UNIVERZITA KARLOVA

Právnická fakulta

Jiří Maršál

Legal aspects of online behavioural advertising

Master's thesis

Supervisor: JUDr. Zdeněk Kučera, Ph.D.

Department: Katedra občanského práva

Date of completion (manuscript closure): 23 December 2022

I hereby declare that the submitted master's thesis is my independent and original work, all its sources are properly cited and listed, and the thesis has not been used to obtain the same or other degree.

I further declare that the main text of the thesis has 268 902 characters including spaces and footnotes.

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 268 902 znaků včetně mezer.

Jiří Maršál

In Prague on 23 December 2022 / V Praze dne 23. prosince 2022.

Acknowledgement / Poděkování

Na tomto místě bych chtěl poděkovat:

Vedoucímu práce panu doktoru Kučerovi za cenné rady, spousty poutavých judikátů a předaných zkušeností, jakož i za jeho semináře, které ve mě vzbudily zájem o právo informačních technologií.

Mým rodičům Janu Maršálovi a Kateřině Maršálové, bez jejichž nekonečné podpory by tato práce nikdy nevznikla.

A dále Anně Jelínkové, Lukáši Závorkovi a Ing. Goranu Zwaanovi, kteří mi byli inspirací a podporou při studiu.

Děkuji.

Table of Contents

"*We've built systems with open borders. The result of these open systems and open culture is well described with an analogy: Imagine you hold a bottle of ink in your hand. This bottle of ink is a mixture of all kinds of user data (3PD, 1PD, SCD, Europe, etc.) You pour that ink into a lake of water (our open data systems; our open culture) … and it flows … everywhere. How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?*"

Leaked document written by Facebook's engineers[1].

"*If a user knowingly or unknowingly gives his consent by means of an "accept all" button, the personal data of the data subject will be shared with hundreds of third parties*"

The Belgian DPA's IAB ruling, para. 393.

[1] As reported in FRANCESCHI-BICCHIERAI, Lorenzo. Facebook doesn't know what it does with your data, or where it goes: Leaked document. VICE [online]. 26 April 2022 [Accessed 19 December 2022]. Available from: https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

Introduction

Advertising is the fuel that turns the gears of today's digital markets. For publishers and content providers in general, it represents a key source of income alternative to traditional subscription-based financing models. Considering that users can be very price-sensitive when purchasing digital content and services, advertising removes barriers for market entry and promotes competition by allowing small players to attract new users with free services, relying exclusively on ad revenue. Similar benefits are felt by advertisers. Thanks to online ads, companies can efficiently expand their customer base and raise awareness about goods and services. Finally, all of this serves to benefits the end users who gain access to an immense array of free information and tools offered within competitive markets thriving on technological development and innovation, while being continuously updated with relevant product offers. According to an IAB study[2], the revenue stream provided by digital advertising is invaluable for preserving the internet's current *modus operandi*. The study suggests that consumers are already accustomed to the mostly ad-funded business model of information society services providers ("**ISSPs**") and would in fact be unwilling to pay for subscriptions, should the current business model be abandoned. Notably, the perceived importance of different services to the society would arguably not be reflected in the consumer's allocated budget[3]. These findings are seconded by a GfK study showing that two thirds of internet users never pay for online content or services[4].

The digital advertising market is on the rise – in 2021, the European market grew by 30.5% to € 92 billion[5]. At the same time, new technologies and trends are reshaping the users' online experience. Social networks and portable devices brought media closer to consumers than ever. While this gives advertisers new opportunities for reaching their audience, it also means that consumers are constantly flooded with a never-ending stream of content, making it

[2] IAB EUROPE. *What would an internet without targeted ads look like?* [online]. IAB Europe, March 2021 [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2021/04/IAB-Europe_What-Would-an-Internet-Without-Targeted-Ads-Look-Like_April-2021.pdf

[3] For example, according to the study, 45% of consumers attach very high importance to news; however, only 28% would be willing to pay for a subscription.

[4] GFK. *Europe online: an experience driven by advertising* [online]. GfK, September 2017 [viewed 19 December 2022]. Available from: https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf

[5] IAB EUROPE. *ADEX Benchmark 2021 Report* [online]. IAB Europe, June 2022. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2022/06/IAB-Europe_AdEx-Benchmark-2021_REPORT.pdf

increasingly difficult to grasp their attention. With so much content to consume and interactions to make, users are not willing to spend much time being advertised to. As opposed to the first recorded example of online display advertising (an ad banner purchased by AT&T in 1994) which enjoyed a 44% click-through rate, user today only click on around 0.02% to 2% of ads[6]. Thus, merely delivering ads to a user is no longer enough to actually get seen. Advertisers must try much harder and provide offers that are extremely relevant at a specific moment in time[7]. According to Seitz and Zorn[8], the paradigm shift extends far beyond changes in ad delivery mechanisms. Thanks to large scale data collection, companies are finally able to closely examine consumer preferences and decision-making processes to better predict sales opportunities. Some economic studies even talk about "attention markets", recognizing attention as the primary commodity offered to advertisers by platforms operating on a zero-price business model[9]. This switch to people-oriented advertising drives the expansion of programmatic advertising methods and online behavioural advertising in general.

Unfortunately, the reality of advertising markets is not always idyllic. In recent years, the legitimacy of data processing occurring within online advertising markets has been repeatedly questioned. In its 2017 impact assessment accompanying the proposal for the ePrivacy Regulation[10], the European Commission identified tracking tools used for online behavioural advertising as a key risk for the privacy of individuals.

Similar concerns are echoed through national Data Protection Authorities ("**DPAs**"). Following its assessment of the AdTech industry in 2019, the UK Information Commissioner's Office ("**ICO**") accused the industry of being "*immature in its understanding of data protection requirements*" expressing "*systematic concerns*" around its compliance with data protection laws. These concerns are now starting to translate into regulatory action. In February 2022, the Belgian DPA imposed a € 250.000 fine on IAB Europe for the data processing performed within

[6] CLEARCODE. *The AdTech Book* [online]. Katowice: Clearcode S.A., February 2022 [viewed 23 August 2022]. Available from: https://adtechbook.clearcode.cc/, p. 35

[7] BUSCH, Oliver. The Programmatic Advertising Principle. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 3

[8] SEITZ, Jürgen and Steffen ZORN. Perspectives of Programmatic Advertising. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 40

[9] EVANS, David S. The Economics of Attention Markets [online]. SSRN Electronic Journal, April 2020. Available at SSRN: https://ssrn.com/abstract=3044858

[10] EUROPEAN COMMISSION. Commission Staff Working Document, Impact Assessment, SWD(2017) 3 final, 10 January 2017, Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:bb21abb2-d809-11e6-ad7c-01aa75ed71a1.0001.02/DOC_1&format=PDF

the Transparency and Consent Framework – the consent mechanism used within IAB's OpenRTB advertising protocol (the "**IAB Ruling**")[11]. This decision is considered a major breakthrough in GDPR enforcement against AdTech vendors, as it reveals fundamental deficiencies in current behavioural advertising practices. CNIL – the French DPA – is also increasing scrutiny of AdTech vendors. In October 2018, it hit Vectuary – a demand-side platform – with a fine for invalid data processing[12], following up in August 2022 with a proposal for a € 60 million fine to AdTech vendor Criteo[13]. In May 2019, the Irish Data Protection Commission ("**DPC**") launched an official investigation of Google regarding its data processing practices in its Authorized Buyers advertising exchange[14].

The AdTech industry (and real-time bidding in particular) is also the target of extensive criticism by consumer protection organizations. For example, the Irish Council for Civil Liberties ("**ICCL**") repeatedly refers to real-time bidding as "the biggest data breach ever recorded". The ICCL[15], Brave browser's privacy specialists[16] as well as other privacy advocacy groups[17] have already initiated proceedings with national DPA's and courts all around Europe, pointing to fundamental flaws in advertising systems based on real-time bidding.

Without doubt, the increasing backlash against real-time bidding indicates that there may be inherent flaws in the way AdTech companies handle user data. The potential threats to internet user privacy are further amplified by the monstrous size of advertising markets and the ubiquitous presence of online tracking. In a 2019 study, Google's third-party scripts were found in around 82% of the measured web traffic and operated in a tracking context for slightly less

[11] Autorité de protection des données Gegevensbeschermingsautoriteitesicion decision 21/2022 of 2 February 2022, Case No. DOS-2019-01377.
[12] Commission Nationale de l'Informatique et des Libertés decision No. MED-2018-042 of 30 October 2018.
[13] HUNTON ANDREWS KURTH LLP. CNIL Proposes 60 Million Euros Fine Against French AdTech Company For Non-Compliance with GDPR [online]. Hunton Andrews Kurth LLP, 17 August 2022 [viewed 19 December 2022]. Available from: https://www.huntonprivacyblog.com/2022/08/17/cnil-proposes-60-million-euros-fine-against-french-adtech-company-for-non-compliance-with-gdpr/
[14] DATA PROTECTION COMMISSION. *Data Protection Commission opens statutory inquiry into Google Ireland Limited* [online]. 22 May 2019 [viewed 19 December 2022]. Available from: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited
[15] IRISH COUNCIL FOR CIVIL LIBERTIES. ACTION FILE: RTB online ad auctions [online] [viewed 19 December 2022]. Available from: https://www.iccl.ie/rtb/
[16] BRAVE. RTB evidence [online] [viewed 19 December 2022]. Available from: https://brave.com/rtb-evidence/
[17] FIX ADTECH. Ad Tech GDPR complaint is extended to four more European regulators [online]. 20 May 2019 [viewed 19 December 2022]. Available from: https://fixad.tech/ad-tech-gdpr-complaint-is-extended-to-five-more-european-regulators/

than half that time[18]. In this context, failure of AdTech companies to live up to prescribed data protection standards could lead to a massive infringement of internet user's fundamental right to privacy protected by Art. 10 of the Charter of Fundamental Rights and Freedoms of the Czech Republic and the provisions of international human rights treaties such as Art. 8 of the European Convention on Human Rights. Since tracking is commonly performed without users' knowledge, data subjects are also prevented from exercising their right to informational self-determination.

In addition to legal challenges, the AdTech sector is now facing technological changes that will require a substantial rework of the current online advertising mechanisms. Due to an increasing focus on user privacy, most internet browsers are abandoning third-party cookies, which have until now been used as the primary tool for user targeting. The changes are expected to peak after 2024, when Google plans to phase out third-party cookies from its Chrome browser[19].

In this paper, I would like to address the serious accusations raised against the AdTech industry by performing my own analysis of the applicable privacy protection laws and apply them to the data-handling practices of the leading networks for online behavioural advertising. In particular, I will attempt to answer the following research question that, in my view, best captures the most pressing concern arising from the processing of user data in online behavioural advertising:

- *Is the data processing carried out by AdTech companies engaged in online behavioural display advertising lawful under the applicable laws?*

Since the applicability of privacy protection laws is largely centred around the nature of the data in use and the extent to which the involved parties are responsible for the processing of such data, I expect it will also be necessary to address the following incidental questions:

[18] KARAJ, Arjaldo, Sam MACBETH, Rémi BERSON and Josep M. PUJOL. *WhoTracks.Me: Shedding light on the opaque world of online tracking* [online]. Computers and Society, arXiv:1804.08959, 25 April 2019. Available from: https://arxiv.org/abs/1804.08959, para. 5.1.3

[19] WIGGERS, Kyle. Google delays move away from cookies in Chrome to [online]. 27 July 2022 [viewed 19 December 2022]. Available from: https://techcrunch.com/2022/07/27/google-delays-move-away-from-cookies-in-chrome-to-2024/

- *Is the data collected and exchanged between AdTech companies engaged in online behavioural advertising covered by the concepts of "personal data" and "terminal equipment information"?*

- *To what extend are different parties involved in online behavioural display advertising responsible for the overall data processing performed?*

Given that data protection law is rather technical in nature and the application of its key concepts – such as the classification of data as "device data" or "personal data" or the identification of the responsible data controller – is highly dependent on the technical setup of the assessed data processing activities, I will first need to perform a detailed fact finding to learn how data is treated by the technical systems used for delivery and targeting of online advertisements[20].

Thus, in the first part of this paper, I will use induction and analytical methods to examine the technical nature of the data processing occurring in the leading real-time bidding ecosystems used for online display advertising and identify key observations to be used as a basis for my subsequent legal assessment. Based on the findings of the empirical part, I will then identify the main applicable laws and examine in detail whether the activities performed by AdTech companies when conducting online behavioural advertising comply with the requirements of the identified laws to the extent necessary to answer the outlined research questions. Within the legal assessment, I will primarily rely on a comparative assessment and synthesis of guidance found in case law, authority opinions and relevant academic literature.

