperscript{12}

We are aware from observation of Data Subject 2’s data flows that during their use of SBG’s services, several third-party companies processed personal data on the data subject. Nevertheless, this was not fully disclosed in the SAR responses from SBG.\textsuperscript{13} The network partners were equally not forthcoming. For example, Iovation’s response to the SAR contained only 4 records of data transmissions during website visits. However, the report observed data transmission to Iovation during 7 visits to SBG websites and 5 visits to websites operated by other companies.\textsuperscript{14} The discrepancy was never explained by Iovation.

---

\textsuperscript{10} Section 3.2.7 of the Report.
\textsuperscript{11} Section 3.2.4.5 of the Report.
\textsuperscript{12} Section 3.2 of the Report.
\textsuperscript{13} Section 3.2.1 of the Report.
\textsuperscript{14} Section 3.6.4.4 of the Technical Report.
III. Potential for exploitation of data

Marketing and risk surveillance tools have been developed that allow companies to access profiles of existing and potential customers. Those profiles are built on personal data and records of behaviour collected over various websites and platforms, as well as through other activity, and even information obtained offline.\textsuperscript{15} In short: operators monitor individuals to build rich and granular sets of personal behaviour.

These practices have created a network of interlinked actors that feed such data to each other, including online advertising businesses, data brokers and other companies. This information gleaned about individuals can subsequently be used for advertising and marketing targeted to individual vulnerabilities.\textsuperscript{16} While such advertising is usually seen through the prism of profit, that same technology can be used to maximise engagement.

Increased engagement is particularly acute in the online gambling context. Gambling disorder has been classified as a “behavioural addiction diagnosis”.\textsuperscript{17} Gambling can be addictive and can lead to a gambling disorder. Clean Up Gambling has chronicled how gambling disorders can lead to real-world harms. Real-time monitoring of addictive behaviours allows for this vulnerability to be identified and exploited. In turn, awareness of such behaviours can be used to influence those addictive behaviours, through personalised offers and rewards. The potential for exploitation is aggravated where such profiles are updated in real-time based on an individual’s particular predilections.

The analysis of data flows on the two data subjects in the technical report has shown that specific companies’ websites have access to extensive amounts of personal data pertaining to behaviours of their customers. That personal data is often accessed by third-party companies, which use that information to enhance their own profiles of individuals. However, gambling is a problematic source of such information given the potential to exploit existing vulnerabilities and even addiction.

\textsuperscript{15} Section 2.2 of the Report.
\textsuperscript{16} Ibid.
1. Introduction

Clean Up Gambling has commissioned Cracked Labs to carry out an investigation on digital profiling in the online gambling industry. Clean Up Gambling are represented by AWO, a data rights agency that contributed to the drafting of this report.

The report examines how gambling companies collect and use extensive personal data on players, how they monitor and profile them, and how they may use data against them by exploiting their weaknesses. As an example, we examined the data practices of the UK gambling firm Sky Betting and Gaming (SBG) and its partners.

Technical tests on personal data flows during website visits, responses to legal requests for access to personal data being processed and additional research show that SBG and its partners create far-reaching profiles on players based on granular data on their gambling activities that can potentially be exploited in order to act on them and influence their behaviour.

During the use of its services, SBG transmits personal data to many third-party companies, largely without the user's knowledge. In particular, two companies owned by the credit reporting giant TransUnion receive comprehensive personal data from SBG.

1. Iovation, a fraud detection firm owned by TransUnion that claims to track 7 billion devices globally, constantly assesses whether a player may represent a “risk” to SBG.
2. Signal, a marketing and profiling data firm also owned by TransUnion, constantly assesses and rates how much a player may be worth to SBG, how much should be spent to incentivise further gambling activities and how “promotions” may influence their behaviour. At the same time as assisting with retaining and maximising gambling attention, Signal also processes data on player safety mechanisms such as “self-exclusion”.

In addition to marketing and risk surveillance by two companies owned by TransUnion, SBG transmits extensive data on gambling activities by people who use their services to many other third parties. The list of companies who receive data includes the UK broadcaster and telecommunications company Sky UK and the gambling technology company Playtech, the software vendor and data company Adobe, lesser-known data companies like MediaMath, as well as major platforms such as Facebook, Google and Microsoft. According to our observations, SBG also initiated personal data transmissions to data brokers such as Oracle, Salesforce, LiveRamp, Neustar and Tapad, owned by Experian.

This report contains two parts. First, the report gives an overview of profiling in the gambling industry, risk and marketing surveillance, and technical aspects of digital tracking on websites. Second, it provides a case study on personal data processing by SBG and its partners.

---

18 https://cleanupgambling.com/
19 https://www.awo.agency/
20 Including subsidiaries and related platforms and products.
2. Background

2.1 Profiling in the gambling industry

The gambling industry has long been exploiting data on players to influence their behaviour, to get them to spend more, make them return more often, and maximise profit. After putting electronics and microchips into physical slot machines in the 1960s and 1970s, large international casino companies equipped slot machines with card readers in the 1990s, which then allowed them to collect data on gamblers at the individual level. They introduced loyalty programs, sent personal letters to them and started to gather comprehensive information about the characteristics and behaviours of millions of players. They assigned them customer numbers and collected their names, addresses, birthdates and data about the frequency and duration of visits to the casino, the meals and drinks purchased, the types of hotel rooms booked, and the entertainment programs attended. Above all, casinos started to track the games they play, the times and frequencies they play them, the amounts they bet and how much they win and lose on each play. To gain a line of credit, gamblers disclosed financial details. For games that did not allow for automated tracking, supervisors supplemented the casino company’s profile data by manually entering information from observations about the amounts betted and assessments about how skilled they are playing these games. Data collection was not an end to itself, but a means to act upon players in order to influence their behaviour.21

Losing as a “good experience”. Adam Tanner showed in his book “What stays in Vegas”, how Harrah’s Entertainment, later named Caesars22, became one of the world’s largest casino companies and how it utilised on data on its 45 million loyalty members, who received personalised offers and rewards while collecting loyalty points and moving up from the initial Gold status to Platinum, Diamond and to the “Seven Stars” elite status. Employees had access to an app that told them intimate details about the most valuable customers playing at any given moment, including where they are currently located in the venue.

Tanner describes how the app alerts a supervisor that a top-tier player, who spends around $80,000 annually, lost $688 at this day, yet should have lost only $494, as the slot machines at the venue are set to keep an average of 10 percent of bets. On his last visit he even lost $1,390, according to the data. To appease the player, the supervisor went to the slot machine the player was located at – one out of 1,600 machines at the venue – and singled him out for a friendly conversation. The supervisor later received another alert about a player who had been put into a “behaviour segment” that shows he had been coming less frequently and had been spending less that in the past, according to the data shown in the app. After checking the player’s credit history, the player did not only receive a special greeting, but also $100 worth of free bets.

As Natasha Dow Schüll explained in her book “Addiction by Design: Machine Gambling in Las Vegas”, casinos came up with a “way to measure, act upon and optimize player value” in 2005, even “within the span of an individual play session”. Based on player data, their software calculated personalised “pain points” that indicated how much someone can lose while still being satisfied. When a person approached this pain point, casinos sent a so-called “Luck Ambassador” who provided the player with meal coupons, tickets to shows, gambling vouchers or other rewards, to ease the pain and make losing no less of a “good experience”.23

22 Which now owns a series of UK casino operators, such as William Hill
**Profiling players and influencing behaviour.** Casinos have long been sorting players into different categories, ranking them according to their estimated future value in order to treat them differently. To calculate a customer's likely future spending, one company simply took the amount of their “average bet, multiplied by bets per hour, multiplied by total time gambling, multiplied by the house’s mathematical advantage in the gambler’s preferred game”. Others use sophisticated statistical modelling to calculate how much a player is worth. One casino found that the “customer value” was “strongly associated with frequency of play, type of game played, and the number of coins played per spin or hand”. Players who hit the buttons very fast were easy victims for measures that aimed to make them play more, and others fed a number of “scores” about recency, frequency and spending into personalised marketing algorithms. As early as 2000, the major casino company Harrah’s used data and statistical models to create “behavioural modification reports” that told them that while one group of gamblers would better respond to cash offers, others would play more when being offered a free hotel room.

**Personalised rewards and incentives.** Casinos use a wide range of promotions, perks, and incentives to induce behavioural change, with everything from free food, drinks, entertainment and hotel stays, to chips, bonuses and free plays. Based on profiling, they decide who gets what kind of reward. According to Tanner, the casino company Caesars spent about $25 in perks and rewards per $100 profit at one point. Only $2.50 of that $25 were given to players as a part of the officially advertised loyalty program. An average of $22.50 for every $100 of profit was spent for unpublished personalised offers such as free chips. For players who were rated as “valuable” based on profiling data, Caesars spent a much higher share, while others received significantly less. One gambler quoted by Tanner estimated that he received about $5,000 in free rooms, meals, drinks, spa visits and other perks during his first year at Caesars; at the beginning, he received offers such as $1,000 in free chips. After some time, however, this amount decreased.

Casinos use different channels to deploy personalised behavioural incentives to customers. In addition to getting in touch with players at the venue, this also includes phone calls, letters and email. Around 2013, Caesars sent out 750 million tailored messages and offers to players by mail and email annually. While some players received two or three offers per month, others received up to twenty offers.

**Experiments on gamblers.** The gambling industry has pioneered what has become routine in today’s digital economy: data-driven behavioural experiments on people. More than twenty years ago, Harrah’s started testing hypotheses about what kind of offers that should be sent to which kind of groups of players, in order to make them return more often and spend more. This was based on records of 16 million people from its customer database. To measure the success of the behavioural interventions, Harrah’s used control groups consisting of players who either did not receive any offers or who received different ones. As a result of one such experiment, Harrah’s found that sending certain quickly expiring cash and food rewards to a group of gamblers, who lived nearby and who were observed to hit the buttons of slot machines quickly, made this group visit the venue almost 30 percent more often on average than before.

---

24 Tanner (2014)  
27 Tanner (2014).  
28 Ibid.  
30 Binkley (2000).
“Pavlovian marketing”. Richard Mirman, a mathematician and former consultant at Booz Allen Hamilton who then became Harrah’s chief marketing officer, identified so-called “opportunity segments” – for example, gamblers who appeared to have money and came often but spent little, or those who came infrequently but could be convinced to come more often.³¹ Mirman referred to this kind of behavioural interventions based on analysing customer data and personalised rewards as “Pavlovian marketing”.³²

**Surveillance of risks and undesirables for security purposes.** In addition to profiling for marketing and behavioural change, casinos operate extensive systems to identify and single out suspicious players for security and fraud prevention purposes. Typical large casinos are high-security areas with an estimated 3,000 cameras monitoring every step and activity in order to detect suspicious behavioural patterns and persons; such as troublemakers, thieves, scammers and cheaters. The casinos maintain lists of persons who are denied entry for different reasons, from criminals to gamblers who put themselves on an excluded list to fight their addiction. As in other areas of life, surveillance that is framed to serve security purposes also serves different purposes. In addition to theft or fraud, the gambling industry also wants to prevent players from using legal methods to take advantage – this includes so-called “advantage gambling” and so-called “bonus hunting”.³³

The line between fraud prevention and profit maximisation however became increasingly blurred. When Caesars recognised that some people stayed too long, and consumed too much, in free perks, in relation to how much they spent, the company fine-tuned its loyalty and rewards programs. Its campaign against so-called “grazers” aimed to make sure that gamblers only receive rewards and incentives as long as it benefits the casino’s business goals.³⁴

**In-game personalisation.** Casinos are not allowed to dynamically adjust game mechanics and mathematical odds over the course of a game session; however, they use similar mechanisms that come close to it, but which are considered as “marketing” measures. When a supervisor visits a gambler who loses too much, in order to appease them with a reward, this could be seen as a kind of personalised intervention into the game mechanics. Natasha Dow Schüll points to other practices. For example, a machine may be “set to pay out at the minimum legal payback percentage, or lowest odds allowed” but constantly pays an extra percentage into a “bonus pot”. When players reach their “pain points” according to data analytics, they automatically receive a bonus from the pot. Schüll explains that casinos try to classify such bonus pots as part of a “marketing module” in order to bypass regulations.³⁵

**Online gambling?** In the digital age, personal data collection and personalised manipulation based on profiling and experiments became even more pervasive; almost any technology described above could be applied in online gambling, only much easier, at greater speed and scale. A number of academic papers examined online behavioural tracking in online gambling, however, those mostly investigated the use of data collection for academic research purposes.³⁶ A few media articles revealed how the gambling industry uses data harvested by third-party data companies to target poor people and ex-gamblers via email and digital

---

³¹ Tanner (2014)
³² Binkley (2000)
³³ Tanner (2014)
³⁴ Ibid.
advertising. Generally, however, little is still known about how data is actually collected, shared and utilised by gambling and betting websites. A review of academic studies on “emergent gambling advertising”, published in 2021, concludes that there is “lack of research” that investigates individually targeted advertising online and within mobile apps, which may be “difficult to empirically study due (in-part) to their unpredictable and context-specific nature”. Therefore, it suggests the investigation into online gambling advertisements that use personalised data as an additional future research priority.

A report published by the Gambling Industry Committee in the UK’s House of Lords in 2020 found that the “gambling industry spends £1.5 billion a year on advertising, and 60% of its profits come from the 5% who are already problem gamblers, or are at risk of becoming so”. Gambling operators “have access to vast amounts of data regarding their customers’ age, payment history, any patterns in play and the popularity of specific products”.

2.2 Marketing and risk surveillance in the digital world

In recent years, a wide range of companies has started to monitor, track, and follow people in virtually every aspect of their lives. A vast landscape of data companies has emerged that consists not only of large players such as Facebook and Google, but also of thousands of other businesses from various industries that continuously share and trade digital profiles with each other. Companies have started to combine and link data from the web and smartphones with the customer data and offline information that they have been amassing for decades. Their extensive access to data about the characteristics, behaviours, and lives of consumers allows them to constantly monitor, follow, judge, sort, rate, and rank people as they see fit.

Marketing surveillance. Today, businesses in all industries utilise data, marketing, analytics, and technology services that help them to find, attract, and target valuable new customers, in order to retain existing customers and prospects, and to maximise the profitability or “lifetime value” that they derive from them. Every click on a website and every swipe on a smartphone may now trigger a wide variety of hidden data sharing mechanisms distributed across several companies and, as a result, directly affect a person’s available choices, or determine how personal weaknesses are exploited with calculated efficiency. Digital tracking and profiling, in combination with personalisation, can be used to influence peoples’ behaviour. Personalised offers and persuasion strategies provide the means to effectively influence behaviour at scale. As companies increasingly and unilaterally shape the networked environments and experiences that underlie and determine everyday life manipulative, misleading, deceptive, or even coercive strategies can be automated and customised down to the individual level.

Many businesses try to record and measure every interaction with a consumer, including on websites, platforms, and devices they do not control themselves. The businesses can seamlessly collect rich data about their customers and others in real-time, as well as enhancing them with information from third parties, and

utilise the enriched profiles within the marketing and ad technology ecosystem. Digital advertising has been a major driver for pervasive marketing surveillance, and it is often based on real-time auctions of consumer profiles – a process which has been referred to as “the biggest data breach of all time.”41 The data streams shared between businesses, online advertisers, data brokers, and other companies are not only used to display precisely targeted ads on websites or within mobile apps to users. Rather, they are also increasingly used to dynamically personalise the contents, options, and choices offered to consumers on, for example, a company’s website.

Marketing data firms allow businesses in all industries to combine and link their own data on consumers, including real-time information about purchases, website visits, app usage, and email responses, with digital profiles provided by myriad third-party data providers. The combined data can then be analysed, sorted and categorised, and used to address certain people with certain messages on specific channels or devices. A company could, for example, target a group of existing customers that visited a certain page on its website and who are predicted to become valuable customers, with personalised content or a discount – either on Facebook, in a mobile app, or on the company’s own website. In addition, businesses can conduct tests with different variations of functionalities, website designs, user interface elements, headlines, button texts, images, or even different discounts and prices, and then carefully monitor and measure how different groups of users interact with these variations. In this way, companies systematically optimise their ability to nudge people into acting how they want them to act.

As a side effect, third-party companies that help other businesses to collect, analyse and utilise data, may exploit this data for their own business purposes.

**Risk surveillance.** While people are being constantly rated and assessed on how “valuable” they might be as customers for marketing and advertising purposes, ubiquitous streams of behavioural data are also increasingly being fed into systems that make decisions about whether people may be a risk to a business. With the rise of technology-mediated services, verifying consumer identities and preventing fraud have both become increasingly challenging issues, especially in the light of cybercrime and automated fraud. A number of companies in the risk surveillance industry have aggregated giant databases with sensitive information about entire populations, from names and addresses to information about behaviours, relationships and devices. Their systems monitor, profile, and evaluate payment transactions and many other online interactions for different purposes, including credit assessment, fraud prevention and the verification of identity, age and other claims.