In light of the sudden increase in data protection enforcement against AdTech companies and recent technical changes in the digital advertising landscape, I believe this paper may bring helpful insights into the ongoing discussion on privacy protection in online behavioural advertising.

[20] The technical assessment is performed as to the state in August 2022.

1. Introduction to Online Behavioural Advertising

1.1. Online Behavioural Advertising

In attention markets, human attention is scarce and valuable. New technologies that use data to profile and monitor users help scale down competition for attention at the individual level. Since sharing user attention with "rivals" lowers its value for advertisers, composition of audiences is of high importance and advertisers are willing to pay more for "exclusive" eyeballs than for those that can be reached through multiple means[21]. In digital advertising, this new user-centric approach is enabled by behavioural advertising technologies.

Boerman defines online behavioural advertising ("**OBA**") as "*the practice of monitoring people's online behaviour and using the collected information to show people individually targeted advertisements*"[22]. In this context, online behaviour may include basically any data about users that advertisers may find useful to target ads, including socio-demographic data, location, user interests, search and browsing history, purchases made, information about device usage, content shared as well as interactions with ads or other online experiences.

The popularity of OBA is closely tied to the use of programmatic technologies. Since advertisers are able to buy ad space in real time separately for each individual user, the knowledge they have about that user gains on importance. According to a 2016 market study[23], behaviourally targeted ads have a click-through rate 5.3x higher on average than traditional non-targeted ads (with even better results for retargeting campaigns). Consumers also benefit from OBA – in addition to getting more relevant ads, increased efficiency of ad spending may ultimately be reflected in lower prices for the advertised products and services[24].

---

[21] ARGENTESI, Elena, Paolo BUCCIROSSI, Emilio CALVANO, Tomaso DUSO, Alessia MARRAZZO, and Salvatore NAVA. *Ex-post assessment of merger control decisions in digital markets* [online]. Rome: Lear, 9 May 2019. [viewed 19 December 2022]. Available from: https://www.learlab.com/publication/ex-post-assessment-of-merger-control-decisions-in-digital-markets/, p. 6

[22] BOERMAN, Sophie C., Sanne KRUIKEMEIER, and Frederik J. ZUIDERVEEN BORGESIUS. Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising* [online]. 2017, 46(3), 363–376 [viewed 18 December 2022]. ISSN 1557-7805. Available from: doi:10.1080/00913367.2017.1339368, p. 364

[23] IHS MARKIT. *The economic value of behavioural targeting in digital advertising* [online]. IHS Markit, September 2017. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2019/08/BehaviouralTargeting_FINAL.pdf

[24] UK Competition & Markets Authority. Online platforms and digital advertising. Market study final report. 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, p. 154

1.2. AdTech terminology

This thesis is primarily intended for legal practitioners and academics, who may be unacquainted with the jargon used by the advertising industry. Therefore, I find it practical to first introduce the standard vocabulary that will also be used herein[25]:

- "**ad**" will be used as an abbreviation for "advertisement";
- "**AdTech**", an abbreviation of "advertising technology", describes the software and tools used to run, manage, measure, and optimize digital advertising campaigns;
- "**publisher**" refers to anyone who produces content that attracts an audience and who wishes to monetize on that content by showing ads (typically a website or app provider);
- "**advertiser**" refers to anyone who wishes to acquire ad space to show their own promotional messages to an audience (typically a product manufacturer or distributor);
- "**inventory**", also known as "**ad space**" or "**ad slot**" means the available space that a publisher dedicates for advertisement on its website, app, or other media[26];
- "**creative**" is the actual manifestation of the advertisement that the audience is exposed to – most common types of creatives are text, image, video and audio;
- "**impression**" also known as "**ad view**" refers to each individual instance that a creative is displayed to an end-user (for example, when a user loads a webpage where an ad is displayed and subsequently refreshes that page, two ad impressions have been served);
- "**delivery**" or "**serving**" is the process, by which an ad is selected for display in an available ad slot and shown to its audience;
- "**targeting**" means the selection of the desired audience that best fits the advertiser's marketing objectives;
- "**conversion**" represents the advertiser's ultimate goal, depending on its individual marketing strategy – it is usually realized by audience viewing the ad, clicking on a promoted link, registering on the advertiser's website or buying its product;
- to set aside corporate arrangements, only the familiar brand name will be used to refer to large company groups (e.g. "Google" will be used for all Alphabet, Inc. affiliates).

[25] Key concepts of digital advertising are neatly explained in CLEARCODE. *The AdTech Book* [online]. Katowice: Clearcode S.A., February 2022 [viewed 23 August 2022]. Available from: https://adtechbook.clearcode.cc/.
[26] Although the terms are often used interchangeably, there is slight difference. "Ad slot" is the relevant part of the media that is dedicated for advertisement. "Ad space" is the actual space within the ad slot, where the ad will be displayed. "Ad inventory" refers to the collection of all ad space available on one media or offered by one publisher.

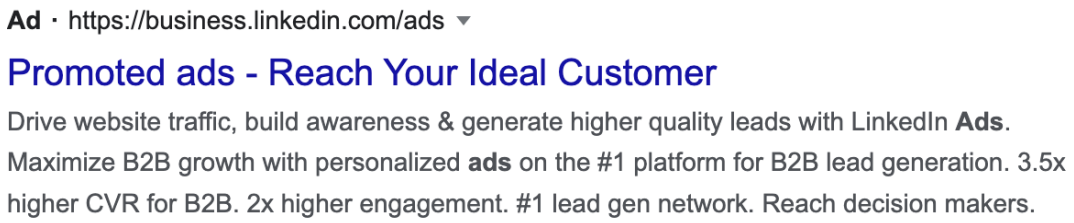
Other key terms will be explained in detail as I encounter them throughout the thesis.

1.3. Types of online advertising

The advertising industry consistently distinguishes between two digital advertising methods that make up the vast majority of all online advertising – search and display[27]. While both methods may leverage user data to better target ads, for several reasons, I have selected display advertising as the primary focus of my thesis. Firstly, programmatic techniques of ad delivery used in display advertising rely heavily on users' behavioural data. Secondly, programmatic is facilitated through widespread data sharing, which raises important legal questions. Finally, the involvement of a large number of market players in different roles makes compliance far more challenging. Nonetheless, some of the findings hereof may also be relevant to data-driven search advertising.

1.3.1. Search advertising

Search advertising, dominated by Google, takes place (as the name suggests) in online search engines. In essence, when a user performs an internet search, the search engine holds a real-time micro-auction in which advertisers may bid on keywords used in the search query. When the search engine retrieves organic search results based on relevance, it mixes in sponsored links provided by the highest bidders. The result may look like this:



The image shows the first displayed result of my "search advertising" query on Google's search engine [23 August 2022].

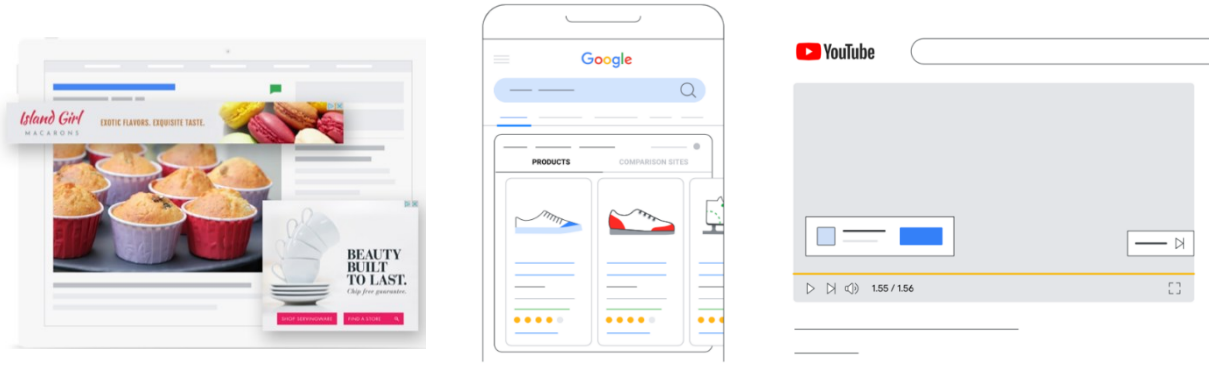
[27] In 2021, search and display represented (respectively) 42.9 % and 49.6 % of European digital ad spend. See: IAB EUROPE. *ADEX Benchmark 2021 Report* [online]. IAB Europe, June 2022. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2022/06/IAB-Europe_AdEx-Benchmark-2021_REPORT.pdf

Targeting of search ads is centred around keywords. By bidding on specific keywords used in user queries, advertisers ensure that their websites will be shown to people looking for the products they offer. However, even search advertising is starting to rely on behavioural targeting. For example, Google Ads already incorporates smart bidding technologies[28]. By analysing data about the user performing the search, smart bidding automatically adjusts advertisers' bids according to the likelihood that the search will lead to conversion.

Since search advertising is administered directly by each search engine, the market is highly integrated. In 2020, the UK's Competition and Markets Authority ("**CMA**") identified Google as the absolute leader with over 90% share on search ad revenue[29].

1.3.2. Display advertising

Display advertising is the collective term used to describe graphic ads on websites, social media and in apps. While search advertising is especially important for retargeting strategies, display advertising is the primary method used for building brand awareness[30]. Examples of display ads include advertising banners filling out unused space on websites, native ads imitating user-generated content in apps, shopping suggestions in internet search or short bumper ads that interrupt video playback. The results may look like this:



Examples of different display ad types used by Google[31].

[28] GOOGLE. *About automated bidding* [online] [viewed 19 December 2022]. Available from: https://support.google.com/google-ads/answer/2979071?hl=en&ref_topic=6294205
[29] UK Competition & Markets Authority. *Online platforms and digital advertising. Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, par. 5.46
[30] OECD. *Competition in digital advertising markets* [online]. OECD, 2022. [viewed 19 December 2022]. Available from: https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf, par. 2.2.2
[31] GOOGLE [viewed 25 August 2022]. Available from: https://support.google.com/

In addition to a wide variety of creative types, display advertising is also very dynamic in terms of ad delivery. Since display ads may be used in any digital channels and are not tied to a specific service provider (e.g. a search engine), the display advertising market is far more decentralized. Thanks to the widespread use of programmatic technologies (described in detail in Chapter 1.4 below), the final ad that will be shown to the user is often selected through automated processes in complex ecosystems of advertisers, technology providers and marketing intermediaries. Even though very large online platforms reap the lion's share, a big portion of display ads is still administered through the open display market[32].

1.4. Programmatic advertising

Traditionally, if you wanted to have your ad published in media, you would need to reach out to the publisher and individually negotiate the terms of the placement. This method of ad delivery is commonly referred to as a "**direct deal**". Unfortunately, direct deals offer only limited ad visibility (only the readers of the selected media will see the ad), involve costly administration, and significantly curtail opportunities to target your preferred audience. Naturally, placing the ad only makes sense for you if it allows you to reach your potential customers. For example, if you sold cars, you would probably seek to publish your ad in a magazine for car enthusiasts. This is the simplest form of audience targeting – **contextual advertising**.

To solve the inefficiencies of direct deals, programmatic advertising developed as the main method for delivering ad impressions in online display advertising. Although direct deals and contextual advertising are still relevant – especially for high-value inventory[33] – programmatic tools allow for more advanced targeting strategies, such as **retargeting**. For instance, if the advertiser manages to identify that the user has previously visited their website,

[32] According to the CMA, over half of UK's 2020 display expenditure was generated by Meta, followed by Google's YouTube. The open display market then represented around 32% of display expenditure. See: UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, par. 5.8.

Dominance of Meta and Google has also been investigated in other European markets. See: OECD. *Competition in digital advertising markets* [online]. OECD, 2022. [viewed 19 December 2022]. Available from: https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf, par. 4.1.1.

[33] DELVIFY. Types Of Programmatic Deals: A Guide [online] [viewed 19 December 2022]. Available from: https://delvify.media/types-of-programmatic-deals-a-guide/

placed items into the shopping cart but failed to check out, they will bid higher to show their ad to this specific user.

Undoubtedly, the industry is moving to programmatic. In 2021, programmatic accounted for the majority of all European as well as worldwide display advertising[34]. As opposed to direct deals, programmatic technologies allow for a more granular way of ad placement, helping publishers to instantly find demand for their advertising space, advertisers to better connect with their target audience and consumers to receive relevant ads tailored to their individual needs. According to Bush[35], programmatic advertising is defined by the following principles:

- **granularity** – decisions about ad placement are made on the level of individual impressions;
- **real-time trading** – the advertiser is selected at the time the advertising opportunity arises;
- **real-time information** – decisions are based on highly specific characteristics and user data;
- **real-time creation** – advertisers serve the ad immediately after winning the ad space;
- **automation** – the whole process is automated.