In particular, online fraud detection services use highly invasive technologies to evaluate billions of digital transactions and collect vast amounts of information about devices, individuals, and behaviours that are assessed as “suspicious”. These systems decide whether an application or transaction is accepted or rejected, and which payment and shipping options are available for someone during an online transaction. When people are singled out by such opaque systems they might get flagged as suspicious and warranting special treatment or investigation, or they may be rejected without explanation. They might get an email, a notification, an error message, or the system may simply withhold an option without the user ever knowing of its existence for others. Inaccurate assessments may spread from one system to another and it is often difficult, if not impossible, to object to such negative assessments that exclude or deny, especially because of how hard it is to object to mechanisms or decisions that someone does not know about the decision at all.

Major players in the online fraud prevention space include ThreatMetrix, a company owned by LexisNexis Risk Solutions, that claims to track “100 million transactions per day across 35,000 websites” and “1.4 billion unique online identities from 4.5 billion devices in 185 countries”. ThreatMetrix was funded by the CIA investment firm IN-Q-TEL and has still close links to the US national security complex. Another major player is Iovation, now owned by the credit reporting giant TransUnion, which is further examined in section 3.2.2 of this report. Both LexisNexis Risk Solutions and TransUnion’s Iovation provide specific services for the gambling industry.

**The role of digital identifiers.** In order to monitor and follow people in many situations of their lives, as well as to combine profiles and always recognise these people as the same individuals again, companies collect a wide range of data attributes that identify them in some way. The most relevant identifiers used to link profiles and behavioural data across different databases, platforms, and devices, are email addresses, phone numbers, and unique codes that refer to smartphones or other devices. On the web, personal identifiers stored in browser cookies are attached to users surfing the web. These identifiers are constantly synchronised between different tracking companies, and then often linked with other, more permanent, identifiers. Linking, matching, and synchronising personal identifiers across companies plays a key role in today’s digital profiling ecosystem.

**Data protection law.** Since it came into full effect in May 2018, all personal data processing conducted by companies in the EU, in the European Economic Area (EAA), and in the UK, must comply with the principles and obligations laid out in the General Data Protection Regulation (GDPR). Several personal data processing activities that are common in today’s digital economy raise concerns with respect to their GDPR compliance and as such, experts, civil society organisations and even the European Parliament are doubting whether the GDPR is appropriately enforced. Personal data practices that may be common in the digital economy generally raise concerns, however, these are specifically problematic when applied in contexts such as online gambling.

Assessing the legal compliance of corporate data practices is beyond the scope of this report. However, as soon as companies collect, analyse and utilise extensive personal data and share it with several other companies, this certainly deserves close scrutiny with respect to compliance with GDPR principles such as purpose limitation, data minimisation, fairness, and the existence of a legal basis to process data at large. Ensuring that affected data subjects can use their right of access to personal data companies process about them is a fundamental precondition for GDPR compliance.

---

43 https://www.iqt.org/portfolio?&taxonomy=tech_areas&tax_id=147 [27.10.2021]
44 https://twitter.com/WolfieChristl/status/1286425637855604737
46 Christ (2017)
2.3 Technical aspects of digital tracking on websites: How does digital surveillance work?

Many website operators incorporate tiny pieces of software that transmit data to third-party companies into their websites. This process is usually referred to as “tracking”. Some of these tracking services, such as embedded YouTube videos, provide user functionality or are otherwise visible to users; many of which are invisible to users visiting a website. These tiny pieces of embedded software are usually referred to as web bugs, tags or pixels.\(^{48}\)

When users browse and interact with a website that contains such third-party software, irrespectively of being visible to the user or not, both website operator and third-party companies may receive personal data about the user and their activities via network requests over the Internet.\(^{49}\) Third parties operate servers that receive this information, which are referred to as network hosts.\(^{50}\) For example, as shown in section 3 of this report, websites that incorporate software by Signal send personal data to “s.thebrighttag.com”, a network host operated by Signal.

A website may incorporate software that explicitly transmits personal identifiers, such as an email address, and behavioural data, for instance about the kind of page visited, to a third party. Personal data transmission can also occur implicitly, for example, if it is contained in the so-called HTTP header of a network request to a third party.\(^{51}\)

If a third-party company stores an identifying code in the user’s browser, for example in a cookie, and later receives the same identifying code during a subsequent website visit, it can track and follow this person across several visits and, as such, is certainly processing personal data. We refer to those identifying codes as pseudonymous personal identifiers (consistently with the definition in Article 4(5) GDPR) or cookie IDs in this report. Cookies and similar technologies allow both website operators and the incorporated third-party vendors to store and retrieve information in and from the user’s browser. Cookies are often used to store and retrieve pseudonymous personal identifiers that are later exchanged with yet other companies, in order to track and follow users across websites operated by different companies.\(^{52}\)

The process of different third-party companies exchanging information in a way that aims to give them the ability to track and follow users across websites operated by different companies is usually referred to as “cookie matching” or “cookie syncing”.\(^{53}\) In particular, so-called third-party cookies that are associated with third-party hosts serve this purpose, however, so-called first-party cookies that are associated with the domain of the website operator can also help to facilitate tracking across websites and companies.\(^{54}\) Pseudonymous identifiers that refer to specific persons are the basis for any other personal data processing that allows companies to profile and act on those persons.

---

\(^{48}\) Christl (2017)


\(^{50}\) https://en.wikipedia.org/wiki/Host_(network)

\(^{51}\) https://en.wikipedia.org/wiki/List_of_HTTP_header_fields


Some third-party companies that track users who are visiting a website may process very little personal data or process it strictly on behalf of the website operator, whereas other companies may exploit the recorded data for their own business purposes, or even facilitate personal data processing to yet other third-party companies.\textsuperscript{55}

\textsuperscript{55} See e.g. The Cybersecurity Effects of Fourth-Parties on Websites (2020): https://www.reflectiz.com/blog/the-cybersecurity-effects-of-fourth-parties-on-websites-2/
3. Case study: Sky Betting and Gaming (SBG) and its partners

SBG is a UK gambling company owned by The Stars Group that operates several gambling and betting websites and apps including Sky Bet, Sky Vegas, Sky Casino, Sky Bingo and Sky Poker. The Stars Group was recently bought by Flutter Entertainment. We examine how SBG processes personal data, how it profiles gamblers and how it shares data with third parties. To do so, we use three types of sources:

- **Subject access requests (SARs):** Information on personal data processing obtained directly from SBG and other companies. For this purpose, two persons who we refer to as “Data Subject 1” and “Data Subject 2” used their right of access to the personal data a company is processing on them.
- **Technical testing:** Observations on personal data flows that occur when a person visits or uses websites operated by SBG. For this purpose, we assisted a person who we refer to as “Data Subject 2” with observing and recording personal data processing in their browser during visits to SBG websites.
- **Desk research:** Publicly available information on corporate data practices from sources such as corporate websites, legal statements, developer documentation, news articles, academic research, and other reports.

The investigation focuses on personal data processing that occurs as a result of using websites and apps operated by SBG, in particular on:

- **Sky Casino**, an online gambling environment available on the web (skycasino.com) and as a mobile app.
- **Other SBG websites, which** were also subject to the investigation but to a lesser extent. This includes Sky Bet, an online betting site available on skybet.com, and Sky Vegas, another online gambling site available on skyvegas.com.

Websites operated by SBG, such as skycasino.com, transmit extensive personal data to several third-party companies, both when using these websites as an “anonymous” visitor and when using them as a registered and logged-in customer. Therefore, the investigation also addresses how SBG shares personal data with other companies and how they process it.

**Detailed evidence about the findings presented in this section** is laid out in the accompanying technical report, which contains the result of our examination about personal data flows based on SAR information and browser tests.

### 3.1 Methodology – observing data flows and SARs

From the year 2009, a person who we refer to as **Data Subject 1** has been a customer, and extensive user, of SBG services. In 2018, this person submitted an initial SAR to SBG. The responses revealed that two third-party companies, Signal and Iovation, were also processing personal data on Data Subject 1 while using SBG services. Responses to subsequent SARs to SBG, Signal and Iovation, submitted throughout 2020, revealed...
that both Signal and Iovation had been processing personal data in a way that can be considered monitoring and profiling of Data Subject 1. Data Subject 1 is not convinced that SBG and its partners have provided sufficient information on their personal data processing to satisfy the requirements of Article 15 GDPR, and thus continues to seek access to that data.

To better understand how SBG and its partners process personal data on gamblers, another person who we refer to as Data Subject 2 used SBG services in February and March 2021. We assisted Data Subject 2 with observing and recording personal data flows in the browser during their visits to SBG websites. The observations revealed that not only Signal and Iovation, but also a number of other companies, were processing personal data on SBG websites visitors and customers, including Sky UK, Adobe and MediaMath. Based on these observations, Data Subject 2 submitted SARs to SBG, Signal, Iovation, Adobe, MediaMath and Sky UK.

The next sections summarise what we have learned about how SBG and its partners process personal data based on the observations in the browser of Data Subject 2 and on the responses to SARs submitted by Data Subject 1 and Data Subject 2.

### 3.1.1 Technical tests

Data Subject 2 was using SBG services for a short period in February and March 2021. We assisted Data Subject 2 with observing data flows in their web browser during their use of SBG services, in order to better understand how SBG and its partners process personal data.

Data Subject 2 used a newly bought Windows 10 laptop, set it up and connected it to the Internet at their home in the UK. They visited the SBG websites skycasino.com, skybet.com and skyvegas.com several times, registered an account at skycasino.com, deposited cash, played games, won and lost money, withdrew cash, briefly used the Sky Casino iPhone app, clicked on links in marketing emails sent by SBG and set up a 24-hours “cool off” period. In total, Data Subject 2 visited the SBG websites skycasino.com, skybet.com and skyvegas.com 56 times. Network traffic has been recorded and archived for 37 website visits using the built-in “developer tools” in the Google Chrome browser and stored in the form of HTTP archive (HAR) files.60 For one recorded visit to skybet.com, the Microsoft Edge browser was used. In addition, Data Subject 2 visited a range of other gambling websites and the website asos.com, in order to examine personal data processing across websites operated by different companies.

When SBG websites showed “cookie banners” to Data Subject 2, ostensibly to give the data subject control over the use of cookies, that banner did not offer them a “reject” button. Rather, they were only offering an “Accept and Close” button. The banner therefore served no useful purpose. Data Subject 2 clicked “Accept and Close” to proceed. The below screenshot shows the cookie banner displayed at skycasino.com:

---

60 [https://github.com/GoogleChrome/devtools-docs](https://github.com/GoogleChrome/devtools-docs)

When Data Subject 2 was asked whether they "would like to receive exclusive bonuses, free spins and communications" during user registration, they chose “Yes”:

![Image of a pop-up asking for contact preferences]

Before visiting SBG websites, Data Subject 2 used Google Chrome to visit 30 of the 50 most visited websites in the UK according to Alexa. With the exception of Google.com, Data Subject 2 did not interact with these websites in any way. Data Subject 2 “consented” to Google’s data collection because they assumed this is the default behaviour for most Internet users.

---

62 Google.com, Youtube.com, Amazon.co.uk, Google.co.uk, Bbc.co.uk, Ebay.co.uk, Ladbible.com, Twitch.tv, Yahoo.com, Facebook.com, Microsoft.com, Vk.com, Imgur.com, Aparat.com, Theguardian.com, Rightmove.co.uk, Fandom.com, Sportbible.com, Roblox.com, Lmdb.com, Dailymail.co.uk, Unilad.co.uk, Bt.com, Virginmedia.com, Chess.com, Bing.com, Amazon.com, Argos.co.uk, Sky.com, Hotukdeals.com
3.2 Findings on personal data flows

Based on observations from technical tests, we find that SBG processes extensive personal data both on registered customers and on people who visit their websites as “anonymous” users.

During 37 visits to the SBG websites skycasino.com, skybet.com, and skyvegas.com, we observed 2,154 network requests to 83 third-party hosts operated by at least 44 third-party companies. Put differently, during 37 visits to SBG websites, SBG transmitted data to at least 44 third-party companies in the background hundreds of times.

Tracking by third parties. The following table shows an overview of companies who received data during 37 visits to SBG websites by Data Subject 2, including the number of times they were contacted over the Internet:

<table>
<thead>
<tr>
<th>Company</th>
<th>Classification of the company’s services</th>
<th>Number of times the company received data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal (TransUnion)</td>
<td>Marketing, personalization, profiling</td>
<td>401</td>
</tr>
<tr>
<td>Iovation (TransUnion)</td>
<td>Fraud, identity, risk</td>
<td>28</td>
</tr>
<tr>
<td>Locate</td>
<td>Identity</td>
<td>5</td>
</tr>
<tr>
<td>Playtech</td>
<td>Gambling analytics</td>
<td>12</td>
</tr>
<tr>
<td>Adobe</td>
<td>Marketing, personalization, profiling</td>
<td>499</td>
</tr>
<tr>
<td>Facebook</td>
<td>Platform, adtech, data</td>
<td>358</td>
</tr>
<tr>
<td>Google</td>
<td>Platform, adtech, data</td>
<td>240</td>
</tr>
<tr>
<td>Qubit</td>
<td>Marketing, personalization, profiling</td>
<td>129</td>
</tr>
<tr>
<td>Ve Interactive</td>
<td>Marketing, personalization, profiling</td>
<td>48</td>
</tr>
<tr>
<td>MediaMath</td>
<td>Adtech, data</td>
<td>77</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Platform, adtech, data</td>
<td>71</td>
</tr>
<tr>
<td>Xandr / AT&amp;T</td>
<td>Adtech, data</td>
<td>22</td>
</tr>
<tr>
<td>IDS</td>
<td>Data</td>
<td>8</td>
</tr>
<tr>
<td>Oracle</td>
<td>Data</td>
<td>8</td>
</tr>
<tr>
<td>Verizon Media / Yahoo</td>
<td>Platform, adtech, data</td>
<td>6</td>
</tr>
<tr>
<td>ComScore</td>
<td>Data</td>
<td>6</td>
</tr>
<tr>
<td>OpenX</td>
<td>Adtech, data</td>
<td>5</td>
</tr>
<tr>
<td>Tapad / Experian</td>
<td>Data</td>
<td>4</td>
</tr>
<tr>
<td>PubMatic</td>
<td>Adtech, data</td>
<td>4</td>
</tr>
<tr>
<td>Index Exchange</td>
<td>Adtech, data</td>
<td>4</td>
</tr>
<tr>
<td>Magnite</td>
<td>Adtech, data</td>
<td>4</td>
</tr>
<tr>
<td>Semasio</td>
<td>Adtech, data</td>
<td>4</td>
</tr>
<tr>
<td>Medianrithmics</td>
<td>Adtech, data</td>
<td>4</td>
</tr>
<tr>
<td>FreeWheel / ComCast</td>
<td>Adtech, data</td>
<td>2</td>
</tr>
<tr>
<td>Sonobi</td>
<td>Adtech, data</td>
<td>2</td>
</tr>
<tr>
<td>LiveRamp</td>
<td>Data</td>
<td>2</td>
</tr>
<tr>
<td>Neustar</td>
<td>Data</td>
<td>2</td>
</tr>
<tr>
<td>Twitter</td>
<td>Platform, adtech, data</td>
<td>2</td>
</tr>
<tr>
<td>Salesforce</td>
<td>Data</td>
<td>1</td>
</tr>
<tr>
<td>Adform</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>The Trade Desk</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>Iponweb</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>FlashNetwork</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>SmartClip / RTL Group</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>AdScale / Strider Media</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>Storm</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>ZoeTap</td>
<td>Data</td>
<td>1</td>
</tr>
<tr>
<td>Smart AdsServer</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>GumGum</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>Videoom</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>Voluum</td>
<td>Adtech, data</td>
<td>1</td>
</tr>
<tr>
<td>New Relic</td>
<td>Application monitoring</td>
<td>168</td>
</tr>
<tr>
<td>Report URI</td>
<td>Application monitoring</td>
<td>52</td>
</tr>
<tr>
<td>Cloudflare</td>
<td>Content delivery</td>
<td>2</td>
</tr>
<tr>
<td>Requests to hosts operated by unknown companies</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>
Among the third-party companies who received the greatest number of network requests while visiting skycasino.com, skybet.com, and skyvegas.com, are Adobe (499), Signal (401), Facebook (358), Google (240), Qubit (129), MediaMath (77), Microsoft (71), Ve Interactive (48), Iovation (28) and Xandr (22). 19 companies received between 2 and 10 requests, and 13 companies received only one request. A low number of requests does not necessarily mean that the data transmitted is not highly sensitive. While a high number of requests can point to extensive behavioural profiling, a single request to a host operated by a third-party company that transmits wide-ranging information can also enable problematic data practices.

Personal data processing by third-party companies. In many cases, these third-party companies processed or received personal data on Data Subject 2. This includes the following companies:

- **Iovation**, a fraud prevention firm that claims to collect data on 7 billion devices across 50 countries, and which was acquired by the major credit reporting firm TransUnion in 2018. 63
- **Signal**, a company that provides consumer data and profiling services for marketing purposes, which was acquired by TransUnion in 2020. 64
- **Adobe**, a major software company that also provides consumer data and profiling services for marketing purposes. 65
- **Sky UK**, a UK broadcaster and telecommunications company, who has partnerships with SBG. 66
- **MediaMath**, a digital advertising company that claims to have data on “more than a billion consumers”. 67
- **Playtech**, a gambling technology company that is mentioned as a software provider in SBG’s terms and conditions. 68

Other companies who processed or received personal data during visits to SBG websites include platform giants Facebook, Google, Microsoft and Yahoo (Verizon Media), as well as advertising and data companies such as Xandr (AT&T), PubMatic and Flashsalking, and companies commonly referred to as data brokers, such as Oracle, Salesforce, LiveRamp, Tapad (Experian) and Neustar. We did not further examine data transmissions to other advertising and data companies such as OpenX, Index Exchange, The Trade Desk, Magnite, Adform, Smartclip, Sovrn, Semasio, Freewheel (ComCast), Sonobi, Iponweb, ID5, Comscore and ZeoTap.

We observed many network requests to the host “smetrics.sky.com”, which appears to be jointly operated by Adobe and Sky UK. 70 When we mention data transmission to “Adobe (Sky UK)” in the next sections, this refers to data transmission to the host smetrics.sky.com.

68 Sky Casino and other SBG sites are actually operated by its subsidiary Bonne Terre Limited, which has several brand license, advertising services and commercial relationship agreements with Sky UK: https://sec.report/Document/0001104659-18-046311/ [12.8.2021]
71 While the domain sky.com is owned and operated by Sky UK, smetrics.sky.com is a CNAME record that points to sky.com.ssl.d1.sc.omtrdc.net. The domain omtrdc.net is owned and operated by Adobe.
Third-party companies received extensive behavioural data. During visits to skycasino.com, several third-party companies received detailed personal data on behaviours and activities conducted by Data Subject 2 while visiting skycasino.com, including on the pages visited, the games played, customer registration, cash deposits and withdrawals and login activities. For example, when Data Subject 2 deposited £30 at Sky Casino, this information, including the cash amount, was immediately sent to Signal, Adobe (Sky UK), MediaMath, Facebook, Google and Microsoft. Iovation also received information about the fact that Data Subject 2 deposited cash at Sky Casino.

The following chart shows examples of behavioural data received by third-party companies when Data Subject 2 used the website skycasino.com:

Together with behavioural data, Signal, Iovation, Adobe (Sky UK), MediaMath, Facebook, Google and Microsoft received at least one personal identifier referring to Data Subject 2 from a cookie stored in the browser. Google and MediaMath also received the customer ID that SBG assigned to Data Subject 2 when they registered an account. In addition, MediaMath received the SBG username of Data Subject 2.

The gambling technology firm Playtech did not receive identifiers from cookies but rather directly received the SBG username. When Data Subject 2 played Sky Casino’s slots game “Djinn of Storms”, Playtech received behavioural data on every spin, as well as the amounts bet, won, and lost.

Tracking across websites operated by different companies. During visits to skycasino.com, SBG initiated network requests to several third-party companies that transmitted personal identifiers from cookies in the browser of Data Subject 2 to them. We refer to these identifiers as Signal ID, Iovation ID, Adobe ID, MediaMath ID, Facebook ID, Google ID and Microsoft ID. Several third-party companies received the same

Digital Profiling in the Online Gambling Industry. Report, December 2022

2021 Clean-Up Gambling / Cracked Labs
personal identifiers when Data Subject 2 visited websites operated by other companies, for example, when they visited the online retailer asos.com or the betting websites boylesports.com, betway.com and unibet.co.uk. The following chart shows which third-party companies received personal identifiers across websites:

Some third parties received personal identifiers during visits to skyscasino.com and stored those identifiers in cookies in the browser of Data Subject 2. Those third parties included Signal, Iovation, Adobe and Google. The stored personal identifiers were then being transmitted to those third parties during visits to websites operated by other companies, by way of a signal of a visit taking place. As SBG initiated the storage of personal identifiers that are also being processed during visits to other websites, SBG would be facilitating the personal data processing by websites operated by other companies.

In some cases, we observed that a third party had been processing one single personal identifier across websites operated by different companies over weeks (e.g. Signal and Iovation). In other cases, we observed that a company had been constantly replacing one personal identifier with another one, but was still able to know that those identifiers refer to the same person (e.g. Google). We also observed companies processing two or more personal identifiers referring to Data Subject 2 (e.g. Adobe and Google), as well as companies processing one type of personal identifier only during visits of skyscasino.com but another across websites operated by different companies (e.g. Adobe).
As these third parties can recognise a visitor to skycasino.com as the same person when they visit a website operated by another company, these third parties can potentially track, follow and profile people across websites.

**SARs.** After the technical tests, Data Subject 2 sent SARs to SBG, Signal, Iovation, Adobe, Sky UK and MediaMath. While Signal, Iovation and MediaMath provided some information about their personal data processing activities on Data Subject 2, Adobe and Sky UK did not provide any information about personal data processing related to the use of SBG services. SBG itself provided some information about personal data processing on its own systems but the information provided about personal data processing by third-party companies was incomplete. SBG did not provide any information about personal data processing by Playtech, Facebook, Google, Microsoft and other third-party companies to Data Subject 2.

**Player profiling.** Section 2.1 shows that behavioural data on gamblers can potentially be used for profiling. The gambling industry typically uses profiling based on behavioural data as a means to act upon players in order to influence their behaviour. According to the responses to SARs from Data Subject 1 and Data Subject 2, Signal has actually been processing extensive personal data on their characteristics and behaviours that can be useful for profiling or are the result of advanced profiling.

Signal stored up to 186 profile attributes about the data subjects. The following table shows examples of profile data processed by Signal, according to its responses to the SARs:

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples of attributes processed and stored by Signal</th>
<th>These attributes can be considered raw personal data and can be useful for profiling.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Information that can be useful for profiling</td>
<td>Date of account creation, account balance, number of deposits, date of the last login, last browsed category, whether a customer has ever bet on football, date of the first and the last bet, number of days since the last football bet, number of “rounds” played in a certain game, whether a customer is excluded from receiving free bets</td>
<td></td>
</tr>
<tr>
<td>(2) Information that is the result of basic inferences</td>
<td>Email open rate, favorite SBG product, second favorite product, favorite type of game at Sky Casino, whether a customer became inactive at Sky Casino</td>
<td>These attributes are the result of basis inferences, and can, at the same time, be useful for further profiling.</td>
</tr>
<tr>
<td>(3) Information that is the result of advanced profiling</td>
<td>Customer group (e.g. &quot;high value&quot;), customer lifestage (e.g. &quot;winback&quot;, &quot;grow&quot;), overall customer value score (1-9), overall customer value band (e.g. &quot;very high value&quot;, &quot;low value&quot;, &quot;very low value&quot;), separate value scores and bands for each product (e.g. Sky Poker, Sky Bingo, Sky Vegas), potential cross sell product (e.g. Sky Vegas), winback margin (&quot;predictive model for how much a customer would be worth if they returned over next 12 months&quot;, e.g. £ 1190.46), predicted share of a customer's betting wallet compared to competitors (e.g. 10%), promo influence score (&quot;whether the customer is positively or negatively influenced by promotions&quot;), segment (e.g. &quot;2 days or less&quot;, &quot;slots 3+ days&quot;, &quot;slots 3-4 days&quot;, &quot;daily football - mostly pre&quot;)</td>
<td>These attributes are also the result of inferences. However, neither SBG nor Signal disclosed how these inferences were calculated.</td>
</tr>
</tbody>
</table>
The following chart shows examples of profile data SBG and Signal collected about Data Subject 1, according to their responses to the SARs:

The next sections describe in detail how Iovation, Signal and other companies have been processing personal data on Data Subject 1 and Data Subject 2 according to technical tests and SARs.

### 3.2.1 Personal data processing by SBG

SBG ultimately initiates all personal data processing that occurs during the use of its services. This includes any personal data processing by third-party companies during visits to its websites as described in the previous and the next sections.

SBG itself processes extensive personal data on users and customers of its services in order to provide those services to them. Naturally, SBG has access to data about almost any user activity on its websites. Still, it must comply with data protection law and can only process personal data for lawful purposes. Compliance includes providing a data subject with sufficient information about personal data processing in response to a SAR that satisfies the requirements of Article 15 GDPR. As the previous and the next sections show, the information provided in response to SARs by SBG is incomplete.

As long as a third-party company processes personal data on behalf of SBG based on a contractual relationship with that third party, SBG is likely responsible for this personal data processing as the data controller. The responses to SARs suggest that SBG has contractual relationships with at least Signal, Iovation, Adobe and MediaMath. While these companies may process personal data on behalf of SBG, they may also process data for their own purposes. Technical testing and responses to SARs suggest that several third parties also process personal data for their own business purposes.

For example, we observed Signal and Iovation storing personal identifiers in the user’s browser during visits to SBG websites. The same identifiers are also being received by Signal and Iovation during visits to websites
operated by other companies. Processing personal data across websites operated by different companies is not restricted to personal data processing on behalf of SBG. While it appears that SBG facilitates this personal data processing across websites, third-party companies are also responsible for their own processing.

According to SAR responses, SBG itself processed a wide range of personal data about Data Subject 1 and Data Subject 2 on its own systems. This includes, among others:

- The full gaming history (product, stake, return and date for every game played).
- A list of completed bets.
- A list of free bets and tokens.
- Dates and amounts of deposits and withdrawals.

As the following table shows, this data is extremely comprehensive for Data Subject 1:

<table>
<thead>
<tr>
<th>Data category</th>
<th>Number of entries stored by SBG (data subject 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaming history</td>
<td>5,717</td>
</tr>
<tr>
<td>Completed bets</td>
<td>44,063</td>
</tr>
<tr>
<td>Free bets</td>
<td>826</td>
</tr>
<tr>
<td>Deposits and withdrawals</td>
<td>1,359</td>
</tr>
</tbody>
</table>

3.2.2 Personal data processing by Playtech

Playtech72 is a gambling software company that is mentioned as a software provider in SBG’s terms.73

3.2.2.1 Observations on personal data processing from technical tests

According to our technical tests, Playtech processed the following personal data on Data Subject 2:

- During one visit to the skycasino.com website, Data Subject 2 played several rounds of a game called "Djinn of Storms". We observed 12 network requests that transmitted data to Playtech during this website visit.74
- Playtech received detailed behavioural data on how Data Subject 2 interacted with the game, including data on every spin, the amount won or lost, and information about the exact date and time the activity occurred.
- Each data transmission included the SBG username of Data Subject 2.

3.2.2.2 SAR information is incomplete

SBG did not provide information about the observed personal data processing activities by Playtech to Data Subject 2 upon their SAR.

3.2.3 Personal data processing by Iovation (TransUnion)

Iovation is a subsidiary of TransUnion, a large credit reporting agency and data broker, and provides “identity verification, authentication and fraud prevention” solutions. It states that it “collects billions of global online and offline consumer data points”. Iovation promises its clients to use “online and offline data to get the most accurate view of a consumer’s identity, behavior and reputation” to help them “[d]iscover the real stories

---

72 https://en.wikipedia.org/wiki/Playtech
74 We observed data transmission to the network host tgw.bit.ptechna.io, which is operated by Playtech
behind billions of consumer data points and devices”. It promises to help them keep their “websites and apps secure from fraud by identifying suspicious devices the moment they try to connect” and “[i]nstantly know which devices and consumers [they] can trust, and which ones [they] can’t”. Iovation states that it tracks 7 billion consumer devices globally. It claims that it has tracked and “protected” 54 billion customer transactions since 2004 and that its “customers and analysts” have “contributed 83 million reports of fraud and abuse attempts”.

**Products for the gambling industry.** Iovation provides its products, among others, to the gambling industry and promises to help them to handle “fraud challenges from registration right through to withdrawal”, to “instantly recognize who is an honest player, and who is a repeat abuser” and prevent a wide range of undesired behaviours such as “account takeover”, “cheating”, “player collusion”, “bonus abuse” and “license agreement violations”. It states that it “immediately know[s] the “reputation” of a “device that tries to connect to [a client’s] site or app”, including the “reputation of other devices in its history”.

Iovation markets its products for the gambling industry in a way that suggests that consumer profiling for the purposes of fraud prevention may quickly turn into consumer profiling for marketing purposes. It suggests that by using Iovation’s services, gambling companies can “[t]reat [their] good players like VIPs, while blocking cheats and crooks”, “[i]dentify VIPs and keep [their] best players coming back” and even “[k]eep [their] customers playing longer and coming back for more”. Tying together the constant evaluation a consumers’ risk potential with the evaluation of their economic potential as a customer is a wider trend in today’s data industry.

At the same time, Iovation provides solutions to “[m]anage player self-exclusion and promote responsible gambling” by helping clients to “identify and block” gamblers who self-excluded. In a presentation from 2020 available on the web, Iovation states that it handled 483 million gambling transactions in the last 12 months and that more than hundred “gambling operators” and “platform providers” use Iovation. It also provides advice for how to optimise the “gambling player’s journey”.

**Global risk surveillance.** Iovation states it has a “360-degree view of consumer identity” based on “online and offline data sets” that “create a precise view of personal and digital identity”, including “[u]p to five years of historical device data”. It collects “over 100 device attributes” to either “recognize an existing device and return its ID” or it “assign[s] a new ID to the device”. Iovation states that it “provides real-time view into associations between devices via common accounts across Iovation subscribers” and “tracks relationships between devices and accounts”, which suggests that it processes data across clients.

In addition, it offers its clients to “[c]onfidently identify devices associated with good loan applicants” in order to “[r]ecognize good loan applicants from their first visit” by “leveraging insights from your [their] business or from any of the 35,000 brands we protect globally”. This suggests that Iovation combines device data and financial data.

---

78 See p.10: https://crackedlabs.org/dl/CrackedLabs_Chrisl_CorporateSurveillance.pdf
Iovation claims that “devices or accounts associated with fraud are linked together without relying on personally disclosed information”. As “personally disclosed information” is not a term in data protection law, this is a questionable statement. According to the TransUnion page about Iovation’s system, it “offers an accurate and comprehensive view of each consumer by linking proprietary data, personal data, device identifiers and online behaviors”.86

**Risk scoring.** Iovation states it “tracks over 50 different types of fraud” and the “actionable Approve/Review/Deny response” it provides to clients would include “detailed reasons why a transaction was denied”.87 A presentation from 2017 lists examples of fraud types tracked by Iovation, referring to financial services, gambling and other areas. Fraud categories listed include “potential fraud”, “loan default”, “abusive to support”, “policy/license violations”, “promotion abuse”, “arbitrage betting”, “gold farming”, “collusion”, “chip dumping”, “all-in abuse”, “trading restrictions” and “requested exclusion”. The presentation confirms that Iovation processes data on device associations across industries and clients, and mentions additional device attributes such as the list of installed fonts.88 Iovation also states it provides access to a “network of 6,000 fraud and security analysts” who investigate and provide millions of fraud reports.89

Iovation’s SureScore product combines data on “30 million subscriber-placed fraud reports”, data on “billions of online transactions across the globe”, data on “millions of device and transaction attribute permutations” and data on “hundreds of device and transaction attributes” to calculate a risk score for every online interaction based on machine learning. It promises clients to return a score for “100%” of their transactions, even when they “have no prior experience with the customer and/or device”.90 SureScore promises to identify “attributes of trustworthy customers”. Iovation suggests that clients can “offer special incentives and reduce spending caps” for “customers who return a high trust score”. 91

### 3.2.3.1 Observations on personal data processing from technical tests

According to our technical tests, Iovation processed the following personal data on Data Subject 2:

- During visits to skycasino.com and skyvegas.com, we observed 28 network requests that transmitted data to Iovation.92 We also observed network requests to Iovation during visits to websites operated by other companies.
- Iovation received the same personal identifier referring to Data Subject 2 (“Iovation ID”) from Iovation’s “io_token” cookie93 in the browser of Data Subject 2 across visits to skycasino.com, skyvegas.com and visits to websites operated by several other companies. Iovation also stored the Iovation ID1 in the “io_token” cookie in the browser of Data Subject 2 across visits to skycasino.com, skyvegas.com and visits to websites operated by several other companies.
- Websites operated by other companies that received and stored the same Iovation ID include boylesports.com, betway.com, sportnation.bet, gentingbet.com and redzonesports.bet. At least four

---

89 [https://content.iovation.com/resources/device-risk.pdf](https://content.iovation.com/resources/device-risk.pdf) [3.10.2021]
90 [https://content.iovation.com/case-studies/iovation-SureScore-datasheet.pdf](https://content.iovation.com/case-studies/iovation-SureScore-datasheet.pdf) [3.10.2021]
91 [https://content.iovation.com/resources/iovation-SureScore-datasheet.pdf](https://content.iovation.com/resources/iovation-SureScore-datasheet.pdf) [3.10.2021]
92 We observed data transmission to the network host mpsnare.iesnare.com, which is operated by Iovation
93 “ok_token” is the name Iovation uses for this cookie
of these websites stored the Iovation ID in a cookie in the browser without any kind of confirmation or consent from Data Subject 2.