Put simply, programmatic advertising is the automated process for serving of digital ads in real time based on individual ad impression opportunities and user data. In other words, instead of buying a specific ad space on one publisher's website, advertisers transact separately for every single opportunity to show an ad to a particular user. This allows advertisers to independently assess the value of each transaction and optimize their bid based on its utility for reaching their goals (such as the probability of a user clicking on the displayed ad)[36]. Without

[34] Programmatic accounted for 57% of European non-social display advertising in 2021. See: IAB EUROPE. *ADEX Benchmark 2021 Report* [online]. IAB Europe, June 2022. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2022/06/IAB-Europe_AdEx-Benchmark-2021_REPORT.pdf

According to GCG, 72% of worldwide display ads in 2021 were served through programmatic. See: GREENWICH CAPITAL GROUP. *Industry Update. Adtech & Marketing Services Q4 2021* [online]. 2022 [viewed 19 December 2022]. Available from: https://greenwichgp.com/wp-content/uploads/2022/03/AdTech-and-Marketing-Services-Industry-Update-Q4-2021.pdf

[35] BUSCH, Oliver. The Programmatic Advertising Principle. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 8

[36] WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049, p. 48

automation, such level of detail could never be achieved given the extreme volume and speed of the resulting transactions. Generally, the entire process for the sale of ad impressions is completed before the website loads in the user's browsers and takes less than 100 milliseconds[37].

Another great benefit of programmatic is aggregation. Through programmatic tools provided by intermediaries, publishers (the supply) may offer their available advertising space to countless advertisers (the demand), creating complex ad impression marketplaces. For example, the Google Display Network spans across over 2 million websites, videos, and apps claiming to reach 90% of internet users worldwide[38].

Given the technical properties of programmatic advertising, there are rarely any direct negotiations between the publisher and the advertiser. The legal terms of the campaign are mostly imposed by the involved intermediaries facilitating the ad delivery or set through functionalities offered by those intermediaries[39]. For example, the publisher usually sets the per-impression price or the floor price (in auction-type mechanisms), the advertiser designs their bid and sets targeting parameters.

Although programmatic methods are currently mostly used for online display advertising, programmatic is just as well suitable for other online and even offline channels. The AdTech industry is already working hard to expand the use of programmatic technologies. For example, with the eager development of connected TVs, AdTech experts predict programmatic TV – a TV that serves both content and ads automatically according to the user's preferences – as a real possibility for the future[40]. What is more, programmatic ad serving could find its way even to offline channels. For digital out-of-home (e.g. ad banners at bus stops), programmatic could be a promising way to maximize ad revenue. Some advertising companies are already known to experiment with behavioural out-of-home ads that adapt according to the passer-by to attract their attention or measure their responses to the ad. Curiously, programmatic

[37] *ibid*., p. 2
[38] GOOGLE. Display Network: Definition [online] [viewed 19 December 2022]. Available from: https://support.google.com/google-ads/answer/117120?hl=en
[39] In its 2020 report, the UK CMA discusses the issue of unequal bargaining power between publishers and large platforms providing advertising services. See: UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, par. 6.36
[40] BUSCH, Oliver. The Programmatic Advertising Principle. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 13

methods have also been applied in offline retail. A start-up in Berlin has created a programmatic coupon system. Prior to entering the store, the user would present their loyalty card, which is used to record their purchases. Next, the system holds a micro-auction between participating grocery producers for discounts to be offered to the user based on the user's shopping habits[41].

1.4.1. Categories of programmatic advertising

Before taking a closer look at real-time bidding – the most prevalent programmatic method today – I would like to briefly describe the different subtypes of programmatic advertising[42].

Open Auction	Private Auction	Preferred Deals	Programmatic Guaranteed
Buyers: Hundreds of buyers	**Buyers:** Several advertisers (by invite)	**Buyers:** One-to-one	**Buyers:** One-to-one
Pricing: Auction pricing	**Pricing:** Auction with CPM floor	**Pricing:** Fixed CPM pricing	**Pricing:** Fixed CPM pricing
Impressions: Unreserved impressions	**Impressions:** Unreserved impressions	**Impressions:** Unreserved impressions	**Impressions:** Reserved impressions

Summary of programmatic deal types offered in Google AdSense[43]. "CPM" or "cost per mile" is the price paid for 1000 ad impressions.

The simplest form – **programmatic guaranteed** (also called **programmatic direct**) – is basically an automated way of preforming direct deals for guaranteed inventories (mostly highly viewable ad spaces on popular websites rich in first-party data)[44]. Given their high value, these ad slots are usually sold in bulk for a guaranteed price. The buying process requires no auctions and can be compared to buying items on an e-shop – the publisher places their inventory for sale and the deal is closed once an advertiser makes their order. The inventory is then reserved in the sense that the advertiser is obliged to serve the agreed number of

[41] WAESCHE, Niko Marcel, Tilman ROTBERG and Florian RENZ. The Contribution of Measurement in a Cross-Device, Data-Driven, Real-Time Marketing World. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 155

[42] A helpful summary of different programmatic deal types highlighting their key differences has been provided by AdTech company Ad Butler. See: ADBUTLER. *Types of Programmatic Advertising: Deals & Formats Explained* [online]. 9 March 2021 [viewed 19 December 2022]. Available from: https://www.adbutler.com/blog/article/types-of-programmatic-advertising-deals-and-formats-explained

[43] GOOGLE. *Google Marketing Platform Academy* [online] [viewed 30 August 2022]. Available from: https://marketingplatformacademy.withgoogle.com/

[44] WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049, p. 69

impressions at a fixed price and the publisher may no longer offer the ad space for sale. Like in manual direct deals, the primary targeting method is contextual.

In **preferred deals**, publishers give priority to advertisers with a preferred deal arrangement. These advertisers have the option to buy the ad impressions for a fixed price before they are submitted to the open exchange. Thus, preferred deals are similar in functioning to the right of first refusal[45]. However, the inventory is not reserved and if the publisher chooses to opt for a programmatic direct deal with another advertiser, they are not obliged to honour the preferred deal. Preferred deals give advertisers priority access to high-quality inventory but allow for more flexibility than programmatic guaranteed. For publishers, they usually generate a higher yield than open auctions. In practice, preferred deals take place simultaneously with open auction bidding – if an advertiser with a preferred deal joins the auction, they have priority regardless of the bids placed, otherwise, the largest bidder wins.

Private auctions are almost identical to open auction bidding with the exception that only invited advertisers may participate. They tend to offer more exclusive inventory for higher prices. In addition, through whitelist functions, both sides have better visibility over who they contract with.

Open auctions via real-time bidding are the most open form of programmatic deals. **Real-time bidding** (commonly abbreviated as "**RTB**") was developed in the late 2000s as a protocol for selling off leftover inventory[46]. However, it quickly became the industry standard for most online display advertising. In essence, RTB is an automated process for buying and selling of online advertising space through real-time auctions based on user data[47]. Since RTB is realized through open market auctions, it can be compared to stock market transactions[48]. However, thanks to programmatic technologies, the entire process of an RTB auction from

[45] ADBUTLER. *Types of Programmatic Advertising: Deals & Formats Explained* [online]. 9 March 2021 [viewed 19 December 2022]. Available from: https://www.adbutler.com/blog/article/types-of-programmatic-advertising-deals-and-formats-explained

[46] CLEARCODE. *The AdTech Book* [online]. Katowice: Clearcode S.A., February 2022 [viewed 23 August 2022]. Available from: https://adtechbook.clearcode.cc/, p. 164

[47] I have used my own definition to best highlight the key aspects of RTB. An overview of different industry (mainly Google's or IAB`s definition) and academic definitions can be found in VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden). Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284, p. 20, par. 1.1.

[48] WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049, p. 49

creating an ad impression opportunity to evaluating, selling, processing, and serving an ad to users occurs nearly instantly[49]. The scale of RTB is truly tremendous – according to ICCL's estimates, on average, 239 RTB broadcasts take place each day per every person in the Czech Republic[50]. For leading ad exchanges, the amount of bid requests received is estimated at tens to hundreds of billions daily[51].

As identified above, RTB is the most complex method of programmatic display advertising. At the same time, out of all ad delivery methods for display advertising, RTB benefits the most from OBA techniques. Since ad slots are traded per-impression in real-time auctions, user data is crucial. Elements of RTB can be found in other programmatic methods – for example, private auctions employ the same auction mechanism. Preferred deals and programmatic guaranteed appear to be more straightforward than RTB in terms of buying mechanism; however, they also employ programmatic tools administered by advertising intermediaries. Due to the widespread use and complexity of RTB as well as its high reliance on OBA techniques, I have chosen RTB as the primary focus of my examination of the online display advertising landscape. Although other programmatic methods will not be further discussed, the findings for RTB may also be relevant to those methods, where they exhibit features that are also present in RTB.

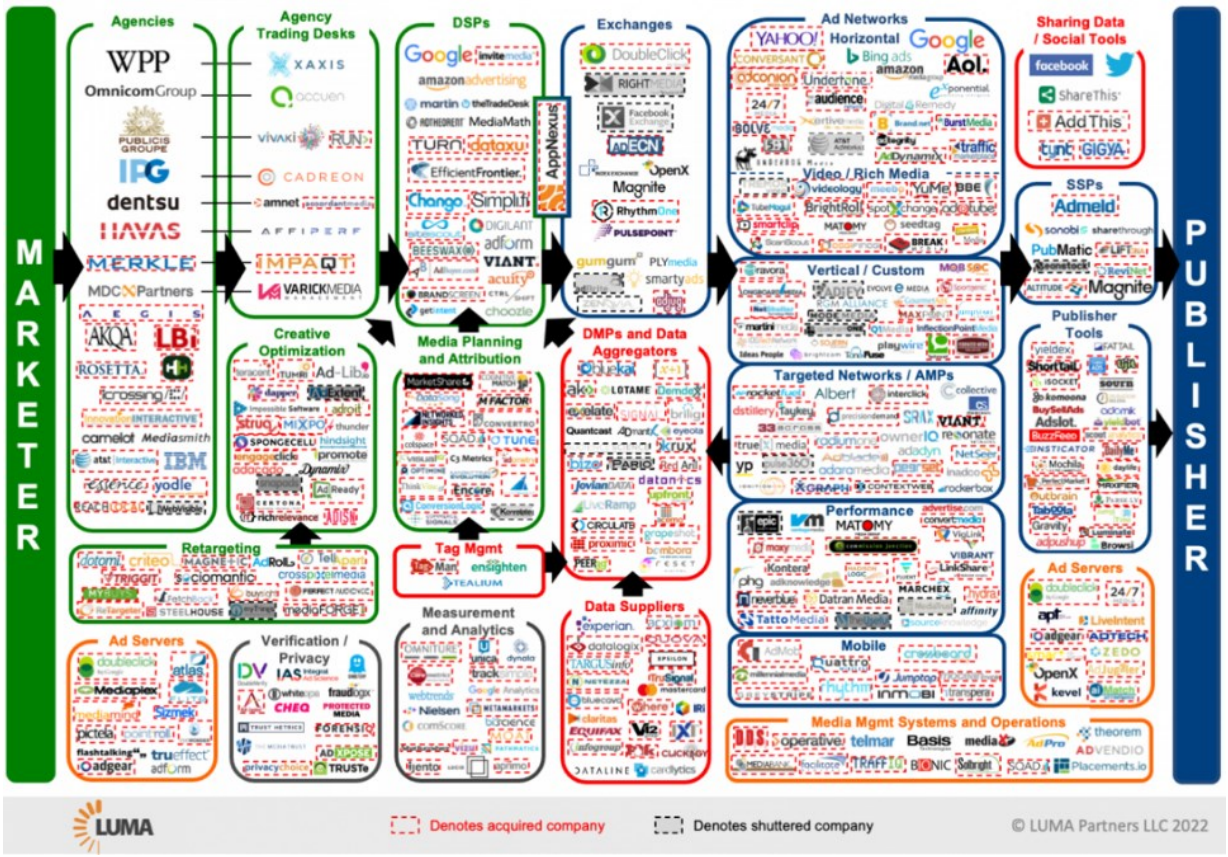
1.4.2. RTB ecosystems

Open market RTB transactions are characterized by the involvement of a large number of advertising intermediaries who each serve a specific purpose in facilitating different parts of the transaction process. Based on the function that those intermediaries perform within the RTB process, it is possible to categorize them into several groups. Since RTB protocols allow for multiple parties to appear in the same role and compete between each other, it is indeed more fitting to speak about "RTB ecosystem" rather than a supply chain.

[49] BUSCH, Oliver. The Programmatic Advertising Principle. *Programmatic Advertising*. Cham: Springer International Publishing, 2016. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6, p. 9

[50] IRISH COUNCIL FOR CIVIL LIBERTIES. *The Biggest Data Breach* [online]. Dublin: 16 May 2022 [viewed 19 December 2022]. Available from: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

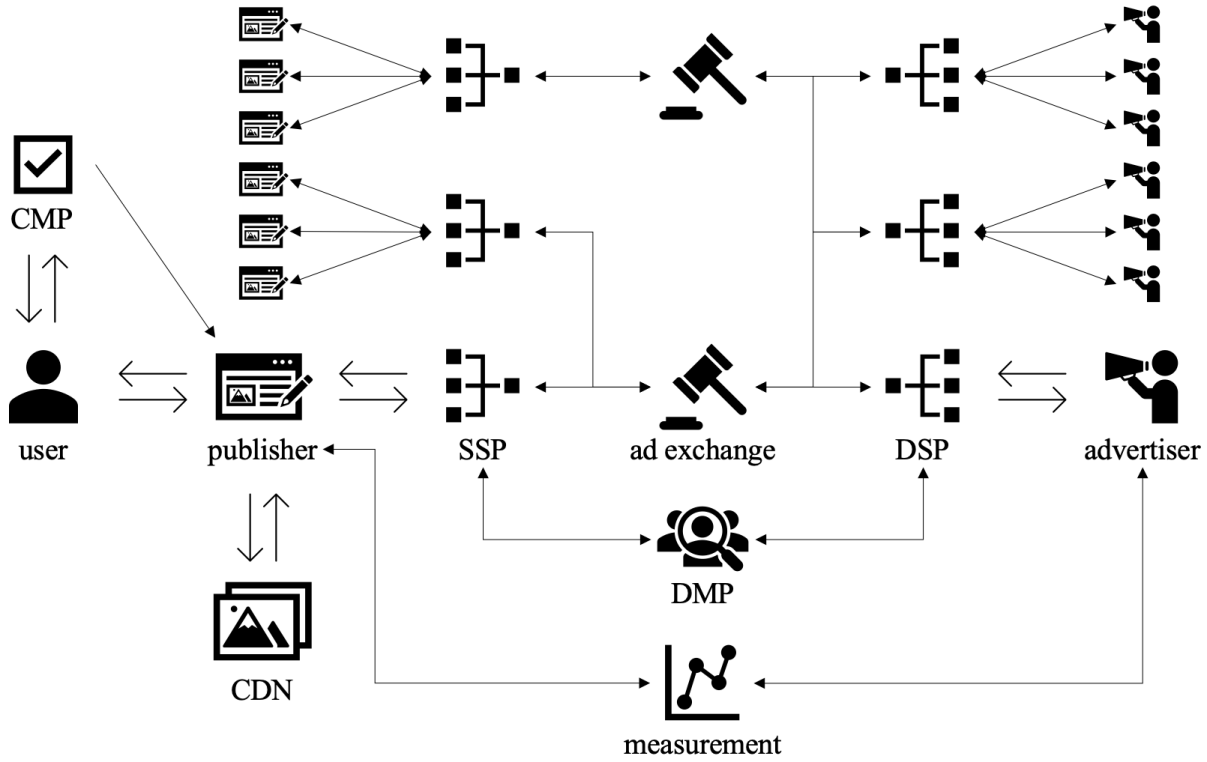
[51] FIX ADTECH. *Appendix on market saturation of the systems* [online]. 4 February 2019 [viewed 19 December 2022]. Available from: https://fixad.tech/wp-content/uploads/2019/02/4-appendix-on-market-saturation-of-the-systems.pdf



Display LUMAscape[52] *is a popular visual guide to the AdTech ecosystem featuring the most influential companies in the digital advertising industry.*

Before discussing the RTB auction mechanism, I will briefly describe each category of RTB players and the function they serve.

[52] LUMA PARTNERS LLC. *Display LUMAscape* [online]. Luma Partners LLC, 2022. [viewed 30 August 2022]. Available from: https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/



Illustrative scheme of the RTB ecosystem.

- **Publishers** create content that attract users' attention and sell this attention to advertisers. They collect first-party data about user interactions with their websites or apps. Since they are in direct contact with users, they are also uniquely positioned to address any privacy requirements such as collecting users' consents with the RTB data processing. Large publishers – such as Meta and Google – often use their own tools to sell inventory directly to advertisers, cutting out AdTech intermediaries.

- Some publishers outsource privacy compliance to **consent management platforms** ("**CMPs**"). Consent tools embedded in publishers' websites allow CMPs to collect users' data processing preferences and administer them across different apps and websites.

- **Supply-side platforms** ("**SSPs**") are AdTech providers that act as network optimizers for publishers. They connect publishers with ad exchanges, allowing them to target several advertiser networks via a single bid request. In addition, they provide software tools that help publishers manage their inventories and set the parameters of their bid requests, such as the per-impression floor price. Since each SSP acts as an agent for

multiple publishers, SSPs aggregate the supply of inventory and remove the need to contact each publisher separately.

- **Ad exchanges** connect publishers and SSPs with hundreds of advertisers and DSPs and act as virtual auction houses for RTB transactions, evaluating the price and quality of impressions. By grouping parties on the supply and demand side, they expand the pool of potential contracting parties and help both sides get access to better deals, without having to redirect to each counterparty separately.

- **Demand-side platforms** ("**DSPs**") are AdTech providers that act as network optimizers for advertisers. DSP tools allow advertisers to manage their ad campaigns and set up their bidding and targeting strategies. By grouping together advertisers, they aggregate the demand side of the RTB market. A**gency trading desks** ("**ATDs**") are similar to DSPs. However, as opposed to DSPs that only provide software tools, ATDs usually also offer professional services and manage DSP tools on behalf of their clients. However, not all publishers allow the use of DSPs. Platforms with significant recognition may rather chose to provide their own tools to reserve direct contact with advertisers for themselves. For example, advertisements on Facebook, Instagram and Messenger are sold exclusively by Meta's own Ads Manager.

- **Advertisers** represent the demand for ad impressions. They place bids in RTB auctions either alone or through DSPs. After winning an auction, they provide the creative that is displayed to the user. Advertisers often make use of **content delivery networks** ("**CDNs**") – global distributed networks of servers – to ensure minimum delays when ad impressions are served across longer geographical distances.

- To verify that ads are properly displayed, to measure their performance, and prevent ad fraud, parties may employ third-party **measurement vendors**. RTB protocols standardly offer software developer kits ("**SDKs**") that allow parties to involve viewability and measurement vendors.

- **Data management platforms** ("**DMPs**") are used to improve audience targeting. They specialize in aggregation of consumer data and creation of extensive user profiles to

learn about user interests. In RTB, they act as data brokers, help identify users (such as by matching user IDs across platforms) and enrich targeting data included in bid requests. Data held by DMPs is usually acquired from third parties such as e-shops and brick and mortar stores, credit card companies, ISSPs or from publicly available sources such as social media. For publishers, DMP services increase the value of their inventory, while advertisers benefit from improved ad targeting.

Naturally, not all RTB systems involve all the above parties. While advertising intermediaries certainly contribute to the efficiency of RTB processes, they also consume a significant share of the profits, decreasing net revenue for publishers. According to a PwC study conducted in 2020[53], intermediary fees take up almost half of the expenses paid by advertisers. Although the UK CMA found[54] that the "AdTech take" could be closer to 35 %, it considered that this may be an underestimate.

To decrease intermediary costs, advertisers and publishers may at times choose to cut out the agents (such as DSPs and SSPs) and perform some of their functions in-house. Instead of using ad exchanges, advertisers may also connect directly to SSPs that offer an exchange function (especially for less complex programmatic deals such as preferred deals or programmatic guaranteed). In addition, some companies provide services that cover several functions at once. For example, Google offers services to both publishers (Google Ad Sense and Google Ad Manager) and advertisers (Google Ads and Google Display & Video 360), runs its own ad exchange (Google Ad Exchange) and even develops its proprietary RTB protocol (Authorized Buyers)[55].

1.4.3. The RTB protocol

RTB protocol lies at the heart of RTB ecosystems. To be able to effectively operate on the same market, RTB players need a common way of communication. The RTB protocol

[53] PRICEWATERHOUSECOOPERS LLP. *Programmatic Supply Chain Transparency Study* [online]. London: The Incorporated Society of British Advertisers Ltd, May 2020 [viewed 19 December 2022]. Available from: https://www.isba.org.uk/system/files?file=media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf

[54] UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, p. 273

[55] For a great overview of Google's presence across the whole AdTech stack (with over 50% market share at each level), see *ibid*., p. 271

provides a set of application programming interface ("**API**") specifications that AdTech providers incorporate into their software tools to ensure interoperability with tools provided by other AdTech companies. RTB protocol defines the auction mechanism, the contents of bid requests and bids responses submitted in RTB auctions and determines the data formats in which participants exchange information about themselves (e.g. content of the destination website), the parameters of the auctioned inventory (e.g. size and proportion), the terms of the deal (e.g. floor price or bid value), data about the user (e.g. the user's purchase interests), and the creatives to be displayed. Currently, the industry relies on two leading RTB protocols[56]:

- **OpenRTB**[57] protocol is developed by the Interactive Advertising Bureau[58] ("**IAB**") – a worldwide non-profit trade organization comprised of over 700 leading advertising companies that develops AdTech technical standards and solutions. Even though the OpenRTB version 3.0 has already been released in 2018, the majority of AdTech vendors still run on 2.X versions of the protocol due to extensive costs of migrating to v. 3.0[59]. For this reason, I will predominantly base my findings on OpenRTB v. 2.6 introduced in April 2022.

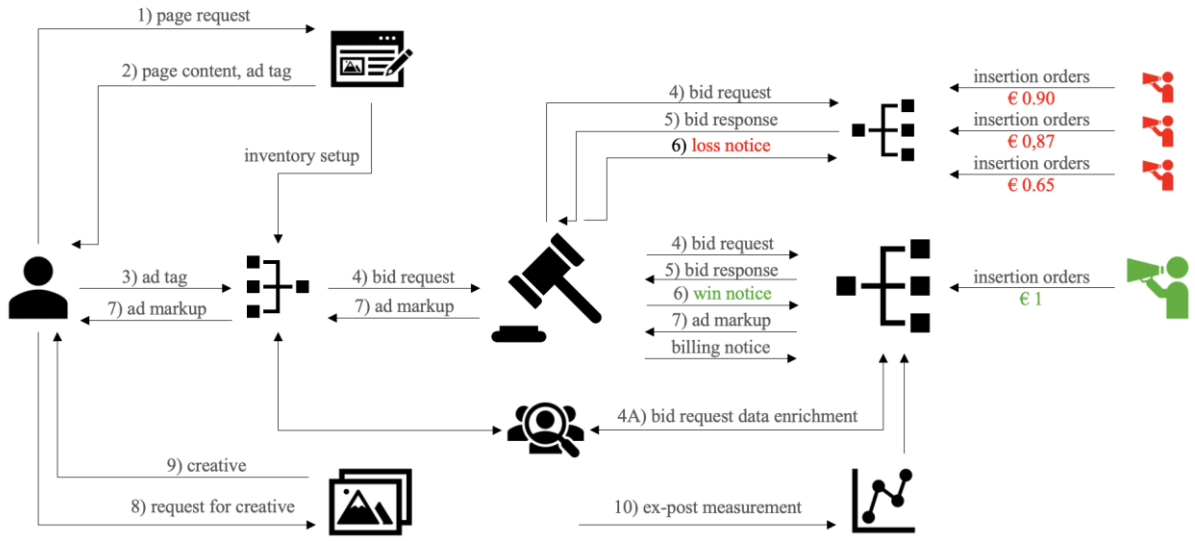
- **Authorized Buyers**[60] is Google's proprietary RTB system. However, in its ad exchange, Google also supports the use of OpenRTB.

Other popular RTB protocols include the **Facebook Exchange** and **AppNexus Creative API**[61].