- Iovation also stored the Iovation ID in the local storage of the browser of Data Subject 2 in a way that is only accessible to the SBG domain www.skybet.com.
- We observed Iovation processing information about the device (operating system, CPU type), browser (type, version), language settings, screen size and installed browser extensions of Data Subject 2.

3.2.3.2 Evidence on personal data processing via SARs

As responses to their SARs, and after extensive back-and-forth correspondence, both Data Subject 1 and Data Subject 2 received information about personal data Iovation processed on them:

Information provided. Data Subject 1 received a spreadsheet that contains information about 423 transactions Iovation recorded during visits to SBG websites, each transaction record containing 50 attributes. Data Subject 2 received a spreadsheet that contains information about 4 transactions Iovation recorded during visits to SBG websites, each transaction record containing 49 attributes. In both cases, not every attribute contains a value.

The information on transactions provided by Iovation shows that it has been processing extensive personal data about both data subjects during their use of SBG websites and mobile apps:

- **Activity data.** The provided transaction records are related to activities a data subject conducted during visits to SBG websites. They contain information about the SBG product used (e.g. Sky Casino, Sky Bet, One Vegas), the type of activity conducted (e.g. registration, initial deposit, deposit, withdrawal, “split withdrawal”, “my account”), as well as the exact date and time the activity was conducted. Every transaction record contains a unique “tracking ID”.

- **Identifiers.** Each transaction record contains the SBG username of the data subject, an IP address, a “device ID” and several “tokens” that contain personal identifiers. It also includes an attribute that indicates whether Iovation considers a data subject's device to be “new” or not.
  - The spreadsheet provided to Data Subject 1 contains 85 different IP addresses, 313 different personal identifiers in an attribute labelled “lstoken”, 421 different personal identifiers in an attribute labelled “jtoken” and 83 different device IDs. For 83 out of 423 transactions, Iovation considered the device of Data Subject 1 to be “new”.
  - The spreadsheet provided to Data Subject 2 with information about 4 transactions always contains the IP address of Data Subject 2 and each transaction record contains the same device ID. For one transaction, Iovation considered the device of Data Subject 2 to be “new”. The attribute labelled “jtoken” always contains the “Iovation ID”, which we observed in the web browser during several visits to websites operated by SBG and by other companies. Three other attributes labelled “ctoken”, “lstoken” and “wdbtoken” also contain the “Iovation ID” we observed in the browser.

- **Device data and fingerprinting.** The provided transaction records also contain information about the devices, browsers and type of internet connectivity used by the data subjects, including device type, operating system version, browser name and exact version, screen resolution, language settings, and the internet service provider used. In some cases, those attributes indicate that Iovation tracked a transaction during the use of SBG services on a mobile phone. In other cases, they indicate that Iovation tracked transactions during visits to SBG websites. In addition, the provided transaction records contain information about the so-called “black box”. According to explanations provided by
Iovation this “black box” is a file that collates device attributes. 94 This suggests that Iovation uses the device attributes to generate a unique digital fingerprint of a device in order to recognise it again. Transaction records provided by Iovation also include a “blackbox timestamp” that contains information about the “time and date that the Iovation Black Box was created”. Another attribute contains the “time and date that the device was first seen by Iovation’s systems” and an attribute labelled “iggy” that also appears to collate information about the device used by a data subject.

- **Location data.** The records provided also contain information about the location of which a transaction was conducted by a data subject, including latitude, longitude, city, region, and country. While the latitude and longitude attributes contain very detailed coordinates with a precision of 4 or 5 decimal places (1-10m), they often point to locations that are few hundred meters or even a few kilometres away from the locations the data subjects have actually been at, according to their statements. This suggests that Iovation may infer the locations from IP addresses or from other data.

- **Profiling and (semi)automated decisions.** The transaction records provided by Iovation contain several attributes that are related to profiling and decisions about data subjects:
  - Each record contains an attribute labelled “result” that indicates the “outcome of the activity once it has been processed through Iovation’s services”, according to the company, and thus the result of a decision on the data subject. The value of this attribute is always “Allow” for both data subjects.
  - Another attribute indicates the “number of fraud prevention ‘rules’ triggered by the device”, which is “0” for most transactions, “1” for some transactions and “3” for one transaction.
  - One more attribute labelled “rules matched” indicates the type of fraud rules that have been triggered. This attribute exists only in the data provided to Data Subject 1 and is either empty or contains the values “New Device for Existing Account” and “New Account-Device Association”. Iovation emphasises that these rules are “determined by the Iovation subscriber”. For Data Subject 2, similar information appears to be stored in the “rule list” attribute, which contains the value “ISPs not from the White List, NEW ACCOUNT 48 HRS (GBP), New Account (7 days)” in one transaction record.
  - The attribute “rule score”, which indicates the “extent to which the identification of a specific rule contributed to the overall ‘score’ (i.e. likelihood of fraud) of the activity”, according to Iovation, is always “0” across transactions for both data subjects.
  - The transaction records provided by Iovation also include an attributed labelled “reason” that indicates the “reason why an activity was identified as being fraudulent”, according to Iovation. It is empty across transactions for both data subjects.
  - Likewise, the attribute labelled “SureScore”, which indicates the “attributed ‘score’ given to the activity that demonstrates the likelihood of fraud”, according to Iovation, is empty across transactions for both data subjects.

### 3.2.3.3 What we do not know

Evidence from technical tests and responses to SARs leaves open questions. We do not know:

- Whether Iovation processes additional personal data that we did not observe in the browser or that cannot be observed in the browser, and, if so, what kind of data.
- Whether SBG or its partners transmit any additional data to Iovation, and, if so, what kind of data.

---

94 Iovation states: “When Iovation compiles device attributes, these are collated into a file that we call a ‘Black Box’.”
• Whether Iovation obtains additional personal data from third parties that it did not disclose in the responses to the SARs, and, if so, what kind of data.
• How exactly it processes data on “relationships between devices and accounts”.
• The logic of how Iovation decides that a user transaction is considered not fraudulent and thus returns the “Allow” value to the client (as provided in the responses to the SARs).
• Whether Iovation conducts additional profiling that it did not disclose in the responses to the SARs.
• Whether Iovation processes personal data on users of websites or apps operated by companies that were not subject of technical testing, and, if so, in which way.

3.2.3.4 SAR information is incomplete
Iovation provided both data subjects with information about personal data they process about them. However, some personal data Iovation received on Data Subject 2 according to observations from the technical tests was not provided in the response to the SAR:

• We observed 13 network requests to Iovation during 6 visits to the skycasino.com website. 12 network requests involved the transmission of personal data to Iovation. They included the transmission of the “Iovation ID” identifier and resulted in Iovation storing this identifier back to the browser of Data Subject 2. However, Iovation provided only 4 transaction records to Data Subject 2.
• We observed a network request that transmitted personal data to Iovation during a visit to skyvegas.com. Iovation did not provide information related to this visit to Data Subject 2.
• We observed network requests that transmitted personal data to Iovation during visits to five other gambling websites. Iovation did not provide information related to these visits to Data Subject 2.

3.2.3.5 Discussion
In its response to the SAR of Data Subject 2, Iovation stated that it processes “[s]mall amounts of non-directly identifying Personal Data” related to their devices, for example to a “mobile/cell phone, laptop, personal computer or tablet”, for the purpose of the prevention of fraud. It does “retain personal data where fraud has not been identified as being linked to a device or account for a period of two years from the date that the device was last ‘seen’ by Iovation”. Iovation states that personal data is “collected in collaboration with [their] customers”. According to its privacy policy, it uses the data to “enable our consortium of Customers to share information about known fraudulent or malicious devices” and for “other legitimate business purposes”, among others.

As laid out in the initial paragraphs in this section, Iovation states that it collects “billions of global online and offline consumer data points”. It processes data on billions of devices and on a “consumer’s identity, behavior and reputation”, “linking proprietary data, personal data, device identifiers and online behaviors”. It states that it tracks “relationships between devices and accounts” and thus processes data across client and even promises to “[c]onfidently identify devices associated with good loan applicants” in order to “[r]ecognize good loan applicants from their first visit”, which suggests that Iovation also links device data and credit data. This amount of data processing can be contrasted with Iovation’s claim to Data Subject 2 that it processes only “small amounts” of personal data.

Assessing the legal compliance of Iovation’s data practices is beyond the scope of this report. However, a system that processes such vast quantities of personal data should be transparent so as to be demonstrating its compliance with GDPR principles (e.g. legal basis, purpose limitation, data minimisation). Article 14 GDPR imposes a particularly important obligation, given the especial need for transparency in respect of data subjects who would otherwise not be aware that the controller is processing their data.
Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG, we conclude:

- By storing a personal identifier in the browser and later receiving the same identifier from that same browser during a visit to a website operated by another company, Iovation gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing across companies, and any personal data processing that relies on it.

As laid out above, Iovation also made the argument that it collects personal data “in collaboration with” its clients. As Iovation’s clients appear to facilitate Iovation’s personal data processing across many other companies at scale, it is unclear whether those clients have a legal basis under the GDPR to contribute data on their users and customers. In the context of this report, it is important to know whether SBG has a legal basis to do so. It is unclear from either SBG or Iovation what legal basis is relied on. We do not speculate as to whether the lawful basis they are relying on is sufficient, but we note that the legal basis is not clear.

Conversely, the scale of Iovation’s personal data processing raises the question of how TransUnion and other TransUnion subsidiaries may use this data. The striking fact is that that the same company that is operating a global fraud surveillance system is advertising its product to the gambling industry as a means to “[k]eep [their] customers playing longer and coming back for more” yet at the same time providing solutions for player self-exclusion and “responsible gaming”.

**Profiling and automated decisions on data subjects?** Iovation acknowledges in its privacy policy that it conducts “profiling” as defined in the GDPR but states it does not conduct automated decision making. In its response to Data Subject 2, it claims that “[a]ny decision made by our Subscriber Customers, based on information received from Iovation, is wholly their responsibility”. However, in a brochure that is available on the web, Iovation states that “[t]hose with lower scores may be automatically denied, flagged for manual review, or challenged for further authentication”. This raises the question whether Iovation’s clients actually always make independent decisions based on information received from Iovation.

### 3.2.4 Personal data processing by Signal (TransUnion)

Signal is a subsidiary of TransUnion, a large credit reporting agency and data broker, and sees itself as a “customer intelligence platform”. Clients can use its platform to collect customer data from different sources, including from their customer databases and from their websites and apps, analyse and profile their customers, and then further transmit data to many other platforms. Signal claims to receive and process “50 billion signals” about the activities of its clients’ customers each day.

Signal promises to connect “real-time actions across channels and devices with a persistent customer ID” in order to create a “single customer profile”. Clients can “identify and connect to individual customers on previously unknown devices” and “connect their customers’ digital profiles” to “external data and media partners”. By “synchronizing profiles” with data processed by other companies, clients can “continuously

---

95 [See initial paragraphs in this section.](#)
recognize customers” across the digital world. Signal also provides its clients “tag management” services that simplify the transmission of data to third-party companies.98

Signal does not provide much public documentation about its services. Based on how it advertises its services, it says it processes personal data about customers and other consumers on behalf of its clients. At the same time, it appears to facilitate consumer recognition across many platforms and help its clients to further transmit data to many other companies, while making sure that the companies who receive data still exactly know how to recognise, single out or target a person. It is not clear if a data subject’s data is shared across Signal clients. However, Signal appears to process extensive personal data in a way that occurs not strictly on behalf of a single client but across many clients and companies.

3.2.4.1 Observations on personal data processing from technical tests

According to our technical tests, Signal processed the following personal data on Data Subject 2:

- During 37 visits to skycasino.com, skybet.com, and skyvegas.com, we observed 401 network requests that transmitted data to Signal.99 We also observed network requests to Signal during visits to websites operated by other companies such as Asos.
- Signal received the same personal identifier referring to Data Subject 2 (“Signal ID1”) from Signal’s “bt3” cookie100 in the browser of Data Subject 2 across visits to skycasino.com and visits to a website operated by another company (asos.com). Signal also stored the Signal ID1 in the “bt3” cookie in the browser of Data Subject 2 across visits to skycasino.com and visits to a website operated by another company (asos.com).
- Signal received and stored the Signal ID1 across both “anonymous” and logged-in visits to skycasino.com that occurred after Data Subject 2 registered as a SBG customer.
- During visits to skycasino.com, Signal received behavioural data on activities of Data Subject 2, including information about the exact date and time the activities occurred:
  - Information on the pages visited (e.g. homepage, “slots” page, “blackjack” page, “roulette” page, page on the “Quantum Blackjack” game).
  - Information on the fact that Data Subject 2 registered as a customer at skycasino.com.
  - Information on the fact that Data Subject 2 logged in at skycasino.com.
  - Information on the fact that Data Subject 2 deposited cash, including the deposit amount and current balance in British pounds sterling, and information about whether or not it was the first cash deposit.
- These transmissions of behavioural data to Signal always included Signal ID1 referring to Data Subject 2 and one or more “event” numbers that describe the type of activity being tracked.
- Some of these network requests to Signal initiated network requests to yet other companies. For example, when Data Subject 2 deposited £30 to Sky Casino, Signal initiated data transmissions to Facebook, Google, Microsoft and MediaMath. Consequently, Facebook and Microsoft learned that Data Subject 2 made an initial deposit of £30 at Sky Casino. Google and MediaMath learned that Data Subject 2 purchased something worth £30 at Sky Casino. Both received other attributes that

---

99 We observed data transmission to the network hosts s.btstatic.com and s.thebrighttag.com, which are operated by Signal.
100 “bt3” is the name Signal uses for this cookie
may refer to the fact that a deposit occurred. All four companies also received personal identifiers stored in cookies associated with domains by these companies.

- Signal also received information about visits of Data Subject 2 to skybet.com and skyvegas.com.
- While Data Subject 2 did not log into the skybet.com website, code inspection shows that skybet.com may transmit even more fine-grained behavioural data to Signal, including on activities such as clicking a “tab”, opening and closing a “grid”, opening the “betslip”, adding to the “betslip”, removing “selections” from the “betslip”, and placing bets. Code inspection shows that Signal defines more than 500 different types of activities across different SBG services.

In addition, Signal exchanged and synchronised personal identifiers referring to Data Subject 2 with two other data companies:

- Signal sent a personal identifier\(^{101}\) to MediaMath, who was thus able to match it with its own personal identifier referring to Data Subject 2. In return, MediaMath sent both identifiers back to Signal. Consequently, Signal stored a new personal identifier in a cookie labelled “btv3.mm” in the browser of Data Subject 2. This suggests that Signal processes a personal identifier related to MediaMath in a cookie associated with Signal.
- Signal sent a personal identifier to Flashtalking, who stored a new personal identifier in a cookie associated with Flashtalking in the browser of Data Subject 2. Flashtalking then sent this new personal identifier back to Signal, who stored a new personal identifier in a cookie labelled “btv3.dJNjEOZ” in the browser of Data Subject 2. As the code “dJNjEOZ” is part of the data exchange between Signal and Flashtalking, the identifier stored in the “btv3.dJNjEOZ” cookie may be related to Flashtalking. This suggests that Signal processes a personal identifier related to Flashtalking in a cookie associated with Signal.