[56] ICO. *Update report into adtech and real time bidding* [online]. 20 June 2019. Available from: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, p. 14
[57] IAB TECH LAB. OpenRTB Version 2.6 [online]. IAB Technology Laboratory, April 2022 [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide
[58] In the EU, IAB is represented by its local branch IAB Europe. However, technical standards are mostly developed by its US affiliate IAB Technology Laboratory, Inc.
[59] THE MEDIAGRID. The publisher brief: OpenRTB 2.6 and the addressable future of CTV [online]. the mediagrid [viewed 19 December 2022]. Available from: https://blog.themediagrid.com/the-publisher-brief-openrtb-2.6-and-the-addressable-future-of-ctv
[60] GOOGLE. Authorized Buyers Real-time Bidding Proto [online]. Google, 2022 [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide
[61] VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden). Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284, p. 146

1.4.4. RTB auctions

The process of an RTB auction is similar under both Authorized Buyers and Open RTB, as it is constrained by the technical possibilities of the HTML protocol. The process takes place in the following steps:



Infographic explaining the process of an RTB auction. Icons used herein for different RTB players are explained above in the illustrative scheme of the RTB ecosystem.

0) Before the process is initiated, both sides set up their AdTech tools. Publishers register their inventory with their SSPs and insert the bid request parameters – most importantly, the auction floor price. In DSP tools, advertisers create **insertion orders** specifying their budgets, performance goals and targeting parameters.

1) The auction process starts when the user's browser makes a request to the publisher's server to load a webpage[62] that contains an empty ad slot.

2) In response to the browser's request, the publisher's server returns the page's content in HTML code together with an ad tag for the relevant ad slot.

[62] The auction process is demonstrated on website advertising. However, it may also be used to serve ads in apps, video playback, connected TV, or even on out-of-home ad banners.

3) **Ad tag** is a piece of code that initiates a HTML redirect and instructs the user's browser to retrieve the ad from an AdTech server (such as an ad server or SSP). Together with the ad request, the browser passes on certain data about the user (such as device and cookie data).

4) Once the browser makes a call to an SSP, the SSP initiates the RTB auction by broadcasting a **bid request** to all connected ad exchanges, DSPs and advertisers. The bid request contains information about the publisher, the ad impression, terms of the deal, and data about the user attempting to load the ad in the format prescribed by the RTB protocol in use.

4a) Both SSPs and DSPs may use additional data acquired from DMPs to identify the user and enrich the bid request to increase targeting potential.

5) Based on advertisers' insertion orders, DSPs reply to the bid request with bid responses, each stipulating the advertiser's bid and details about the advertiser and the creative.

6) The ad exchange compares the bids, and the highest bidder wins the impression. Win and loss notices are then sent to the participating advertisers.

7) In response to the win notice (unless it was already included in the bid response), the winning advertiser provides an **ad markup** – a code snippet to be rendered in the user's browser to retrieve the creative.

8) Executing the ad markup in the user's browser triggers a redirect to the advertiser's ad server or a CDN, where the creative is stored. In addition to creative delivery, ad markup is also used to load tracking tags for ad verification, measuring and ad fraud prevention purposes.

9) From there, the browser loads the creative into the ad slot and the ad is displayed to the user.

10) Through tracking pixels, dedicated JavaScript features or open measurement SDKs, publishers and advertisers can then verify viewability of the ad and measure user engagement metrics, such as clicks or conversions.

Generally, auctions are performed at several levels. For example, once an ad exchange receives bid responses from advertisers, it carries out the auction and selects the winning bid. Winning bids from different ad exchanges are then sent to the publisher's SSP which determines the final winner. To increase revenue and fill rates, publishers sometimes use a waterfall structure (subsequent calls to several ad exchanges until the ad slot is filled) or header bidding (a JavaScript that concurrently triggers several SSPs, collects their winning bids and performs a final evaluation at the browser level).

1.4.5. RTB bid request

For the purposes of this paper, it is also necessary to take a closer look at the anatomy of a bid request. In RTB, bid requests provide advertisers with all the details necessary to place their bid. They identify the publisher, the terms of the deal, and describe the offered ad impressions. Bid requests are also a key element of OBA – in the **objects** (data fields) of a bid request, RTB parties exchange valuable information about users that forms the basis for ad targeting.

From a bid request adhering to the most common RTB protocols, advertisers may learn in particular the following information relevant for targeting[63]:

- **site/app data**, such as the URL of the website/app visited and description of its content (e.g. content title, ID of a specific content category within a content taxonomy[64], content keywords, content type description, content language, etc.);

[63] For great summary of bid request objects relevant to OBA targeting under the OpenRTB and Authorized Buyers protocols, see RYAN, Dr Johnny. *Report from Dr Johnny Ryan – Behavioural advertising and personal data* [online]. Brave Software, Inc., 5 September 2018. [viewed 19 December 2022]. Available from: https://brave.com/static-assets/files/Behavioural-advertising-and-personal-data.pdf

[64] For the taxonomy used in OpenRTB, see IAB TECH LAB. Content Taxonomy [online]. IAB Technology Laboratory [viewed 28 August 2022]. Available from: https://iabtechlab.com/standards/content-taxonomy/

- **device data**, such as the user's IP address, hardware manufacturer, brand, model and operating system, device ID (such as IMEI or Android ID), browser software; data about network connection and carrier, language settings, screen dimensions;
- **user demographics**, such as their date of birth and gender;
- **user location**, such as GPS coordinates, country, city, and ZIP code;
- **user identifiers**, such as a unique ID assigned to the user by the publisher, DMP or other AdTech intermediary;
- **user interests**, usually communicated in the form of keywords or vertical IDs[65].

As explained above, in order to perform RTB auctions, bid requests containing these types of data are disseminated to hundreds or thousands of participating parties across the world. For this reason, some academics (such as Dr Johnny Ryan) refer to bid requests as RTB "broadcasts".

1.4.6. Privacy controls in RTB

Bid requests may also be used to communicate user's privacy preferences. For example, OpenRTB bid request flags the applicability of GDPR (marked as YES/NO) and whether the publisher maintains a privacy policy (also as YES/NO only). Additionally, to avoid revealing user's private data, some bid request objects may be encrypted via a hash function[66]. For example, both OpenRTB and Authorized Buyers communicate hardware and device IDs in their hashed form.

OpenRTB further includes a "do not track" and "limit ad tracking" flags to notify bidders about user preferences. However, the objects have merely contractual significance and do not amount to any technical impediments in use of the bid request data.

[65] Verticals are narrowly defined categories of products or topics that users may be interested in. For ease of use, AdTech players create comprehensive lists of verticals, assigning each a unique ID. For example, see Google's publisher verticals at https://developers.google.com/adwords/api/docs/appendix/verticals

[66] Hash function is a one-way mathematical operation that transforms a data set into a fixed-size value. For example, when encrypted through SHA-1 hashing, the sentence „The red fox jumps over the blue dog" will look like this: „0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC". It is impossible to determine the original value from its hash. However, applying the same hashing function to the same original data will always lead to an identical hash value. See: Cryptographic hash function [online]. Wikipedia [viewed 19 December 2022]. Available from: https://en.wikipedia.org/wiki/Cryptographic_hash_function

In Authorized Buyers, some bid request objects are dependent on privacy settings. Most importantly, the bid request includes a "privacy treatment" object, which allows publishers to flag that the user has opted out of personalized advertising. Including this object in a bid request will cause certain data – namely the Google User ID, cookie data obtained through matching with the User ID, session ID and device IDs – to be cleared from the bid request. Authorized Buyers also states that location data is fuzzified "as necessary to protect user privacy" (although details are not provided). By deselecting the "data collection" option, publishers may further bar bid request recipients from further processing user data for profiling[67]. However, the signal does not limit the amount of data communicated in a bid request and thus represents merely a contractual restriction. Naturally, prohibiting data collection may lead to decreased ad revenue, since user data shared in bid requests represents a valuable resource for advertisers.

Initiatives to promote user privacy in RTB include the IAB Transparency and Consent Framework ("**TCF**"). TCF is an IAB framework for cross-platform tracking of user consent. To participate in the TCF, AdTech companies must be registered in the Global Vendor List managed by IAB. The Global Vendor List uses a standardized list of processing purposes, requiring each vendor to list the purposes for which they intend to process user data and the legal bases relied upon. This allows publishers to choose which vendors will be allowed to process their users' data for OBA purposes and to include those vendors in their website's consent tool. The TCF also features a protocol for communicating privacy preferences between OBA stakeholders. When a user submits their data processing preferences – such as through a CMP cookie banner provided on a publisher's website – the users preferences are recorded in a TC string placed on the user's device by a CMP domain. The consent cookie records the binary value of consent granted for each processing purpose and each authorized AdTech vendor. Both OpenRTB and Authorized Buyers include the TC string as an object in bid requests, allowing RTB players to easily communicate users' data processing preferences. Recently, the legality of TCF has been significantly challenged by the Belgian DPA as will be further discussed in next chapters[68].

[67] GOOGLE. *Google Marketing Platform Academy* [online] [viewed 30 August 2022]. Available from: https://support.google.com/admanager/answer/11956152
[68] See the *IAB Ruling*.

Otherwise, RTB players rely mostly on contractual measures. For example, entities participating in Authorized Buyers must[69]:

- only upload creatives complying with Google's advertising policies on restricted content and restricted advertising practices;
- maintain a comprehensive privacy policy;
- not use any Flash Cookies, locally stored objects (e.g. HTML5 local storage) or fingerprinting for behavioural targeting;
- declare any calls to third-party servers (such as those used for bid request data enrichment, identity resolution, or tracking) and limit the number of third-party matching calls to the prescribed maximums;
- unless otherwise permitted, only involve certified vendors;
- collect valid user consent in line with the requirements of GDPR;
- unless specifically authorized refrain from using the acquired user data for purposes other than the buying of ad inventory;
- not use acquired data for user profiling if they are not the winning bidder;
- not use acquired data for data harvesting and delete all matched data upon user opt out;
- comply with all applicable laws and Google's policies.

Parties involved in the IAB TCF must also adhere to IAB's policies. Nonetheless, since IAB does not itself act as an AdTech vendor and OpenRTB only serves as a technical standard, the policies are less detailed and not so restrictive.

Even though both IAB and Google reserve the right to audit compliance with their policies, these policies have been repeatedly criticized for their unenforceability. Even the UK ICO agrees that in RTB ecosystems where bid requests are broadcasted to hundreds of parties without technical restrictions to limit the dissemination of user data, contractual measures are insufficient to protect users against data misuse[70]. Through contractual frameworks,

[69] The Authorized Buyers policies can be accessed from: GOOGLE. Authorized Buyers Help [online] [viewed 28 August 2022]. Available from: https://support.google.com/authorizedbuyers/?visit_id=637985105897694840-1257107195&hl=en&rd=1#topic=22149

[70] ICO. *Update report into adtech and real time bidding* [online]. 20 June 2019. Available from: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, p. 21

responsibility for compliance is thus shifted to the parties participating in RTB without any realistic means to consistently control how these entities dispose with the acquired data.

2. Advertising tailored to the user

2.1. Tracking users online

Wefers Bettink, Van Eijk, and Wagner define web tracking as *an act by a party, or host, or service, of reading or writing Unique Identifiers (UIDs) that are connected directly or indirectly to an end-user, computer, or device while the end-user is interacting with various services of the web, in order to collect, combine, or analyze data about the end-user for charitable, philanthropic, or commercial purposes*[71]. No elaborate examination is needed to point to the vast amounts of data that companies nowadays collect through direct interactions with users in both offline and online contexts, all of which can be used to learn about user behaviour for OBA purposes. However, as the definition shows, tracking is only possible when behavioural data can be linked, exchanged, and combined across different contexts. Therefore, to successfully serve targeted ads, it is not enough to have knowledge of a particular user's preferences. Companies must also be able to identify that user when the user is encountered by other OBA stakeholders. Performing such re-identification in digital environments represents a key obstacle for OBA.

Based on tracking accuracy, AdTech theory distinguishes between deterministic and probabilistic identification (matching). **Deterministic matching** is based on a common identifier that consistently marks the same user or device. Deterministic identifiers are highly accurate fixed identifiers such as user contact details (e.g. a name, telephone number, or e-mail address), HTML cookies or device ID. **Probabilistic matching** does not use a common identifier. Instead, individual pieces of information about the users' device or behaviour are analysed in combination to arrive at a statistical probability of a match. For example, if two devices regularly connect to the same private Wi-Fi, they are likely to belong to the same household. Although probabilistic matching is generally less effective than deterministic, it can increase the overall accuracy of user identification or assist where deterministic methods fail (e.g. when cookies are deleted or unavailable).