In addition to its main personal identifier Signal ID1, Signal often receives three other personal identifiers stored in cookies in the browser of Data Subject 2 during visits to skycasino.com. This includes identifiers stored in the “btv3.mm” and “btv3.dJNjEOZ” cookies that may be related to MediaMath and Signal. It is not clear, which company the fourth identifier stored in the “btv3.abYVto9” cookie is related to. The code “abYVto9” is part of a network request prepared by Signal that aims to transmit data to Twitter.

3.2.4.2 Evidence on personal data processing via SARs

In response to their SARs, and after extensive back-and-forth correspondence, both Data Subject 1 and Data Subject 2 received information about personal data Signal processed on them.

**Identifiers and profile data provided.** Signal provided Data Subject 1 with five sets of profile attributes linked to five different “cookie” identifiers. One set contains 63 profile attributes. Four sets contain 73 attributes. Data Subject 2 was provided with one set of profile attributes linked to one “cookie” identifier, containing 186 profile attributes. As described below, the profile attributes provided to Data Subject 1 and Data Subject 2 contain extensive personal data. They also contain additional personal identifiers. For both data subjects, the profile attributes contain the SBG customer ID and a “hashed” version of their email address.\(^{102}\) Profile attributes for Data Subject 2 also contain a “hashed” mobile device ID. Signal stated in its response to Data Subject 2 that it generally stores “user-related information associated with a one-way hashed email address”.

\(^{101}\) While we do not have any access to documentation about this personal identifier sent from Signal to MediaMath, it was clearly referring to Data Subject 2. Code inspection showed that Signal prepared another network request to Twitter that included the same personal identifier. We did, however, not observe Signal sending it to Twitter.

\(^{102}\) See p. 68: [https://crackedlabs.org/dl/CrackedLabs_Chrisl_CorporateSurveillance.pdf](https://crackedlabs.org/dl/CrackedLabs_Chrisl_CorporateSurveillance.pdf)
Profile attributes. Signal has been processing extensive personal data on the characteristics and behaviours of both Data Subject 1 and Data Subject 2 that are either the result of profiling or can be useful for profiling. According to the sets of profile attributes it provided to data subjects, Signal processed and stored:

- **Information that can be useful for profiling**, such as the date of account creation, the account balance, the number of deposits, the date of the last login, the last browsed category on the web, the first product a customer had been using (“nurture product”). For example, Signal recorded that Data Subject 1 made 2,514 deposits and that Data Subject 2 made two deposits. Signal also stored information about whether a customer has ever bet on particular sports such as football, the date of the first and the last bet, the number of days since the last football bet, the number of “rounds” played in a certain game, the “most recent season” played and the last date a customer created a “team” in another game. In addition, Signal stored an attribute that indicates “whether the customer is excluded from receiving free bets”. It is unclear why Signal records this latter information. All these attributes can be considered raw or “actual” personal data.\(^{103}\)

- **Information that is the result of basic inferences** and can, at the same time, be useful for further profiling, such as the email open rate (i.e., the percentage of emails opened), the favourite SBG product, the second favourite product, the favourite type of game at Sky Casino and an attribute that indicates whether a customer has “lapsed” (became inactive) at Sky Casino. To this end, Signal recorded that the favourite product of Data Subject 1 was Sky Bet, the second favourite product was Sky Casino, the favourite type of Sky Casino game was “Slot” and the email open rate was 100%. The favourite product of Data Subject 2 was Sky Casino, the favourite type of Sky Casino game was “Table” and the email open rate was 98%. Both data subjects have “lapsed” at Sky Casino. All these attributes can be considered inferred data.\(^{104}\) The logic of how the inferences are created is quite simple, however. For example, someone’s email open rate could be calculated by dividing the number of emails opened by the number of emails sent to the customer.\(^{105}\) Someone’s favourite product could be determined by counting how often certain products are used by a customer and then choosing the product with the highest number of uses.\(^{106}\) Nevertheless, data subjects are unlikely to know that their data is being stored in such a way.

- **Information that is the result of advanced profiling**. The following attributes processed and stored by Signal can also be considered inferred data. However, the logic of how these inferences were created and calculated is not clear. This includes:
  - Signal assigned Data Subject 1 to the customer group “High Value – Casino” and to the customer “life stages” of “Winback” and “Grow”. This suggests that Data Subject 1 was profiled as a very profitable SBG customer who should be incentivised to come back and spend more. Data Subject 2 was also considered a customer to “Winback”.
  - For the Sky Casino product, Data Subject 1 was assigned a “value score” of 9 and the “value band” attribute was set to “VHV” (very high value). Data Subject 2 was assigned a “value score” of “0” and the “value band” attribute was set to “VLV” (very low value).
  - Data Subject 1 was assigned separate value scores and bands for several other SBG products. For Sky Poker, Data Subject 1 was assigned a value score of “0” and the value band attribute was set to “VLV” (very low value). For Sky Bingo, Data Subject 1 was assigned a value score of 2 and the value band attribute was set to “LV” (low value). For Sky Vegas, Data Subject 1 was assigned a value score of 8 and the value band attribute was set to “VHV” (very high value). This

\(^{103}\) See p. 15: [https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf](https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)

\(^{104}\) Ibid.

\(^{105}\) Anyway, it requires to track, store and evaluate whether customers open emails sent to them.

\(^{106}\) Anyway, it requires to track, store and evaluate how often customers use specific SBG products.
suggests extensive profiling of the habits and behaviour of Data Subject 1 such that Data Subject 1 was considered a not so profitable customer for Sky Poker and Sky Bingo, but a very profitable customer for SBG’s Sky Vegas product. Consequently, “VGS” (Sky Vegas) was considered a potential “cross sell product” for SBG’s Sky Bet product. This might have led to SBG trying to incentivise Data Subject 1 in the context of its Sky Bet product to use Sky Vegas.

- For Data Subject 1, Signal stored a “Winback Margin” attribute that is a “data science predictive model for how much a customer would be worth if they returned over next 12 months”, according to Signal. This “Winback Margin” attribute was set to “1190.46”. This suggests that SBG could spend hundreds of pounds for incentives to make Data Subject 1 an active customer again and would still make a profit.

- Signal also stored an attribute that is labelled “Sportsbook: Low SOW Decile”. According to Signal’s description of a very similar attribute it may indicate “the predicted share of the customer's betting wallet that is spent on SBG's Sportsbook compared with competitors”. For Data Subject 1, this attribute was set to 10. No information is given about this score. It may for example suggest that Data Subject 1 spends 90 percent of the betting wallet at services operated by other online betting platforms and only 10 percent at SBG, and thus may be worth promotions and incentives that may make them spend more at SBG.

- Signal also stored “promo influence” scores, which indicate “whether the customer is positively or negatively influenced by promotions”, according to Signal. While Data Subject 1 was assigned a “positive” influence score for the Sky Casino product, Data Subject 2 was assigned a “neutral” influence score. Data Subject 1 was also assigned “promo influence” scores for other SBG products – “negative” for Sky Bet, “neutral” for Sky Bingo and “positive” for Sky Vegas. These “promo influence” scores point to profiling that predicts how easy it is to influence a customer by promotions.

- Signal put both data subjects into additional “segments”, i.e. groups with certain characteristics. For the Sky Casino product, Data Subject 1 was assigned to the segment “Slots 3+ Days” and Data Subject 2 was assigned to the group “2 Days or Less”. Data Subject 1 was also assigned to the Sky Vegas segment “Slots 3-4 Days” and to the Sky Bet segment “Daily Football - Mostly Pre”. No explanation was provided as to what these segment names mean.

- Signal discloses other attributes that did not have any value assigned for Data Subject 1 nor Data Subject 2. This includes attributes that indicate whether a customer tends to be a “high frequency” or “low frequency” player at Sky Bingo, the day of the week a customer preferably uses different SBG products, the “time of day” a customer preferably uses “Sky Poker”, the probability that a customer will bet “in-play” for football bets and the days since a customer was “won back”.

**Data on digital marketing experiments.** Signal stored data on whether or not a customer was in a “marketing measurement holdout … i.e. part of a marketing measurement analysis control group”, according to Signal. Signal’s descriptions of these attributes are not comprehensive. They may indicate whether a customer has been subject to special monitoring after receiving certain kinds of marketing messages on the web (“display”), throughout the digital world (“digital”), on Facebook, Twitter or via MediaMath. According to the information provided by Signal, Data Subject 1 was a member of the “display” and “Facebook” control groups. Data Subject 2 was a member of the “Facebook”, “Twitter” and “digital” groups. Signal also stored data on whether a customer was in an “A/B group for advertising across Sky Sports Digital Media … i.e. part of advertising analysis test or control group”. According to Signal, Data Subject 1 was a member of the “B” group and Data Subject 2 a member of the “A” group.
**Data on marketing and profiling settings.** Signal stored an attribute labelled “customer profiling consent” that indicates whether a customer has “opted into profiling”, according to Signal, which contains the value “Y” for both data subjects. Another attribute labelled “contact OK flag” that indicates whether a customer is “opted into marketing and is OK to contact”, according to Signal, which also contains the value “Y” for both data subjects. Yet another attribute labelled “marketing exclusion” indicates “whether a contactable customer has any form of marketing exclusion”, according to Signal, which is set to “Y” for both data subjects. The implications of this “marketing exclusion” are not clear. Neither Data Subject 1 nor Data Subject 2 “opted into Sky Bet Club”.

**Data on player safety.** Signal stored two attributes that should indicate whether a customer is “currently using the Cool Off feature” and whether a customer “has ever used the Cool Off feature before”. Both attributes contain the value “N” for Data Subject 1 and the value “Y” for Data Subject 2. While Data Subject 2 did use the “cool off” feature to lock themselves out of SBG for 24 hours, they were not using it when they made the SAR to Signal. Thus, the information that Data Subject 2 is “currently using” this feature appears to be inaccurate. Two other attributes indicate whether a customer is “currently Self Excluded on any SBG product” and whether a customer “has ever Self Excluded with SBG before”. Both contain the value “N” for both data subjects. Another attribute labelled “self excluded products” contains the value “BSPVCL” for Data Subject 2. This is unclear, as Signal stores the value “N” for any kind of self-exclusion for Data Subject 2. Another attribute stored by Signal should indicate whether a customer has a “basic marketing exclusion, including self exclusion, cool off or GAMSTOP”. It is striking that this metric contains “basic marketing exclusion” alongside self-exclusion markers. This attribute contains the value “N” for Data Subject 1 and “Y” for Data Subject 2. The reason for why this attribute is set to “Y” for Data Subject 2 and its implications are not clear. Another attribute stored by Signal labelled “GAMSTOP” is empty for both data subjects.

### What we do not know

Evidence from technical tests and responses to SARs leaves open questions. We do not know:

- Whether Signal processes additional personal data that we did not observe in the browser or that cannot be observed in the browser, and, if so, what kind of data.
- Whether SBG or its partners transmit any additional personal data to Signal, and, if so, in which way.
- Whether Signal does exchange any additional personal data with other companies that we did not observe or that cannot be observed in the browser, and, if so, in which way.
- Whether Signal uses personal data on website visitors and customers of SBG or information derived from it for its own business purposes, and, if so, in which way.
- Whether Signal obtains additional personal data from third parties that it did not disclose in the responses to the SARs, and, if so, what kind of data.
- The logic of how SBG and/or Signal calculate the profile attributes obtained via SARs.
- Whether Signal, SBG and/or other companies use this profiling data to market to or influence data subjects or make decisions on them, and, if so, in which way.
- How third-party companies that we observed receiving personal data as a result of network requests initiated by Signal further process this data.
- Whether Signal processes personal data on users of SBG mobile apps and, if so, in which way.
- Whether Signal processes personal data on users of websites or apps operated by companies that were not subject of technical testing, and, if so, in which way.
3.2.4.4 SAR information is incomplete

Signal and SBG provided both data subjects with information about personal data they process about them. However, as our observations from the technical tests show, they did not provide information about:

- The personal identifiers referring to Data Subject 2 processed by Signal as observed in the browser, and possible related data processing.
- The exchange of personal identifiers referring to Data Subject 2 between Signal and other third-party companies as observed in the browser, and possible related personal data processing.
- Personal data processing on Data Subject 2 during a visit to a website operated by Asos.
- Signal’s initiation of the transmission of behavioural data about activities by Data Subject 2 to third-party companies such as Facebook, Google and Microsoft. Signal also initiated personal data transmission to MediaMath, who provided at least some information about those personal data processing activities whereas neither Signal nor SBG did so.

In addition, Signal may process personal data in other ways that it did not disclose to the data subjects:

- Signal received behavioural data on the activities of Data Subject 2 many times. However, it provided only a single set of profile attributes. It may have processed and stored more personal data it received during website visits than it provided to the data subjects.
- Signal may have processed additional personal identifiers referring to the data subjects and exchanged them with other third-party companies.

3.2.4.5 Discussion

In its responses to the SAR of both data subjects, Signal states that the data it processed on them, and subsequently provided to them, was previously “provided directly to [Signal] by the client, or was captured using [its] tools on that specific client's site”. The company emphasises that it “does not share information between clients”. In its response to Data Subject 2, Signal states that the data is “only used toward [its] clients’ marketing efforts”. Signal suggests that it sees itself as a “data processor” on behalf of its client as defined in the GDPR for some personal data processing activities and as a “data controller” for other personal data processing activities. Signal does not clearly explain what activities it considers itself a data controller for nor what it considers itself a processor for.

SBG stated in its response to Data Subject 2, that it “uses” the Signal cookie “to share anonymous information about visitors with advertising and analytics partners”. SBG does not however share “anonymous” information with Signal but rather shares extensive data from which individuals can be identified, which is in turn shared with other third-party companies. The premise of SBG’s position therefore seems to be based on an erroneous understanding of whether data is anonymous.

Personal data processing across companies. When Signal states it “does not share information between clients”, this is not accurate for the personal identifier referring to Data Subject 2 that Signal received and stored in the browser across visits to websites operated by different companies, which we witnessed in technical tests. Signal also stored a hashed version of the email address of Data Subject 1 in profile attributes related to both SBG and Asos, according to its response to Data Subject 1.

Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG we conclude:

- By storing a personal identifier in the browser and later receiving the same identifier from that same browser during a visit to a website operated by another company, Signal gained the ability to
recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing across companies, and any personal data processing that relies on it.

- Signal exchanged personal identifiers with third-party companies MediaMath and Flashtalking. In this way, Signal, MediaMath and Flashtalking gain the ability to exchange other personal data with each other they independently process during visits of websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this exchange of personal identifiers between third-party companies, and any personal data processing that relies on it.

- Signal initiated a network request that allowed Flashtalking to store its own personal identifier in the browser, which it later received from the browser during a visit to a website operated by a different company. In this way, Flashtalking gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing by Flashtalking, and any personal data processing that relies on it.

- Signal stored identifiers that may be related to MediaMath and Flashtalking in cookies associated with Signal, which it later transmitted from the browser to other companies. This suggests that Signal further processed personal data it received from MediaMath and Flashtalking and shared it with yet other companies. SBG and other companies who embed the relevant code in their websites facilitate this personal data processing by Signal, and any personal data processing that relies on it.

Signal may exchange personal identifiers with additional third-party companies, it may initiate network requests that allow additional third-party companies to gain the ability to track users across websites operated by different companies, and it may store additional identifiers related to third parties in cookies associated with Signal.

Sharing of personal data on characteristics and behaviours with third parties. Signal initiated network requests that led to the transmission of personal data on characteristics and behaviours to third-party companies such as Facebook, Google, Microsoft and MediaMath. Both SBG and Signal facilitate this personal data sharing.

Profiling, influencing data subjects and making decisions on them? According to responses to SARs, Signal processes up to 186 profile attributes on a SBG customer, including information that is useful for profiling, information that is the result of basic inferences and information that is the result of advanced profiling. The latter includes information about the predicted customer value (customer value scores, value band classifications, win-back margin, the predicted share of a customer’s betting wallet compared with competitors), the estimated degree of how easy or difficult it may be to influence a customer by promotions, and about recommended actions (“win back”, “grow”, “cross-sell product”).

We do not know how SBG and/or Signal calculate most of these profile attributes. We do not even know in detail which data they use as a basis for those calculations. We do, however, know that Signal received personal data on some characteristics and behaviours of Data Subject 2 during visits to SBG websites, according to observations from technical tests. Most important, we do not know whether Signal, SBG and/or other companies use this profiling data to influence data subjects or make decisions on them, and if so, in which way.

Generally, they could use this profiling data to:
• Personalise the functions, messages, available choices, offers and incentives on SBG websites or apps.
• Personalise messages or offers sent to customers via channels directly controlled by SBG (e.g. email).
• Personalise messages or offers sent to customers via channels controlled by third parties (e.g. ads or “sponsored content” on websites, in mobile apps or on platforms such as Facebook).

Those personalised functions, messages, choices, offers, and incentives could be designed in ways that aim to influence the behaviour of existing customers. Specific messaging or incentives such as bonuses or free bets could be used to, for example, make someone return as a customer, make someone return more often, make someone play certain games or make someone calm down if they lose too often. Conversely, a gambling company could deny customers certain functions or choices that are considered not profitable for the company.

Profile attributes and other personal data stored by Signal could also be transmitted to third-party companies in order to find and target new customers, for example, Facebook users who are similar to existing customers. This concerns not only profile attributes and other personal data stored by Signal, but also the transmissions of data on the characteristics and behaviours to third-party companies such as Google, Facebook, Microsoft and MediaMath that Signal initiated during visits to SBG websites as observed in the browser. We do not know whether data transmitted to these companies has been used for profiling and whether it has been used to influence data subjects or make decisions on them.

3.2.5 Personal data processing by Adobe

Adobe is commonly known as the “Photoshop” and “Acrobat” company, but also provides a variety of products that aim to help businesses collect, analyse, utilise and trade personal data for marketing and advertising purposes. Adobe’s “Experience Cloud”107 promises its clients to help them “[c]ollect, connect and activate customer data in real time” from “just about any source”, to “consolidate” the collected data within its platform “to build out powerful customer profiles”108, to “[u]se data from every channel on every channel in real time”, and to give clients “insights into customer behaviour based on every single interaction”.109

Adobe provides web analytics services that helps its clients “recognise” site visitors110, as well as digital advertising services.111 Its “Audience Manager” helps clients to “collect and merge data from practically any source”112, build “profiles” and “segments” based on user “behaviour” as well as “personal interests” based on “online and off-line data”, merging “user identities from devices and touchpoints”, and ingesting data from “data providers, off-line data on-boarders, ad servers, device graphs and more”.113

Adobe is also engaged directly in reselling consumer data from a wide range of data companies and data brokers, which makes Adobe itself a data broker.114

---

At the core of Adobe’s data services lies its “ID Service” that creates a “common key or ID which can be used to link profiles and identities” as well as synchronises personal identifiers within Adobe’s Experience Cloud services and across its clients, partners and “different third-parties across the adtech ecosystem”.\[^{115}\] In addition, Adobe provides a “Cloud Device Co-op” that helps clients to “work together to better identify consumers” in the digital world across companies and contexts. Adobe emphasises that “members do not share data directly with each other” for this purpose. Instead, Adobe “acts as a broker to make device link data available”.\[^{116}\]

### 3.2.5.1 Observations on personal data processing from technical tests

According to our technical tests, Adobe processed the following personal data on Data Subject 2:

- During 37 visits to skycasino.com, skybet.com and skyvegas.com, we observed 499 network requests that transmitted data to Adobe.\[^{117}\] We also observed network requests to Adobe during visits to websites operated by other companies, such as Asos and Unibet.
- Adobe received the same personal identifier referring to Data Subject 2 (“Adobe ID1”) from Adobe’s “demdex” cookie\[^{118}\] in the browser of Data Subject 2, across visits to skycasino.com and visits to websites operated by other companies (asos.com, unibet.co.uk). Adobe also stored the Adobe ID1 in the “demdex” cookie in the browser of Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies (asos.com, unibet.co.uk).
- Adobe also processed several other Adobe IDs referring to Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies.
- We also observed that SBG processed Adobe identifiers referring to Data Subject 2 in cookies associated with its domains operated by SBG (skycasino.com, skybet.com) in a way that is directly accessible to SBG.
- During visits to skycasino.com, Adobe received behavioural data on activities of Data Subject 2, including information about the exact date and time the following activities occurred:
  - Information on the pages visited (e.g. “slots” page, “roulette” page).
  - Information on the fact that Data Subject 2 started registering as a customer at skycasino.com and detailed behavioural data about every step taken during the registration (entering name, entering date of birth, entering postcode, entering email address, entering phone number, choosing username, entering mother’s maiden name, answering security questions, choosing PIN code, reviewing account data, accepted terms, adding credit card info, chose Visa credit card for payment, deposited £30, clicked “go to my account”).
  - Information on the fact that Data Subject 2 deposited cash, including the amount in British pounds sterling.
  - Information on the fact that Data Subject 2 withdrew cash, including the amount in British pounds sterling.

\[^{117}\] We observed data transmission to the network hosts dpm.demdex.net, cm.everesttech.net, skybet.demdex.net and assets.adobedtm.com, which are operated by Adobe, and to the network hosts smetrics.sky.com (CNAME to sky.com.ssl.d1.sc.omtrdc.net), bskyb.sc.omtrdc.net and bskybskycasinoprod.112.2o7.net, which appear to be jointly operated by Adobe and Sky UK (see section 3.2.5).
\[^{118}\] “demdex” is the name Adobe uses for this cookie
Information on the fact that Data Subject 2 set a 24-hours "cool-off" period.

- These transmissions of behavioural data to Adobe always included at least one Adobe personal identifier referring to Data Subject 2. Many also included the SBG customer ID of Data Subject 2. Most of them included a wide range of other parameters that describe the type of activity that is being tracked.
- The transmissions of behavioural data we observed appear to be received not only by Adobe but also by a network host that appears to be jointly operated by Adobe and Sky UK.

In addition, Adobe exchanged personal identifiers referring to Data Subject 2 with other data companies:

- We observed Adobe receiving the MediaMath ID from MediaMath.
- We observed Adobe sending the Adobe ID1 to the identity surveillance firm ID5 and receiving another personal identifier from ID5.
- We observed ID5 storing a personal identifier that appears to be related to Adobe in a cookie associated with ID5.
- We observed PubMatic storing an Adobe identifier in a cookie associated with PubMatic. We did not, however, observe how PubMatic received this identifier from Adobe.

### 3.2.5.2 What we do not know

Evidence from technical testing leaves open questions. We do not know:

- Whether Adobe processes additional personal data that we did not observe in the browser or that cannot be observed in the browser, and, if so, what kind of data.
- Whether SBG or its partners transmit any additional personal data to Adobe, and, if so, in which way.
- Whether Adobe uses personal data on website visitors and customers of SBG or information derived from this data for its own business purposes, and, if so, in which way.
- Whether Adobe obtains additional personal data from third parties, and, if so, what kind of data.
- Whether Adobe created any kind of inferences or profiles based on the data it received according to our observations.
- Whether SBG, Adobe and/or other companies use personal data to influence data subjects or make decisions on them, and, if so, in which way.
- How third-party companies that we observed receiving personal identifiers from Adobe, or otherwise processing them, further process the data.

### 3.2.5.3 SAR information was not provided

Data Subject 1 did not send a SAR to Adobe.

Data Subject 2 sent a SAR to Adobe. However, Adobe did not provide any information about personal data processing activities related to Data Subject 2’s use of SBG services that we observed.

Neither Adobe, Sky UK, nor SBG provided any relevant information about the observed personal data processing by Adobe to Data Subject 2 upon their SARs sent to Adobe, Sky UK and SBG.

---

119 See section 3.2.5
120 See section 3.2.5
3.2.5.4 Discussion

In contrast to Iovation, Signal and MediaMath, Adobe did not provide any relevant information about the observed data processing activities. Despite Data Subject 2 sending SARs to SBG and Adobe, neither of the companies provided relevant information about Adobe’s processing while using SBG services.

In its response to the SAR sent to Data Subject 2, SBG stated that it “can confirm” that it “processes” the Adobe cookie, but did not provide any information about personal data processed by or shared with Adobe.

Since a part of the data Adobe was observed to receive appears to be jointly processed by Adobe and Sky UK, Data Subject 2 also sent a SAR to Sky UK. However, Sky UK, too, did not provide any relevant information in their response.\(^\text{121}\) SBG stated in its SAR response that it does “not process” the cookie related to Sky UK, however, the evidence from technical testing suggests this may not be correct. Rather, our observations suggest that SBG facilitates the transmission of extensive behavioural data to Adobe and/or Sky UK.

**Personal data processing across companies.** Based on the observations from the technical tests on personal data processing about Data Subject 2, during visits to websites operated by SBG, we conclude:

- By storing a personal identifier in the browser, and later receiving the same identifier from that same browser during a visit to a website operated by another company, Adobe gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing across companies as well as any personal data processing that relies on it.
- We also observed Adobe exchanging personal identifiers with other data companies during visits to SBG websites. SBG embedded code into its website that facilitates this personal data processing by Adobe and these third-party companies, as well as any personal data processing that relies on it.

According to our observations, Adobe processed a range of different personal identifiers referring to Data Subject 2 during visits to SBG websites. Some of these personal identifiers appear to be specific to one particular client, i.e. to SBG. Others were observed during visits to websites operated by SBG and by other companies.

Adobe’s documentation suggests that it processes both client-specific personal identifiers and personal identifiers that are used across clients. This includes the “Experience Cloud ID” (MID) or “AMCV” identifier that may be client-specific and the “demdex ID” that may be used across clients.\(^\text{122}\) Adobe’s documentation states that the “Experience Cloud ID” is “derived mathematically” from a client ID and the “demdex ID”, which suggests that both identifiers are related with each other. Our observations suggest that Adobe processes both client-specific identifiers and cross-client identifiers within the same network requests and data transmissions, which enables Adobe to know that both refer to the same data subject.

It is also unknown to us whether SBG or its partners participate in Adobe’s “device co-op” that involves extensive personal data sharing across clients.\(^\text{123}\)

**Profiling, GDPR legal basis?** As Adobe did not provide any information upon the SAR, the scale and scope of its personal data processing is unknown. It is not clear whether Adobe conducted profiling or automated decision-making on Data Subject 2. Also, it is not clear which legal basis Adobe relies on with respect to the personal data it processed on Data Subject 2.

\(^{121}\) See section 3.2.5

\(^{122}\) [https://experienceleague.adobe.com/docs/id-service/using/intro/cookies.html][16.11.2021]

\(^{123}\) [https://experienceleague.adobe.com/docs/device-co-op/using/about/overview.html][16.11.2021]
3.2.6 Personal data processing by Sky UK

During visits to skycasino.com, we observed many data transmissions that appear to be co-operated by Sky UK, a UK broadcaster and telecommunications company\(^{124}\), who has partnerships with SBG.\(^ {125}\)

3.2.6.1 Observations on personal data processing from technical tests

As shown in section 3.2.5.1, we observed Adobe receiving behavioural data on activities of Data Subject 2 several times. The network host smetrics.sky.com that received this data appears to be jointly operated by Adobe and Sky UK. While the domain sky.com is owned and operated by Sky UK, the network host smetrics.sky.com points to the network host sky.com.ssl.d1.sc.omtrdc.net\(^{126}\), which is owned and operated by Adobe.\(^ {127}\)

In this way, every data transmission to smetrics.sky.com arrived at a service operated by Adobe, and both Sky UK and Adobe received extensive personal data on behaviours of Data Subject 2 when they visited SBG websites.

In addition, we observed Sky UK storing Adobe ID1 (Adobe’s “demdex” identifier)\(^ {128}\) and two different Google identifiers in cookies associated with the domain sky.com. We also observed data transmissions to two other network hosts that also appear to be jointly operated by Adobe and Sky UK.\(^ {129}\)

3.2.6.2 SAR information was not provided

Neither SBG nor Sky UK provided any information about personal data that Sky UK may have been processing during Data Subject 2’s use of SBG services.

---


\(^{126}\) smetrics.sky.com is a so-called CNAME record pointing to sky.com.ssl.d1.sc.omtrdc.net. See: [https://en.wikipedia.org/wiki/CNAME_record](https://en.wikipedia.org/wiki/CNAME_record)

\(^{127}\) [https://www.adobe.com/privacy/experience-cloud.html](https://www.adobe.com/privacy/experience-cloud.html) [3.10.2021]

\(^{128}\) See section 3.2.5.1

\(^{129}\) bskyb.sc.omtrdc.net and bskybskycasinoprod.112.2o7.net
3.2.7 Personal data processing by MediaMath

MediaMath is a US-based advertising and data company that claims to have data on “more than a billion consumers”\textsuperscript{130} As a “demand-side platform” (DSP) it promises that advertisers, brands and other clients can use its products to “reach and influence customers and prospects on any screen”, to “[reach] the most relevant, highest-value customers at scale”, and to “[b]uild larger and better performing audiences” with its “deep segmentation tool that marries data from brands/partners with MediaMath data and third-party data”.\textsuperscript{131} MediaMath resells consumer data provided by third parties in the form of “audiences” and “segments”\textsuperscript{132}, which makes it a data broker.

3.2.7.1 Observations on personal data processing from technical tests

According to our technical tests, MediaMath processed the following personal data on Data Subject 2:

- During 37 visits to skycasino.com, skybet.com, and skyvegas.com, we observed 77 network requests that transmitted data to MediaMath.\textsuperscript{133} We also observed network requests to MediaMath during visits to websites operated by other companies such as Betway and Unibet.
- MediaMath received the same personal identifier referring to Data Subject 2 (“MediaMath ID”) from MediaMath’s “uuid” cookie\textsuperscript{134} in the browser of Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies (unibet.co.uk, betway.com).
- MediaMath received the MediaMath ID across both “anonymous” and logged-in visits to skycasino.com that occurred after Data Subject 2 registered as a SBG customer.
- During visits to skycasino.com, MediaMath received behavioural data on activities of Data Subject 2, including information about the exact date and time the following activities occurred:
  - Information on the pages visited (e.g. homepage, “slots” page, “blackjack” page).
  - Information on the fact that Data Subject 2 registered as a customer at skycasino.com.
  - Information on the fact that Data Subject 2 logged in at skycasino.com.
  - Information on the fact that Data Subject 2 deposited cash, including the amount in British pounds sterling.
  - Information on the fact that Data Subject 2 withdrew cash.
- These transmissions of behavioural data to MediaMath always included the MediaMath ID referring to Data Subject 2. Some of them also included the SBG customer ID and the SBG username of Data Subject 2. Most of them included one out of four different MediaMath “pixel” codes that may further describe the type of activity that is being tracked.

In addition, MediaMath exchanged and synchronised personal identifiers stored in cookies in the browser of Data Subject 2 with several other data companies. During visits to skycasino.com, MediaMath constantly

\textsuperscript{131} \url{https://www.mediamath.com/platform/} [29.9.2021]
\textsuperscript{132} See e.g. \url{https://apidocs.mediamath.com/dmp/audience-segments} [16.11.2021]. Companies who provide “audiences” include data brokers such as Experian, Epsilon, Axiom and Oracle: \url{https://www.mediamath.com/partners/} [16.11.2021]
\textsuperscript{133} We observed data transmission to the network hosts pixel.mathtag.com and sync.mathtag.com, which are operated by MediaMath.
\textsuperscript{134} “uuid” is the name MediaMath uses for this cookie
initiated network requests that directly or indirectly led to personal data processing activities by at least 20 digital advertising firms and data brokers.

The following table shows which third-party companies received the MediaMath ID and which companies sent their own company-specific IDs to MediaMath. It also shows which companies received their company-specific ID from a third-party cookie in the user’s browser and which companies stored their company-specific ID in a third-party cookie. Another column shows whether the company also processed the same company-specific ID during a visit to another website operated not by SBG (unibet.co.uk):  

<table>
<thead>
<tr>
<th>Third-party company</th>
<th>Received MediaMath ID</th>
<th>Sent company-specific ID to MediaMath</th>
<th>Received company-specific ID from cookie</th>
<th>Stored company-specific ID in cookie</th>
<th>Processed company-specific ID on unibet.co.uk</th>
<th>Exchanged IDs with other third-party companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xandr/AT&amp;T</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Received ID from Google</td>
</tr>
<tr>
<td>Yahoo, advertising.com</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Sent ID to IDS; received ID from IDS</td>
</tr>
<tr>
<td>Oracle</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Sent ID to IDS; received ID from IDS</td>
</tr>
<tr>
<td>PubMatic</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Stored MediaMath ID in PubMatic cookie; retrieved Xandr ID and Adobe ID from cookie</td>
</tr>
<tr>
<td>LiveRamp</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Received ID from Google</td>
</tr>
<tr>
<td>Google</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Sent IDs to LiveRamp, Semasio, Xandr</td>
</tr>
<tr>
<td>Tapad/Experian</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Sent ID to IDS</td>
</tr>
<tr>
<td>Salesforce</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adobe</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Sent ID to IDS; received ID from IDS</td>
</tr>
<tr>
<td>Freewheel/Comcast</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Sent ID to IDS; received ID from IDS</td>
</tr>
<tr>
<td>Zeotap</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sovrn</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semasio</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Received ID from Adform, The Trade Desk, Google</td>
</tr>
<tr>
<td>Adform</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Sent ID to Semasio</td>
</tr>
<tr>
<td>The Trade Desk</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Sent ID to Semasio</td>
</tr>
<tr>
<td>Smartclip/RTL Group</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Stored MediaMath ID in Smartclip cookie</td>
</tr>
<tr>
<td>Neustar</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Received ID from Gumgum, Tapad, Oracle, Adobe; sent ID to Oracle, Adobe</td>
</tr>
<tr>
<td>Gumgum</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Sent ID to IDS</td>
</tr>
</tbody>
</table>

According to our technical tests, MediaMath directly or indirectly initiated the following personal data processing activities by third-party companies during visits to skycasino.com:

- MediaMath sent its MediaMath ID to at least 13 third-party companies, including Yahoo, Oracle, PubMatic, LiveRamp, Tapad, Salesforce, Freewheel, Zeotap, Sovrn, Semasio, Smartclip, Neustar and IDS. As all of them also received their company-specific IDs referring to Data Subject 2 from third-party cookies in the user’s browser, they were able to learn that both IDs refer to the same data subject.