[71] WEFERS BETTINK, W., VAN EIJK, R., & WAGNER, F. Strictly Speaking: Cookies, Consent and Compliance. Europe Data Protection congress [presentation]. Brussels: IAPP, 2012. as cited in VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden) [online]. Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284

Tracking options vary across devices used and environments visited. Of course, user identification is simplest, when the users directly identify themselves such as by their e-mail or other fixed identifier. Many apps and online platforms also operate on a subscription basis, requiring their users to create a user account to take full advantage of their services. **Account identification** allows companies to consistently monitor user behaviour across their platforms or third-party platforms linked to their account (for example, many apps allow users to sign in via their Facebook or Google account as a single sign-on option). **Real-world identifiers** (such as a credit card number) can also help companies connect related data across data sets. These types of identification are particularly relevant for data collection and creation of user profiles. However, they usually cannot serve to re-identify the user in OBA settings, since account and real-world identifiers are almost never shared in RTB auctions.

2.1.1. Web identification

Without account identification, identifying users on the internet can be rather challenging due to the distributed nature of the internet and limitations of the HTML protocol. Since contact with the user is intermediated by internet browsers, OBA players also need to overcome obstacles posed by browser settings and anti-tracking features. Furthermore, unlike devices, browsers do not communicate any fixed IDs to ISSPs. From a technical perspective, Janc and Zalewski[72] distinguish between three methods used to identify internet users: (i) explicitly assigned client-side identifiers; (ii) machine-specific characteristics; and (iii) user-dependent behaviours and preferences.

Explicitly assigned client-side identifiers encompass the storage a unique token on the user's device to identify them in later interactions. The most common forms include HTML cookies, HTML5 local storage and cached objects. Although new methods of identification are gaining on importance, HTML cookies are still the dominant identifier used for web OBA[73].

[72] JANC, Artur and Michal ZALEWSKI. Technical analysis of client identification mechanisms [online]. The Chromium Projects, wiki page [viewed 7 September 2022]. Available from: https://www.chromium.org/Home/chromium-security/client-identification-mechanisms/#explicitly-assigned-client-side-identifiers

[73] ICO. Update report into adtech and real time bidding [online]. 20 June 2019. Available from: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, p. 10.

See also: VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden). Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284

Identification based on **machine-specific characteristics** and **user-dependent behaviours and preferences** (also known as "**fingerprinting**") analyses unique attributes of the user's device and browser (such as the IP address, device and browser settings, time zone, or screen dimensions) as well as user-specific settings (such as the language preferences, mouse gestures, or even the use of tracking-prevention settings and tools[74]).

Attribute	Similarity ratio (All time)	Value
User agent	0.06%	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Safari/605.1.15
Accept	7.86%	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content encoding	94.96%	gzip, deflate, br
Content language	<0.01%	cs-cz
Referer	53.27%	https://amiunique.org/

Illustrative image of a browser fingerprinting analysis[75].

In addition, a new advanced method called **canvas fingerprinting** is starting to gain traction. Through the HTML Canvas feature of HTML5, the website instructs the browser to render an image on the webpage. Due to complexities of the rendering process, the image painted by each device will be slightly different. By comparing nuances of the resulting image, the website can then create a unique identifier for each user.

[74] Janc and Zalewski suggest that by employing privacy measures such as Do Not Track signal or blocking of third-party cookies, users can actually be making themselves more susceptible to fingerprinting. See: JANC, Artur and Michal ZALEWSKI. Technical analysis of client identification mechanisms [online]. The Chromium Projects, wiki page [viewed 7 September 2022]. Available from: https://www.chromium.org/Home/chromium-security/client-identification-mechanisms/#explicitly-assigned-client-side-identifiers

[75] You can test your browser's susceptibility to fingerprinting for free at: https://amiunique.org/

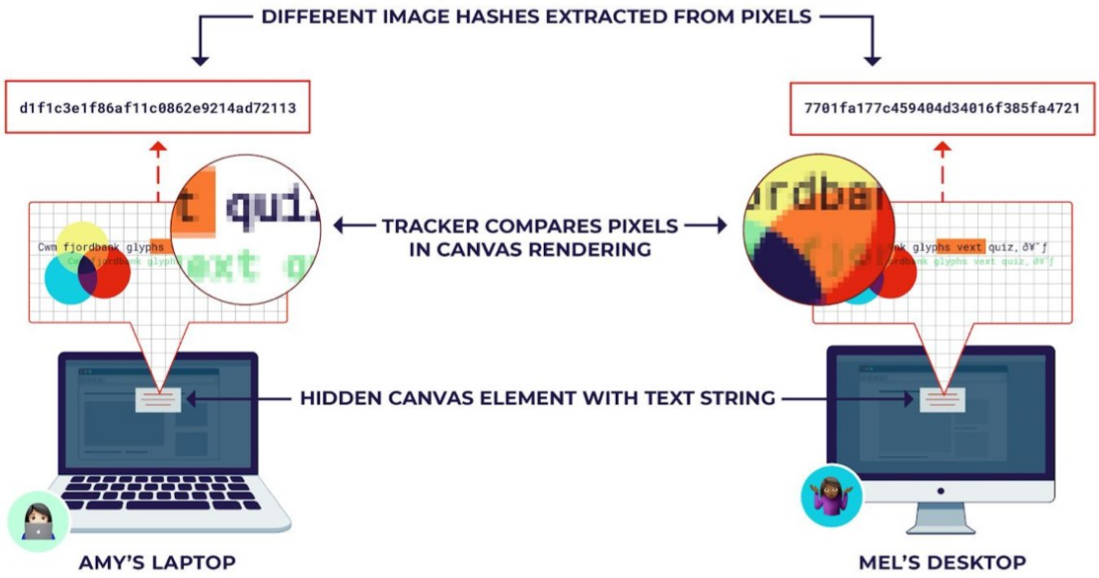


Illustration of the canvas fingerprinting process[76].

While the individual pieces of information (such as the user's language preferences or device model) reveal only little about the user's identity, when combined, they can be used to distinguish between users with surprising effectiveness[77]. Since fingerprinting does not require any data to be stored on the device, it is significantly more difficult to detect and prevent it, although some browsers already provide different extents of fingerprinting protection[78].

2.1.2. Mobile identification

Compared to the web, tracking users via computer programmes and mobile apps is much easier. Since applications run code directly on users' devices, their developers have more freedom to engage in user tracking. SDKs implemented in apps then allow developers to share the collected data with advertising intermediaries. In such case, user control over data sharing

[76] GEBHART, Bennett Cyphers and Gennie, 2021, Behind the one-way mirror: A deep dive into the technology of Corporate Surveillance. *Electronic Frontier Foundation* [online]. 10 February 2021. [viewed 19 December 2022]. Available from: https://www.eff.org/wp/behind-the-one-way-mirror, p. 16

[77] In 2010, the Electronic Frontier Foundation found that out of 470,761 participating users, 83.6% were identifiable based on their browser fingerprint. Although a later study conducted by HAL confirmed only 33.6% success rate, results achieved by current AdTech providers could be significantly higher. For example, FingerprintJS, Inc. claims that their fingerprinting tools can identify users with a 99.5% accuracy. See: ADGUARD. You can hide, but you can't escape: how fingerprinting revolutionized online tracking [online]. AdGuard, 17 August 2022 [viewed 19 December 2022]. Available from: https://adguard.com/en/blog/browser-fingerprinting-gpu.html

[78] HUGHES, Karl. Fingerprinting in the Modern Browser: Are Privacy Updates Making It Harder to Prevent Fraud? [online]. Chicago: Fingerprint, 25 May 2021 [viewed 19 December 2022]. Available from: https://fingerprint.com/blog/browser-fingerprinting-privacy/

may be limited to a "take it or leave it" choice, as it is impossible to grant a permission to the app without granting the same privilege to all the third-party code running inside it[79]. To some extent, in-app tracking may be hindered by privacy controls offered by operating systems that allow users to limit developers' access to certain device features (for example, iOS apps require explicit user permission to access location data[80]). However, disabling such features usually affects the functioning of the app itself.

In mobile advertising, user identification is also largely facilitated by **unique device identifiers** (e.g. an IMEI or MAC address). For example, the MAC address is commonly used to track the device's physical proximity to other devices or wireless beacons set up in locations of interest (such as brick and mortar stores). Thanks to MAC tracking, advertisers can learn that a person has visited their store or associate different devices belonging to the same user. In addition, iOS, Android and Windows mobile operating systems mark each device with a **dedicated advertising ID** to help applications serve targeted ads. Even though all of these ad IDs may be manually turned off, all are enabled by default[81] and are available to all apps without any special permissions[82].

2.2. Cookies

It is without doubt that RTB markets are built around HTML cookies. Even though legislative and technical changes are expected to push out third-party cookies from the web, today, they are still the main method used by AdTech businesses to track users. On the other hand, first-party cookies are likely to remain a key feature of the internet. For this reason, I find it necessary to explore how cookies are used in OBA.

[79] GEBHART, Bennett Cyphers and Gennie, 2021, Behind the one-way mirror: A deep dive into the technology of Corporate Surveillance. *Electronic Frontier Foundation* [online]. 10 February 2021. [viewed 19 December 2022]. Available from: https://www.eff.org/wp/behind-the-one-way-mirror, p. 17

[80] APPLE INC. About privacy and Location Services in iOS and iPadOS [online][viewed 19 December 2022]. Available from: https://support.apple.com/en-us/HT203033#:~:text=You%20can%20turn%20Location%20Services,access%20to%20Location%20Services%20data

[81] Following changes in the iOS 14.5 release, tracking on Apple mobile devices now requires user's prior consent via the App Tracking Transparency framework.

[82] GEBHART, Bennett Cyphers and Gennie, 2021, Behind the one-way mirror: A deep dive into the technology of Corporate Surveillance. *Electronic Frontier Foundation* [online]. 10 February 2021. [viewed 19 December 2022]. Available from: https://www.eff.org/wp/behind-the-one-way-mirror, p. 19

In the early days of online display advertising, advertisers had to overcome a key obstacle for targeted advertising on the internet – the stateless nature of the HTML protocol. Essentially, what this means is that the protocol treats each connection request (e.g. request to load a webpage) independently and does not allow ISSPs to make associations between different requests made within a single browsing session or by a single user[83]. Cookies aim to solve this problem. In other words, they intend to "*give the Web a memory*"[84].

Cookies are small text files that are stored in the browser's memory. When the user attempts to load a website that they previously visited, cookies for that website will be sent to the website's publisher. Cookies may hold any information about the user (such as their language preferences). Since cookies have limited size, it is also common for several cookies on the same website to be replaced by a single multi-purpose cookie. In such case, the cookie only holds the user's unique ID. All other data about the user (that would otherwise be recorded in the cookie) is stored under that ID in the publisher's database and is consulted after that user's identity is established via cookie ID.

Cookies were first introduced in 1994 as a solution for creating a virtual shopping cart that records user-selected items over their shopping session on an e-shop. Since then, they have become a widely used solution wherever ISSPs need their websites to "remember" things about their users. From a technical perspective, cookies are divided into **session cookies** (deleted at the end of each browsing session) and **persistent cookies** (with a pre-set retention period, such as one year). According to the function they serve, the industry also traditionally distinguishes between the following cookie types:

- **technical cookies**, commonly referred to as "**necessary**" or "**essential**" cookies, are mostly session cookies that enable the site to function properly and provide essential features such as an e-shop shopping cart, continuous user login over a browsing session or security functions (e.g. to recognize repeated infringers);

[83] Although the ISSP has the user's IP address, on its own, it is generally not a reliable way of user identification, due to the widespread use of dynamic IP addresses, Virtual Private Networks (VPNs), proxies and Wi-Fi connection.
[84] VEALE, Michael and ZUIDERVEEN BORGESIUS, Frederik, 2022, Adtech and Real-Time Bidding under European Data Protection Law [online]. German Law Journal. 2022. Vol. 23, no. 2p. 226–256. DOI 10.1017/glj.2022.18., p. 4

- **preference cookies** are used to remember user choices such as language and currency preferences or other user-profile settings, or to automatically fill in login username upon repeated visit;
- **analytical** or **performance cookies** provide the ISSP with information about user interactions with their website, such as the number of visits or interactions with content and ads;
- **targeting cookies** (also known as **advertising cookies**[85]) are used to monitor users' online behaviour and to serve them personalized ads.

Another key distinction is between first-party and third-party cookies. The difference is again technical in nature. When the HTML started to support frames as a method for loading website content from multiple sources at once (such as through embedding), web browsers adopted the **Same Origin Policy** as an important security feature[86]. In short, the Same Origin Policy ensures that cookies placed on the user's browser may only be read by the domain from which they originate. **First-party cookies** are those cookies that are set directly by each publisher. They are mostly used to provide essential functions and improve the user experience. However, they are less convenient for OBA, since they don't enable cross-site tracking.