- Conversely, MediaMath received company-specific IDs referring to Data Subject 2 from at least three companies, which enabled MediaMath to learn that the IDs it received from these companies refer to the same data subject as its MediaMath ID. This included Xandr, Neustar and Google.

- 16 third-party companies stored company-specific IDs referring to Data Subject 2 in third-party cookies in the browser, which they also processed during visits to unibet.co.uk, a website operated not by SBG.

135 The exchange of identifiers between MediaMath and Adobe was observed during a visit to skyvegas.com
136 Adobe received the MediaMath ID during a visit to skyvegas.com
• Directly or indirectly initiated by MediaMath, several third-party companies exchanged company-specific IDs referring to Data Subject 2 with each other. For example, the identity surveillance firm ID5 received IDs from Tapad, Oracle and Adobe, as well as sent IDs to Oracle and Adobe.
• PubMatic and Smartclip stored the MediaMath ID in third-party cookies associated with them after receiving it from MediaMath.

As section 3.2.4.1 shows, MediaMath also exchanged and synchronised personal identifiers with Signal. In addition, Signal stored a personal identifier in a cookie labelled “btv3.mm” in the browser that appears to be a modified version of the MediaMath ID, and further processed it.

The following chart shows how SBG and MediaMath initiated personal data processing by third-party companies:

3.2.7.2 Evidence on personal data processing via SARs

Data Subject 1 did not send a SAR to MediaMath.

As a response to the SAR sent by Data Subject 2, MediaMath sent a file that confirms that it received personal data on Data Subject 2’s visits to websites operated by MediaMath’s clients SBG, Betway, and “BetGenius”, 108 times. Each time, it received a timestamp, the name of the client company, the IP address and information on country, region, browser and internet connectivity, according to the file. It refers to this data as “pixel data”. MediaMath confirmed that it linked this data to the MediaMath ID we observed in the browser of Data Subject 2. MediaMath stated that is also processes the Apple device ID (IDFA) of the iPhone of Data Subject 2. MediaMath refers to the Apple device ID also as a “MediaMath ID”. 

https://id5.io/
In addition, MediaMath stated that it processes “segments”, which are “grouping[s] of users who share one or more attributes” and contain data on “individuals” that are “identified by a MediaMath ID”. In its SAR response, MediaMath stated that it put Data Subject 2 in one segment with a rather nebulous label:

- “[Private] MM_Demo_Data_Vendor - (Private) - Demo Oracle Taxonomy - Branded Data - Digital - Demos (BR) - Age & Gender - Persons: 55+”

In the SAR response sent to Data Subject 2, MediaMath explains that it processes, obtains, shares and sells personal data in extensive ways:

- It states that it creates “segments” using data received from “data partners”, “media supply sources, such as publishers (i.e., organizations who operate websites, apps or emails)”, “exchanges”, “supply-side platforms who display ads on publishers’ websites”, as well as data regarding “interactions with [its] clients when [users] access their digital properties, including their websites, emails, and apps, and websites, emails and apps where their ads appear”.
- It states that it processes personal data for “business and commercial purposes” such as:
  - “Enabling MediaMath clients to create marketing campaigns”.
  - “Associating multiple browsers and devices with each other”.
  - “Mapping data pixels to third party segments”.
  - “Development, management, and commercialization of MediaMath’s identity management mapping that associates […] different devices with each other”.
  - “Facilitating our partners’ collection of personal information, including by placing partners’ pixels or tags on our clients’ digital properties”.
  - “Synchronizing MediaMath cookie ID with third-party partners”.
  - “Delivering ads based on [users’] interests or activities on digital properties”.
  - “Automated decision-making and profiling based on personal preferences, interests, behavior or location”.
  - “Transferring data to a third-party where clients have elected to use its services or where MediaMath has engaged a subcontractor to provide certain functionality or capabilities as a part of our Platform or to improve our Platform and the products and services that we provide to our clients and partners”.
- It states that it “discloses” MediaMath IDs, pixel data and segments to “clients”, “resellers”, “third parties designated by [its] clients”, “audience partners” and “cookie sync partners” for a “business purpose”. It also states that it "sells" MediaMath IDs and “segments (from third parties)” to “clients”, “resellers” and “third parties designated by [its] clients”.

3.2.7.3 What we do not know

- Whether MediaMath processes additional personal data that we did not observe in the browser or that cannot be observed in the browser, and, if so, what kind of data.
- Whether SBG or its partners transmit any additional personal data to MediaMath, and, if so, in which way.
- Whether MediaMath exchanges any additional personal data with other companies that we did not observe or that cannot be observed in the browser, and, if so, in which way.
- Whether MediaMath uses personal data on website visitors and customers of SBG or information derived from it for its own business purposes, and, if so, in which way.
- Whether MediaMath obtains additional personal data from third parties that it did not disclose in the responses to the SARs, and, if so, what kind of data.
• Whether MediaMath created any kind of inferences or profiles based on the data it received according to our observations beyond the single “segment” that was part of its SAR response.
• Whether MediaMath, SBG and/or other companies use the processed data to market to or influence data subjects or make decisions on them, and, if so, in which way.
• How third-party companies, that we observed receiving personal data as a result of network requests initiated by MediaMath, further process this data.

3.2.7.4 SAR information is incomplete

While MediaMath provided Data Subject 2 with some personal data it processes on them, information about much of the personal data processing activities we observed during the technical tests was not provided. This includes:

• Data on the pages visited, the games played and on activities such as registering, logging in, depositing and withdrawing cash, as well as the SBG customer ID, the SBG username and the "pixel ID".
• Specific information on
  o sending the MediaMath ID to other companies,
  o receiving personal identifiers from other companies,
  o storing personal identifiers related to other companies in cookies associated with MediaMath,
  o directly or indirectly initiating the storage of personal identifiers in cookies associated with other companies,
  o directly or indirectly facilitating the exchange of personal identifiers between other companies, and
  o possible related personal data processing activities that rely on the observed data flows.

In addition, MediaMath may process personal data in other ways that it did not disclose to Data Subject 2:

• When websites such as skycasino.com send data on user interactions, deposit amounts or customer IDs to a company like MediaMath, they typically want to further process it, for example, by putting users into groups, targeting them with ads or disclosing the collected data to other platforms. Neither SBG nor MediaMath disclosed any specific information on how the data collected on SBG websites was further processed or used.
• MediaMath may have processed additional personal identifiers referring to Data Subject 2 and exchanged them with other third-party companies.

3.2.7.5 Discussion

In its SAR response to Data Subject 2, MediaMath acknowledges that it processes, obtains, shares and sells personal data in extensive ways. It also refers to its privacy policy138, which provides additional details about how MediaMath claims to process personal data.

Personal data collection from websites. In its privacy policy, MediaMath mentions the “page URL” as one type of personal data it may collect when users interact with its clients’ websites. While our observations show that MediaMath indeed received the page URL several times, it did not disclose information about it in the SAR response to Data Subject 2.

Personal data processing across companies. Based on the observations from the technical tests on personal data processing about Data Subject 2, during visits to websites operated by SBG, we conclude:

- By receiving the same identifier from the browser during visits to websites operated by SBG and by other companies, MediaMath gained the ability to recognise and track users across websites operated by different companies. If MediaMath uses personal data collected across different websites for its own business purposes, SBG and other companies who embed the relevant code into their websites would facilitate this personal processing by MediaMath. The company’s privacy policy and SAR information disclosed to Data Subject 2 suggest that MediaMath actually uses personal data collected across different websites for its own business purposes, or even shares or sells it to others.

- By initiating network requests to third-party companies, MediaMath directly or indirectly initiated personal data processing activities by at least 21 digital advertising firms and data brokers, including Xandr/AT&T, Yahoo/Verizon Media, Oracle, PubMatic, LiveRamp, Google, Tapad/Experian, Salesforce, Adobe, Freewheel/Comcast, Zeotap, Sovrn, Semasio, Adform, The Trade Desk, Smartclip/RTL Group, Neustar, ID5 and Gumgum. MediaMath shared the MediaMath ID referring to Data Subject 2 with at least 14 of these companies and received personal identifiers from at least three of these companies. During visits to skycasino.com, two companies stored the MediaMath ID in their own third-party cookies. Several companies exchanged additional personal identifiers with each other. At least 16 of these companies stored their own personal identifiers referring to Data Subject 2 in third-party cookies associated with these companies during visits to skycasino.com, and processed the same personal identifiers during visits to websites operated by other companies. As such, they gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing by MediaMath and these third-party companies, and any personal data processing that relies on it.

Our observations align with MediaMath’s general statements about its personal data processing activities in its SAR response to Data Subject 2. As section 3.2.7.2 shows, MediaMath states that it processes personal data for “business and commercial purposes” such as the “development, management, and commercialization of MediaMath’s identity management mapping that associates […] different devices with each other”, “synchronizing MediaMath cookie ID with third-party partners” and “facilitating our partners’ collection of personal information, including by placing partners’ pixels or tags on our clients’ digital properties”. In addition, it states that it discloses MediaMath IDs and other personal data to different kinds of third-party companies including “audience partners”, “cookie sync partners” and “third parties designated by [its] clients”. These statements suggest that MediaMath:

- uses personal data collected across different websites for its own business purposes (e.g. for the “commercialization” of its “identity management mapping”),
- exchanges and synchronises personal identifiers with “third-party partners”, and
- facilitates personal data collection by “partners” on its clients’ websites and other “digital properties”.

As MediaMath’s SAR response to Data Subject 2 lacks specific information about those personal data processing activities, the details of how the company processes and shares personal data for those purposes are not clear. Specifically, it is not clear which third-party companies were “designated” to receive data by MediaMath’s client SBG or how those third parties were selected.

Profiling, influencing data subjects and making decisions on them? In its SAR response to Data Subject 2, MediaMath states that it uses “proprietary algorithms to make decisions about whether or not to bid on
opportunities to serve [Data Subject 2] ads and, if so, how much to bid ... these processes, in combination with client campaigns described below, may constitute profiling in certain jurisdictions”. In its privacy policy, it states that the “ways in which we use algorithms to determine bid prices may be considered automated decision-making in certain jurisdictions”. It is not clear whether MediaMath conducted profiling or automated decision-making on Data Subject 2.

**GDPR legal basis?** In its privacy policy, MediaMath states that it “will normally collect personal data from [data subjects] only where the processing is in our (or a third party’s, such as our clients’) legitimate interests and not overridden by [the data subject’s] rights”. Its legitimate interest “will normally be to operate the Platform and serve [data subjects] ads on behalf of our clients”. However, its legal basis under the GDPR “will depend on the personal data concerned and the specific context in which we process it”. MediaMath does not provide information about how it evaluates whether its legitimate interests are overridden by the data subject’s rights. As MediaMath did not disclose specific information about its legal basis to Data Subject 2, it is not clear which legal basis it relies on with respect to the personal data it processed on Data Subject 2.

### 3.2.8 Personal data processing by Facebook

As of 2020, the social media giant Facebook, now rebranded as Meta, claimed to have 2.6 billion daily active users. Its total revenue for 2020 was almost $86 billion, up from $71 billion in 2019. Ad revenue, which largely relies on exploiting personal data on billions of people, was responsible for $84 billion of total revenue.\(^{139}\) Facebook tracks people on and off its platform. The latter occurs because many websites and mobile apps include software that constantly transmits data to Facebook, from Like and Share buttons to the so-called Facebook Pixel. In 2018, the Like button was embedded in 8.4 million websites, and the Facebook Pixel in 2.2 million websites, according to the company.\(^{140}\) Facebook also tracks people who do not have an account. This has been discussed for a decade\(^{141}\) and was subject to lawsuits.\(^{142}\) In 2018, the company stated that it receives data during visits to websites that embed its services even if people are “logged out or don’t have a Facebook account” and uses the data to “enhance” its “products and services”.\(^{143}\) Facebook’s business and data practices have been subject to criticism, lawsuits and investigations by authorities many times.\(^{144}\)

#### 3.2.8.1 Observations on personal data processing from technical tests

According to our technical tests, Facebook processed the following personal data on Data Subject 2:\(^{145}\)

- During 37 visits to skycasino.com, skybet.com and skyvegas.com we observed 358 network requests that transmitted data to Facebook.\(^{146}\) We also observed network requests to Facebook during visits to websites operated by other companies such as Boylesports and Asos.

---


\(^{140}\) [https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf](https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf)


\(^{144}\) See e.g. [https://en.wikipedia.org/wiki/Criticism_of_Facebook](https://en.wikipedia.org/wiki/Criticism_of_Facebook)


\(^{146}\) Data Subject 2 has never logged into their Facebook account on the computer/browser used for the tests.

---

Digital Profiling in the Online Gambling Industry. Report, December 2022
• Facebook received the same personal identifier referring to Data Subject 2 ("Facebook ID") from Facebook’s “fr” cookie\(^{147}\) in the browser of Data Subject 2 across visits to skyscasino.com and visits to websites operated by other companies (boylesports.com, asos.com).

• Facebook received the Facebook ID across both “anonymous” and logged-in visits to skyscasino.com that occurred after Data Subject 2 registered as a SBG customer.

• We also observed that SBG stored another personal identifier referring to Data Subject 2 in the ".fbp" cookie associated with the domain skyscasino.com ("Facebook ID2")

• During visits to skyscasino.com, Facebook received behavioural data on activities of Data Subject 2, including information about the exact date and time the following activities occurred:
  - Information on the pages visited (e.g. “slots” page, “blackjack” page, “roulette” page).
  - Information on the fact that Data Subject 2 started registering as a customer at skyscasino.com.
  - Information on the fact that Data Subject 2 logged in at skyscasino.com.
  - Information on the fact that Data Subject 2 deposited cash, including the amount in British pounds sterling, and information about whether or not it was the first cash deposit.
  - During one login activity, Facebook received the code "BetABGroup". It is not clear what this means.

• These transmissions of behavioural data to Facebook always included the Facebook ID referring to Data Subject 2. Some of them also included Facebook ID2.

### 3.2.8.2 SAR information is incomplete

SBG did not provide information about the observed personal data processing activities by Facebook to Data Subject 2 upon their SAR.

### 3.2.8.3 Discussion

Facebook received extensive personal data about Data Subject 2 during their use of SBG websites, according to our observations. While SBG provided at least some information about how other companies were processing personal data about Data Subject 2, it did not provide any information about Facebook’s data processing.

**Personal data processing across companies.** Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG we conclude:

• By receiving the same identifier from that same browser during visits to websites operated by SBG and by other companies, Facebook gained the ability to recognise and track users across websites operated by different companies. If Facebook would use personal data collected across different websites for its own business purposes, SBG and other companies who embed the relevant code into their websites would facilitate this personal processing by Facebook.

**SBG may facilitate personal data processing for Facebook’s business purposes.** The observed data transmissions to Facebook appear to be the result of SBG or its partners embedding the so-called “Facebook Pixel” into its websites. The Facebook Pixel is a piece of software that can be embedded into a website to “track visitor activity”. For this purpose, it sends personal data on website visitors to Facebook. Website operators can then use this data for ad targeting on the platform, to measure the “effectiveness” of ads or to

\(^{147}\) “fr” is the name Facebook uses for this cookie.
analyse user behaviour, among other reasons.\textsuperscript{148} The use of the Facebook Pixel by website operators is governed by Facebook’s “Business Tools Terms”. These terms explicitly state that Facebook may use “event data”, which is information “about people and the actions that they take” that website operators “share” with Facebook to “personalize the features and content (including ads and recommendations) that we show people on and off our Facebook Company Products”.\textsuperscript{149} By sending personal data to Facebook, SBG may facilitate personal data processing for Facebook’s business purposes.