On the other hand, **third-party cookies** are not set by the publisher, but a third-party server used to load some elements of the website that the user is trying to access. In OBA, third-party cookies are mostly set by AdTech intermediaries. Since they do not originate from the publisher's website, the publisher's server cannot read them. Nonetheless, if multiple publishers allow the AdTech provider to set its cookies on their websites, the AdTech provider may get a comprehensive picture of the user's cross-site behaviour.

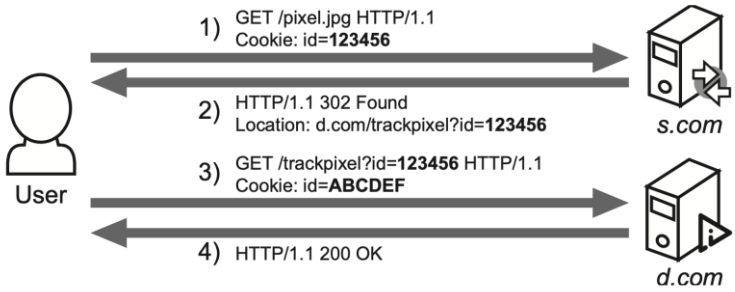
In RTB context, there are two main ways to set cookies. Either the cookie is set when the browser requests the creative or the website incorporates a transparent 1x1 pixel image hosted on the AdTech provider's server (commonly called a **tracking pixel** or a **web beacon**). In both cases, the aim is to make the browser send a request to the AdTech provider's server. Together with the response (e.g. the requested image), the browser downloads the code

[85] However, analytical cookies are also important for OBA, since they are commonly used for counting impressions, tracking conversions, and measuring ad effectiveness.
[86] VEALE, Michael and ZUIDERVEEN BORGESIUS, Frederik, 2022, Adtech and Real-Time Bidding under European Data Protection Law [online]. *German Law Journal*. 2022. Vol. 23, no. 2p. 226–256. DOI 10.1017/glj.2022.18., p. 4

responsible for setting third-party cookies. Another way to trigger these requests is through social media elements, such as Facebook "likes" on publisher websites. When such a social media widget is loaded in the user's browser, the social platform may set or read its cookies.

2.2.1. Cookie syncing

To share cookie data between OBA players, **cookie syncing** (or **cookie matching**) developed as a popular way of overcoming the constraints of the Same Origin Policy[87]. The main goal of cookie syncing is to allow two or more AdTech companies to agree on a mutual identification of the user. Once the user is identified, the companies may then share the data they hold about the user to create a complex user profile spanning across multiple platforms and devices.



cookie-matching table	
DSP ID	DMP ID
123456	ABCDEF

Infographic explaining the process of cookie syncing.[88]

Cookie syncing occurs in the following steps:

1) The browser attempting to load a webpage (e.g. example.com) requests one of the website's elements (e.g. a tracking pixel) from the server of an AdTech intermediary (e.g. a DSP). Upon receiving the "get" request, the intermediary (DSP) assigns a unique ID to the user (e.g. 123456) and places its cookie.

[87] In practice, the vast majority (75%) of all cookie syncing takes place among ad-related domains. See: PAPADOPOULOS, Panagiotis, KOURTELLIS, Nicolas and MARKATOS, Evangelos, 2019, Cookie synchronization: Everything you always wanted to know but were afraid to ask [online]. Proceedings of the 2018 World Wide Web Conference (WWW'19) [viewed 19 December 2022]. DOI 10.1145/3308558.3313542. Available from: https://arxiv.org/abs/1805.10505, p. 10

[88] BASHIR, Muhammad Ahmad, et al. Tracing Information Flows Between Ad Exchanges Using Retargeted Ads [online]. In: Proceedings of the 25th USENIX Security Symposium, 10-12 August 2016, Austin, TX. Austin, Texas: USENIX, August 2016. ISBN 978-1-931971-32-4. Available from: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_bashir.pdf, p. 483

2) Instead of returning the requested 1x1 pixel image, the DSP redirects the browser to retrieve the image from the server of another AdTech intermediary (e.g. a DMP). As an URL parameter of the request, the DSP includes the DSP's ID for that user.

3) Once the DMP receives the second "get" request, it knows that the user visited example.com and that they are listed by the DSP as user 123456. The DMP assigns the user its own ID (e.g. ABCDEF) and both the DMP ID and DSP ID are stored in a cookie matching table.

4) Finally, the DMP sends the requested image and places its own cookie in the user's browser. Optionally, for bi-directional matching, the DMP may repeat step 2) and initiate another redirect back to the DSP server, passing on the DMP ID so that the DSP can also update its cookie matching table.

5) Once the real-time process is completed, the DSP and DMP are free to directly exchange any information they have about the user. Upon the user's repeated visit, the parties apply their collective knowledge about the user's online behaviour to serve them personalized ads.

In the context of RTB auctions, publisher's cookie ID for the user is included in the bid request. Due to the Same Origin Policy, advertisers and intermediaries that have not previously cookie-synced with the publisher will not be able to identify the user at this point[89]. Once the auction is concluded, the winner gets to send their ad markup to the user. In addition to downloading the creative, executing the ad markup initiates an additional "get" request (step 2 *et seq*.) that allows the advertiser and its intermediaries to place their cookies. Therefore, only the winning bidder gets to cookie-sync with the publisher and place its own cookies in the user's browser.

However, this is without prejudice to any cookie-syncing completed preceding the RTB auction. So, if the DMP used by the advertiser's SSP has previously cookie-synced with the publisher for this user, it can relay any knowledge gained to the advertiser to support their

[89] For a comprehensive description of cookie syncing in RTB auctions see: BASHIR, Muhammad Ahmad, and Christo WILSON. Diffusion of User Tracking Data in the Online Advertising Ecosystem. *Proceedings on Privacy Enhancing Technologies* [online]. 2018, 2018(4), 85–103 [viewed 19 December 2022]. ISSN 2299-0984. Available from: doi:10.1515/popets-2018-0033, p. 87

bidding strategy. For example, bid requests in Authorized Buyers contain the user's Google User ID (or the advertiser's ID if the advertiser uses a Google-hosted match table). This means that buyers who have previously served ads to the user through Authorized Buyers and have cookie-synced with Google will recognize the Google User ID and identify the user[90]. In mobile advertising, device advertising IDs offer significant cookie-matching potential since they are used universally in all contexts.

Given their wide reach[91], cookie IDs used by large platforms may also act as common denominators for cookie syncing between other OBA players (unless they are company-specific). For instance, an empirical study conducted by Dr Johnny Ryan has shown how multiple DSPs are able to combine their user profiles through the google_push ID used in Authorized Buyer's cookie matching[92].

According to recent market studies[93], 78% of top websites engage in cookie syncing, giving them the ability to reconstruct up to 73% of a user's browsing history. Within just 30 clicks on search results, there is a 99.5% chance that the user will be tracked by all top 10 trackers[94].

2.3. Self-defence against tracking

From the users' perspective, HTML cookies have one significant advantage – they can be easily managed through browser settings. All leading browsers offer the ability to manage or delete cookies at will. To different extents, browsers further provide enhanced privacy features protecting against more sophisticated forms of online tracking (such as fingerprinting)

[90] For a complex description of Authorized Buyers cookie matching processes see: GOOGLE. Cookie Matching. *Authorized Buyers*. [online] [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/cookie-guide#bidder-initiated:-bidirectional-cookie-matching

[91] According to whotracks.me, Google doubleclick.com cookies used in Authorized Buyers track over 20 % of all internet traffic. See: GHOSTERY GMBH. Doubleclick. *Whotracks.me* [online]. Ghostery GmbH [viewed 19 December 2022] Available from: https://whotracks.me/trackers/doubleclick.html

[92] RYAN, Dr Johnny. *RTB Header Bidder Evidence – Explanatory Document* [online]. Brave Software, Inc., 2 September 2019. [viewed 19 December 2022]. Available from: https://brave.com/static-assets/files/explanatory_note_google_RTB_and_push_pages.pdf

[93] PAPADOPOULOS, Panagiotis, KOURTELLIS, Nicolas and MARKATOS, Evangelos, 2019, Cookie synchronization: Everything you always wanted to know but were afraid to ask [online]. Proceedings of the 2018 World Wide Web Conference (WWW'19) [viewed 19 December 2022]. DOI 10.1145/3308558.3313542. Available from: https://arxiv.org/abs/1805.10505, p. 1

[94] WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049, p. 13

or support privacy plugins (such as the Privacy Badger created by the Electronic Frontier Foundation) that increase resistance to tracking.

To combat browser settings and cookie blocking technologies, some websites engage in **ID respawning**. In addition to HTML cookies, AdTech companies may store copies of the cookie data via other local-storage alternatives (such as HTML5 local storage or browser cache. When the user clears their HTML cookies, the cookies may be automatically re-instated from these alternative sources. As explained above, fingerprinting is another effective weapon against user self-defence strategies.

The risk of cookie respawning practices circumventing user settings is further deepened by the use cookie syncing. For example, if the user deletes their browser cookies for example.com, the website's publisher may consult their cookie matching table to respawn its cookie from third-party IDs that have remained intact. Re-identification of the user by one AdTech company can thus lead to re-identification by all its data partners[95].

Ad blockers are seen as another big threat to the advertising industry. Although these tools generally do not protect from online tracking, they prevent ads from rendering to ensure an uninterrupted user experience. According to market studies, around 37% of internet users worldwide use some form of ad blocking software[96]. Naturally, this causes advertisers to lose a substantial part of their advertising investments.

2.4. Data sharing

Thanks to the rise of digital markets, companies are now hold more data about user behaviour than ever. However, not all companies can rely solely on first-party data. To enrich existing customer profiles and learn more about their target audiences, these companies engage in widespread data sharing. In RTB, Data Management Platforms are regularly engaged as specialized data brokers providing data exchange services. Generally, DMPs provide a combination of the following services; however, instead of outsourcing these activities to

[95] WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049, p. 2

[96] KEPIOS, WE ARE SOCIAL, and HOOTSUITE. *Digital 2022 Global Overview Report* [online]. 2022. [viewed 19 December 2022]. Available from: https://www.hootsuite.com/resources/digital-trends, p. 271

DMPs, companies may as well choose to perform them in-house, within data partnerships established between OBA players (with the results sometimes referred to as second-party data) or between individual entities or departments of large AdTech organisations:

- **data collection** – DMPs can themselves collect user data from public sources (such as by scraping social media, websites, and public registers) or conduct their own market research;
- **data aggregation** – through data partnerships, DMPs acquire data from OBA stakeholders, points-of-sale or other data aggregators (e.g. marketing agencies or credit bureaus) to create comprehensive data pools;
- **data normalization** – by sorting, cleansing, and compiling it, DMPs transform raw data into easy-to-use unified user profiles;
- **intelligence** – some DMPs generate extra value for advertisers by providing them with additional insights inferred from user behaviour (e.g. by identifying common characteristics, grouping users into interest-based audiences or scoring users according to their buying habits[97]);
- **identity resolution** – since DMPs hold data from multiple sources, they are uniquely positioned to assist OBA players with cross-platform and cross-device ID matching; therefore, it is more effective for some advertisers to outsource ID matching to DMPs rather than to maintain their own ID matching tables;
- **data sharing** – DMPs often operate as middlemen between OBA players, providing data storage services and ensuring seamless data exchange in the context of near-instant RTB transactions;
- **de-identification** – to promote user privacy, some DMPs alter the acquired data through privacy-enhancing operations such as anonymization, pseudonymization, generalization, noise-adding, encryption, or hashing;
- **data sale** – DMPs (as well as other OBA players) are also known to directly sell or barter their data sets to other companies within OBA markets.

[97] For example, the infamous Cambridge Analytica used data about Facebook „likes“ to create psychological profiles for over 2 million affected user that were later used for micro-targeting in Trump's presidential campaign. See: HERN, Alex. Cambridge Analytica: how did it turn clicks into votes? [online]. The Guardian, 6 May 2018 [viewed 19 December 2022]. Available from: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

To avoid directly sharing their data while still allowing advertisers to exploit their rich portfolios of first-party data, Google and Meta also came up with a novel way of cross-platform targeting. Google Customer Match and Facebook Custom Audiences allow advertisers to upload their databases of actual customer data. By finding similarities between the uploaded data and their own user profiles, these services offer to display ads to "look-alike" audiences within their advertising networks. Meta even offers to handle the first part of the process. By monitoring the traffic on the advertiser's webpage (e.g. through a tracking pixel), it can learn about the advertiser's preferred audience without the need for any data processing on the advertiser's side.