**Profiling, influencing data subjects and making decisions on them?** When websites operators send personal data on their users or customers to Facebook, they usually want to utilise this data on the platform in some way, for example, for profiling and targeting purposes. Potentially, SBG or its partners could utilise the data sent to Facebook to send personalised messages and offers that aim to influence the behaviour of existing or new customers across Facebook’s platforms. Facebook may sell profiling and targeting capabilities, based on the data SBG sent to Facebook, to other companies, too. As SBG did not disclose any information about the observed personal data processing activities by Facebook to Data Subject 2 in response to their SAR, we do not know whether Facebook engaged in profiling, automated decision-making or influencing of Data Subject 2 (or other persons) based on the data we observed Facebook to receive.

Generally, Facebook has often been accused of allowing advertisers use its profiling capabilities to target vulnerable people and to show them disturbing ads based on sensitive data. A recent study found that one of five Facebook ads presented to a young mother, whose parent died of cancer, was related to health, often with an emphasis on cancer or terminally ill children, which was “most likely” based on data about “the user’s online activity on and off Facebook”. It concludes that Facebook allows “advertisers to exploit inferred traits, sometimes of a highly sensitive nature, which users have not willingly disclosed”.\textsuperscript{150} Facebook also targets children and teens. A recent study found that “Facebook uses data it collects about underage users to create profiles of young people with harmful or risky interests such as 13-17 year olds interested in smoking, gambling, alcohol or extreme weight loss”.\textsuperscript{151} Another recent study showed that social media platforms actually show gambling ads to children and teens. It found that 64 percent of 11-17 year olds had seen gambling ads on social media platforms such as Facebook or YouTube.\textsuperscript{152}

### 3.2.9 Personal data processing by Google

Google and Alphabet provide a wide range of services including Search, YouTube, Android, Chrome and many others.\textsuperscript{153} Most important, it globally dominates digital advertising. Alphabet’s total revenue for 2020 was almost $183 billion, up from $162 billion in 2019.\textsuperscript{154} Most of its revenue comes from digital advertising, which largely relies on exploiting personal data on billions of people. According to a major antitrust lawsuit filed by several US states, Google “leverages intimate user data and personal information to broker billions of daily online ad impressions between publishers and advertisers that target individual users based almost entirely on their personal information”\textsuperscript{155} Google tracks people on and off its services. The latter occurs because many websites and mobile apps include software that constantly transmits data to Google. According

---

\textsuperscript{148} https://developers.facebook.com/docs/facebook-pixel
\textsuperscript{149} https://www.facebook.com/legal/terms/businessstools
\textsuperscript{150} https://en.panoptykon.org/algorithms-of-trauma
\textsuperscript{153} https://about.google/intl/en/products/
\textsuperscript{154} https://abc.xyz/investor/static/pdf/2020Q4_alphabet_earnings_release.pdf
\textsuperscript{155} https://storage.courist.com/recap/gov.uscourts.nysd.564903/gov.uscourts.nysd.564903.152.0.pdf
to large-scale studies, hundreds of thousands of websites include tracking software that transmits data to the platform.\textsuperscript{156}

3.2.9.1 Observations on personal data processing from technical tests

According to our technical tests, Google processed the following personal data on Data Subject 2:

- During 37 visits to skycasino.com, skybet.com, and skyvegas.com, we observed 240 network requests that transmitted data to Google.\textsuperscript{157} We also observed network requests to Google during visits to websites operated by other companies such as Boylesports, Unibet and Asos.
- Google received consecutive versions of a personal identifier referring to Data Subject 2 (“Google ID1”) from Google’s “IDE” cookie\textsuperscript{158} in the browser of Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies (boylesports.com, unibet.co.uk, asos.com). Periodically, Google received one version of the “IDE” identifier and stored another version of it to the browser of Data Subject 2 during visits to skycasino.com. During the test period, Google replaced one version of the “IDE” identifier with another version seven times. Several versions of Google’s “IDE” identifier referring to Data Subject 2 were processed across visits to websites operated by different companies.
- Google received and stored versions of the Google ID1 across both “anonymous” and logged-in visits to skycasino.com that occurred after Data Subject 2 registered as a SBG customer.
- Google also processed several other Google IDs referring to Data Subject 2 across visits to skycasino.com.
- We observed that SBG processed five different Google identifiers referring to Data Subject 2 in cookies associated with the domain skycasino.com in a way that is accessible to SBG, as well as two different Google identifiers in cookies associated with the domain sky.com in a way that is accessible to Sky UK.
- During visits to skycasino.com, Google received behavioural data on activities of Data Subject 2, including information about the exact date and time the following activities occurred:
  - Information on the pages visited (e.g. homepage).
  - Information on the fact that Data Subject 2 started registering as a customer at skycasino.com.
  - Information on the fact that Data Subject 2 logged in at skycasino.com.
  - Information on the fact that Data Subject 2 deposited cash, including the amount in British pounds sterling.
  - Information on the fact that Data Subject 2 added credit card information.
- These transmissions of behavioural data to Google always included a version of its Google ID1 referring to Data Subject 2. Some of them also included different codes that appear to describe the type of activity being tracked and may refer to specific groups Data Subject 2 was added to. 18 data transmissions included the SBG customer ID of Data Subject 2.

In addition, Google exchanged personal identifiers referring to Data Subject 2 with other data companies:

- We observed Google sending personal identifiers referring to Data Subject 2 and labelled “google_gid” to MediaMath, LiveRamp, Xandr and Semasio, who could then match the identifier

\textsuperscript{156}See e.g. https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf
\textsuperscript{157}We observed data transmission to 13 different network hosts operated by Google, including www.google.com, www.google.co.uk, adservice.google.com, googleleads.g.doubleclick.net, pubads.g.doubleclick.net, 3161884.fls.doubleclick.net, cm.g.doubleclick.net, 6203434.fls.doubleclick.net, www.googleadservices.com, www.google-analytics.com, ssl.google-analytics.com, www.googleitagmanager.com and fonts.googleapis.com
\textsuperscript{158}“IDE” is the name Google uses for this cookie.
received from Google with their own personal identifiers referring to Data Subject 2. These exchanges of personal identifiers potentially facilitate further personal data processing that relies on these exchanges.

- During visits to skycasino.com, Google initiated network requests to MediaMath, LiveRamp and Xandr.
- Initiated by Google, the network request to the data broker LiveRamp led to the storage of LiveRamp’s personal identifiers in cookies in the browser of Data Subject 2. We observed LiveRamp processing the stored identifiers across websites operated by different companies.

3.2.9.2 SAR information is incomplete

SBG did not provide information about the observed personal data processing activities by Google to Data Subject 2 upon their SAR.

3.2.9.3 Discussion

Google received extensive personal data about Data Subject 2 during their use of SBG websites, according to our observations. While SBG provided at least some information about how other companies were processing personal data about Data Subject 2, it did not provide any information about Google’s data processing.

Personal data processing across companies. Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG we conclude:

- By periodically storing new versions of a personal identifier in the browser and later receiving the same identifier from that same browser during a visit to a website operated by different companies, Google gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing across companies, and any personal data processing that relies on it.
- We also observed Google exchanging personal identifiers with other data companies during visits to SBG websites. SBG embedded code into its website that facilitates this personal data processing by Google and these third-party companies, as well as any personal data processing that relies on it.

SBG may facilitate personal data processing for Google’s business purposes. Google states in its privacy policy that it uses the information it collects from “all” its services to “provide personalized services, including content and ads”. This suggests that Google may also use personal data collected during visits to websites that include Google software for profiling and ad targeting. By sending personal data to Google, SBG may facilitate personal data processing for Google’s business purposes.

Profiling, influencing data subjects and making decisions on them? When websites operators send personal data on their users or customers to Google, they usually want to utilise this data on the platform in some way, for example, for profiling and targeting purposes. Potentially, SBG or its partners could utilise the data sent to Google to send personalised messages and offers that aim to influence the behaviour of existing or new customers. Google may sell profiling and targeting capabilities, based on the data SBG sent to Google, to other companies, too. As SBG did not disclose any information about the observed personal data processing activities by Google to Data Subject 2 upon their SAR, we do not know whether Google engaged in profiling, automated decision-making or influencing of Data Subject 2 (or other persons) based on the data we observed Google to receive.

---

159 https://www.gstatic.com/policies/privacy/pdf/20210701/7yn50xee/google_privacy_policy_en_eu.pdf
3.2.10 Personal data processing by Microsoft/Bing

While Microsoft is mainly known as a technology company that sells hardware, software and services to consumers and businesses, it is also a relevant player in digital advertising. As a part of its data and advertising services, Microsoft tracks users of thousands of websites. With the help of Microsoft’s “Universal Event Tracking” (UET), companies can embed software into their websites that sends data on “user activity” to Microsoft. Businesses can then use the collected data for profiling and ad targeting purposes.

3.2.10.1 Observations on personal data processing from technical tests

According to our technical tests, Microsoft processed the following personal data on Data Subject 2:

- During 37 visits to skycasino.com, skybet.com, and skyvegas.com, we observed 71 network requests that transmitted data to Microsoft. We also observed network requests to Microsoft during visits to websites operated by other companies such as Boylesports and Asos.
- Microsoft received the same personal identifier referring to Data Subject 2 (“Microsoft ID”) from Microsoft’s “MUID” cookie in the browser of Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies (boylesports.com, asos.com).
- Microsoft received the Microsoft ID across both “anonymous” and logged-in visits to skycasino.com that occurred after Data Subject 2 registered as a SBG customer.
- Microsoft also processed several other Microsoft IDs referring to Data Subject 2 across visits to skycasino.com and visits to websites operated by other companies.
- Microsoft stored two other personal identifiers in the local storage of the browser of Data Subject 2 in a way that is only accessible to SBG, for example, the "uetvid" identifier (“Microsoft ID2”).
- During visits to skycasino.com, Microsoft received behavioural data on activities of Data Subject 2, including information about the exact date and time the following activities occurred:
  - Information on the fact that Data Subject 2 started registering as a customer at skycasino.com.
  - Information on the fact that Data Subject 2 deposited cash, including the amount in British pounds sterling.
- These transmissions of behavioural data to Microsoft always included the Microsoft ID referring to Data Subject 2. Some of them also included Microsoft ID2.

3.2.10.2 SAR information is incomplete

SBG did not provide information about the observed personal data processing activities by Microsoft to Data Subject 2 upon their SAR.

3.2.10.3 Discussion

Microsoft received personal data about Data Subject 2 during their use of SBG websites, according to our observations. While SBG provided at least some information about how other companies were processing personal data about Data Subject 2, it did not provide any information about Microsoft’s data processing.

160 https://about.ads.microsoft.com/
164 We observed data transmission to the network host bat.bing.com, which is operated by Microsoft.
165 “MUID” is the name Microsoft uses for this cookie
Personal data processing across companies. Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG we conclude:

- By receiving the same identifier from that same browser during visits to websites operated by SBG and by other companies, Microsoft gained the ability to recognise and track users across websites operated by different companies. If Microsoft would use personal data collected across different websites for its own business purposes, SBG and other companies who embed the relevant code into their websites would facilitate this personal processing by Microsoft.

SBG may facilitate personal data processing for Microsoft’s business purposes. Microsoft states in its “Advertising Agreement” that Microsoft “own[s] and control[s] all information [it] collect[s] from users in connection with our advertising services”, including “user information collected” from “tags, pixels, or other unique tracking codes”, which Microsoft refers to as “Microsoft Advertising User Data”. It “uses such Microsoft Advertising User Data for the purposes of delivering Microsoft Advertising, including, where applicable, retargeting and conversions”. Microsoft obligates clients to “understand and acknowledge that Microsoft uses Microsoft Advertising User Data for its own purposes, including to improve its services”, as well as “for purposes related to reporting and performance analysis”.166 This suggests that Microsoft uses personal data collected during visits to websites that include Microsoft software for profiling and ad targeting. By sending personal data to Microsoft, SBG may facilitate personal data processing for Microsoft’s business purposes.

Profiling, influencing data subjects and making decisions on them? When websites operators send personal data on their users or customers to Microsoft, they usually want to utilise this data on the platform in some way, for example, for profiling and targeting purposes. Potentially, SBG or its partners could utilise the data sent to Microsoft to send personalised messages and offers that aim to influence the behaviour of existing or new customers. Microsoft may sell profiling and targeting capabilities, based on the data SBG sent to Microsoft, to other companies, too. As SBG did not disclose any information about the observed personal data processing activities by Microsoft to Data Subject 2 upon their SAR, we do not know whether Microsoft engaged in profiling, automated decision-making or influencing of Data Subject 2 (or other persons) based on the data we observed Microsoft to receive.

3.2.11 Personal data processing by Xandr

Xandr, formerly known as AppNexus, is a major advertising and data company that was acquired by the US telecom company AT&T in 2018.167 It provides a variety of products in the digital advertising space for both publishers and marketers168, and it “enables data owners to monetize their proprietary data”.169 According to its privacy policy, Xandr collects personal data about browsers, devices and user activity, as well as “individual profiles, preferences, characteristics, and behaviors”, and lets “digital properties” such as website operators, advertisers and other “buy and sell data”.170

3.2.11.1 Observations on personal data processing from technical tests

According to our technical tests, Xandr processed the following personal data on Data Subject 2:

---

During 37 visits to skycasino.com, skybet.com, and skyvegas.com, we observed 22 network requests that transmitted data to Xandr.\(^{171}\) We also observed network requests to Xandr during visits to websites operated by other companies such as Unibet.

Xandr received the same personal identifier referring to Data Subject 2 (“Xandr ID”) from Xandr’s “uuid2” cookie\(^ {172}\) in the browser of Data Subject 2 across visits to skycasino.com and visits to a website operated by another company (unibet.co.uk). Xandr also stored the Xandr ID in the “uuid2” cookie in the browser of Data Subject 2 across visits to skycasino.com and visits to a website operated by another company (unibet.co.uk).

Xandr received and stored the Xandr ID across both “anonymous” and logged-in visits to skycasino.com that occurred after Data Subject 2 registered as a SBG customer.

During visits to skycasino.com, Xandr received behavioural data on 17 visits to the website skycasino.com, including the exact date and time of the visit and the Xandr ID referring to Data Subject 2. It also received “pixel” and “segment” numbers that may refer to specific groups Data Subject 2 was added to.

In addition, Xandr exchanged personal identifiers referring to Data Subject 2 with other data companies:

- We observed Xandr sending its Xandr ID referring to Data Subject 2 to MediaMath.
- We observed Adobe receiving a personal identifier from Google.
- We observed PubMatic storing the Xandr ID in a cookie associated with PubMatic. We did not, however, observe how PubMatic received this identifier from Xandr.

3.2.11.2 SAR information is incomplete

SBG did not provide information about the observed personal data processing activities by Xandr to Data Subject 2 upon their SAR.

3.2.11.3 Discussion

Xandr received personal data about Data Subject 2 during their use of SBG websites, according to our observations. While SBG provided at least some information about how other companies were processing personal data about Data Subject 2, it did not provide any information about Xandr’s data processing.

Personal data processing across companies. Based on the observations from the technical tests on personal data processing about Data Subject 2 during visits to websites operated by SBG we conclude:

- By storing a personal identifier in the browser and later receiving the same identifier from that same browser during a visit to a website operated by another company, Xandr gained the ability to recognise and track users across websites operated by different companies. SBG and other companies who embed the relevant code into their websites facilitate this personal data processing across companies, and any personal data processing that relies on it.
- We also observed Xandr exchanging personal identifiers with other data companies during visits to SBG websites. SBG embedded code into its website that facilitates this personal data processing by Xandr and these third-party companies, as well as any personal data processing that relies on it.

Profiling, influencing data subjects and making decisions on them? The fact that Xandr received “pixel” and “segment” numbers when it received personal data on Data Subject 2 during visits to skycasino.com suggests that SBG or a SBG partner has a client relationship with Xandr. A client who sends data to a

\(^{171}\) We observed data transmission to the network hosts secure.adnxs.com and ib.adnxs.com, which are operated by Xandr.

\(^{172}\) “uuid2” is the name Xandr uses for this cookie
company such as Xandr usually wants to utilise this data on the platform in some way, for example, for profiling and targeting purposes.

Potentially, SBG or its partners could utilise the data sent to Xandr to send personalised messages and offers that aim to influence the behaviour of existing or new customers. Xandr may sell profiling and targeting capabilities, based on the data SBG sent to Xandr, to other companies, too. As SBG did not disclose any information about the observed personal data processing activities by Xandr to Data Subject 2 upon their SAR, we do not know whether Xandr engaged in profiling, automated decision-making or influencing of Data Subject 2 (or other persons) based on the data on website visits we observed Xandr to receive.