2.5. Measuring ads

Reliable user tracking is necessary not only for ad targeting, but also to measure the effectiveness of ads already displayed. Currently, the price for most online advertising is determined according to the number of impressions viewed, clicks made or other forms of conversion performed[98]. To collect fees for these user actions, publishers must be able to effectively monitor them. Measurement is also important for **attribution** – knowing the audience's habits helps advertisers efficiently distribute their ad resources across the customer journey from the first sighting of an ad all the way to conversion.

Impression tracking is mostly facilitated by a 1x1 pixel on the webpage that calls to an impression tracking server. Alternatively, an impression can be counted by the publisher when they serve an ad tag and by the advertisers when they serve an ad markup. Clicks are tracked through an URL to which the user is directed when they click on the ad. After counting the click, the tracking page redirects the browser to the destination URL. In both cases tracking server may belong to publisher, advertiser and/or measurement vendor, depending on the circumstances (e.g. whether the publisher's measurement data is available to the advertiser and whether it can be trusted). Conversions are harder to measure since they depend on the advertiser's individual goals (e.g. a purchase on their e-shop). Usually, conversions are measured on the advertiser's side, such as by a tracking pixel on the advertiser's webpage (e.g. the page displayed when the customer is informed about successful subscription or payment).

[98] Although new studies propose using attention as the new metric (taking in to account ad time-in-view and user interaction with the webpage), this pricing model has not yet been widely adopted in practice. Currently, the prevailing pricing models are cost-per-mile (CPM), cost-per-click (CPC) or cost-per-action (CPA).

Ad fraud is a serious threat to OBA. Since ad buying is performed in real time through automated means, there are various ways to fraudulently influence the process to shift the perceived ad effectiveness. According to martech.org[99], 24% of all web traffic are bots used for fraud and theft. This leads to estimated 10 % of worldwide ad traffic being invalid or fraudulent, causing the AdTech industry to lose tens of billions of dollars in worldwide ad spend. Practices used by fraudsters to raise illegitimate profits in OBA markets include displaying invisible ads, advertising on fake websites posing as genuine publishers (so called "**domain spoofing**") or using bot traffic to generate artificial views or clicks. Therefore, reliable measurement is essential for preserving the fairness of RTB transactions.

2.6. Recent developments

Without doubt, in 2022, the AdTech industry currently stands on the verge of significant makeover with no clear way forward. The main reason behind this state of uncertainty is the steady deprecation of third-party cookies, which have for a long time served as the primary method for online user tracking. Indeed, the use of HTML cookies is heavily imprinted in RTB protocols and the ways that OBA stakeholders track users, monitor ad performance and exchange data. Google argues that when third-party cookies are disabled without an adequate substitute, publishers' average revenue from ads drops by more than 50%. While later studies suggest that the impact on publishers may not be so drastic[100], the death of third-party cookies will definitely shake up the industry in a major way. According to Epsilon market research[101], 69 % of US marketers surveyed expect the elimination of third-party cookies to have greater impact than the adoption of GDPR.

Why exactly is the industry moving away from third-party cookies? As OBA players' focus shifts towards user privacy, third-party cookies have been found to be encumbered by inherent flaws that make them difficult to reconcile with the requirements of data protection laws. The technology that was originally developed to equip a website with a shopping cart

[99] VON HOFFMAN, Constantine. A statistical picture of the cost of digital advertising fraud [online]. Third Door Media, Inc., MarTech, 9 May 2022 [viewed 19 December 2022]. Available from: https://martech.org/a-statistical-picture-of-the-cost-of-digital-advertising-fraud/

[100] FOU, Augustine. *Impact of Loss of 3P Cookies on Publishers' Ad Revenue* [online]. Medium, 30 April 2021 [viewed 19 December 2022]. Available from: https://acfou.medium.com/abstract-2fefd374edb2

[101] EPSILON. Preparing for a world without third-party cookies [online]. Epsilon Data Management, LLC, 27 October 2020 [viewed 19 December 2022]. Available from: https://www.epsilon.com/us/insights/resources/research-preparing-for-a-world-without-third-party-cookies

feature is now abused to monitor users across different online contexts without their knowledge and to share data about user behaviour between hundreds of OBA participants without effective controls to prevent data misuse. As elegantly described by the UK ICO, the "*evolution of cookies and their use for targeted advertising is a cautionary tale of the risks of repurposing technology without also building in safeguards to protect against misuse and harm*"[102].

As of 2022, most web browsers – including Safari, Brave, Edge and Firefox – have already disabled third-party cookies by default. Chrome – the dominant browser – is yet to take this step. Although the plans to phase out third-party cookies have been announced as early as 2020, the deadline has been repeatedly postponed as Google struggles to find a suitable alternative. Currently, the end of third-party cookies in Chrome is expected by the end of 2024.

The crumbling of cookie-based identification[103] can also be attributed to the looming shadow of the ePrivacy Regulation, which is expected to rewrite existing rules governing locally stored tracking technologies imposed by the ePrivacy Directive. Although the regulation was originally intended to come in to effect together with GDPR, the final text has not yet been adopted. Nonetheless, the proposal has not been abandoned and after the EU Council's new draft proposed in February 2021[104], the trialogue negotiations are still ongoing. Under Art. 8 (2) of the latest proposed text of ePrivacy Regulation, processing of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment, is generally prohibited subject to limited exceptions such as a GDPR-compliant consent. Given that RTB systems currently rely heavily on information communicated within HTTP requests, if adopted, such ban would be very difficult for the AdTech industry to adhere to.

At the moment, it remains unclear what the replacement for third-party cookies will look like. There is a large number of emerging ID-based solutions that aim to provide a reasonable alternative to cookies. Additionally, Google has launched its Privacy Sandbox initiative in an attempt to find a viable cookie-less solution that would serve as a new standard for privacy-

[102] ICO. *Data protection and privacy expectations for online advertising proposals* [online] 25 November 2021. Available from: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf, p. 20

[103] Pun intended.

[104] COUNCIL OF THE EUROPEAN UNION. Interinstitutional file 2017/0003(COD), Council of the European Union mandate ST 6087 2021 INIT of 10 February 2021, available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

friendly online tracking[105]. It argues that blocking cookies without a suitable alternative would only motivate AdTech companies to turn to workarounds that could be even more intrusive than cookies (such as fingerprinting). Most likely, the shift from third-party cookies will lead to major fragmentation in user identification techniques as AdTech players swich to different cookie substitutes. Nonetheless, large platforms like Google will without doubt play significant role in defining the new standards for cookie-less identification.

Furthermore, major changes have recently been experienced by the mobile advertising industry. With its App Tracking Transparency framework ("**ATT**") released in April 2021, Apple has introduced privacy-enhancing features to its iOS mobile operating system. In addition to providing comprehensive information about how their app collects and processes user data in the app's App Store profile, developers must now ask users for explicit permission to perform tracking[106]. With tracking disabled, developers are unable to access IDFA (the Apple's dedicated advertising ID) and are prohibited from tracking user behaviour through other identifiers (although the second part may be much harder for Apple to enforce).

At the same time, the UK CMA warns[107] that large platforms' focus on privacy-enhancing features may not be motivated as much by a user-centric approach as by a determination to strengthen their market positions. According to the CMA, platforms rich in first-party data have a clear incentive to apply a stricter interpretation of data protection laws that favours their own data-processing systems over data sharing with third parties. For example, Apple's ATT has been heavily criticized by Meta for its alleged chilling effect on ad revenue collected by small businesses dependant on third-party tracking tools for targeted advertising[108]. While the Electronic Frontier Foundation has called Meta's anti-ATT campaign a laughable attempt to preserve its dominance[109], the danger that large platforms could use

[105] GOOGLE. The Privacy Sandbox [online] [viewed 19 December 2022]. Available from: https://privacysandbox.com/intl/en_us/
[106] APPLE INC. If an app asks to track your activity [online] [viewed 19 December 2022]. Available from: https://support.apple.com/en-us/HT212025
[107] UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, para. 5.313 *et seq.*
[108] HA, Anthony. Facebook highlights small businesses as it ramps up Apple criticism [online]. TechCrunch. 16 December 2020. [viewed 19 December 2021]. Available from: https://techcrunch.com/2020/12/16/facebook-apple-small-business/
[109] ARRIETA, Andrés. Facebook's Laughable Campaign Against Apple Is Really Against Users and Small Businesses [online]. 18 December 2020 [viewed 19 December 2022]. Available from: https://www.eff.org/deeplinks/2020/12/facebooks-laughable-campaign-against-apple-really-against-users-and-small

privacy argumentation as a weapon to increase their own market power is hardly exaggerated. With the deprecation of third-party cookies and the growing reliance on first-party data for OBA targeting, the influence of large platforms is likely to increase.

3. Regulating OBA

3.1. Summary of key empirical findings

In previous sections, I have explored the basic concepts of OBA. Most importantly we have seen how ads are delivered to users through complex RTB ecosystems and how user data is processed to enable behavioural targeting. The key findings of the empirical examination can be summarized as follows:

- Programmatic ad-buying methods are on the rise and already account for the majority of all display advertising today.
- RTB is the most complex programmatic method, serving ads through near-real-time auctions with thousands of involved parties.
- User data is a valuable resource that enables publishers to generate more revenue from their inventory and maximizes advertiser return-on-investment.
- RTB is facilitated by different categories of AdTech intermediaries, including supply-side platforms, ad exchanges, demand-side platforms, data management platforms, consent management platforms, content delivery networks and measurement vendors;
- To allow advertisers to make informed choices about their purchase of impressions and enable ad targeting, bid requests containing user data are broadcast within RTB ecosystems;
- To monitor user behaviour for OBA purposes, the advertising industry makes use of a wide variety of tracking technologies. Third-party cookies are the main method for identifying users on the internet, although novel methods (such as device fingerprinting) are on the rise. In mobile advertising, dedicated advertising IDs are mainly used.
- To track user behaviour across different contexts, OBA stakeholders engage in extensive ID matching and data sharing, often relying on services provided by data management platforms.
- The effectiveness of online advertisements is affected by ad fraud and user protective measures, such as browser privacy settings or ad blockers.

- The industry is steadily moving away from third-party cookies as the primary method for OBA tracking without a clear-cut alternative in sight. Recent privacy updates by mobile operating systems have also limited the availability of advertising IDs.

3.2. Right to privacy

Even at first glance, it is already clear that OBA is liable to interfere – at least to some extent – with user privacy. On the constitutional level, Art. 10 (3) of the Charter of Fundamental Rights and Freedoms of the Czech Republic provides that everyone is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data. The right to protection of personal data is also firmly established by Art. 8 of the Charter of Fundamental Rights of the European Union and Art. 8 of the European Convention on Human Rights. The right to informational self-determination is a key element of the broader right to privacy. In its case-law, the Czech Constitutional Court has repeatedly stressed the importance of the right to informational self-determination as a key pre-requisite for personal autonomy and dignified human existence. For example, the Czech Constitutional Court repeatedly cites the German Federal Constitutional Court, stating that "[*u]nless the individual enjoys the guarantee of controlling and checking the content and extent of information and data provided by them to be published, stored or used for other than the original purposes; unless they are provided with the possibility to recognise and assess the credibility of their potential communication partner and adapt their action accordingly, then their rights and freedoms are unavoidably restricted or even suppressed*"[110]. As explained by doc. Sobek[111], the right to privacy can be perceived as the right to possess control over information about own personal matters. Even an intentional and free disclosure of personal information could constitute a loss of control, where the individual may no longer influence how such information will be handled by others.

In OBA, the right to informational self-determination is often contrasted with the economic interests of OBA stakeholders on conducting their business. In Google Spain v Costeja[112], the Court of Justice of the European Union ("**CJEU**") confirmed that interference

[110] Czech Constitutional Court judgment No. Pl. ÚS 24/10 of 22 March 2011.
[111] ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3., p. 42
[112] CJEU judgment in Case C-131/12 of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317, para. 81

with the right to data protection "*cannot be justified by merely the economic interest which the operator of such an engine has in that processing*". It is thus clear that the privacy right is in all cases the default position that may only be overridden, if advertising companies manage to show prevailing legitimate reasons justifying the intrusion and provide safeguards for user privacy. In the EU, the framework stipulating the conditions for such legitimate data processing is provided by GDPR and ePrivacy Directive.

3.3. Applicable law

Based on the empirical findings, I have identified the following laws that are likely to apply to the use of user data for behavioural targeting in connection with the delivery of online behavioural ads in the Czech Republic:

Applicable law	Reason for application
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**").	In OBA, AdTech vendors regularly share user data via bid requests or server-to-server data exchanges. They use this data to create rich user profiles for behavioural targeting purposes. It is likely that at least some of the processed data constitutes personal data, triggering the application of GDPR.[113]
Article 5 (3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ("**ePrivacy Directive**"), implemented without material deviations in	Art. 5 (3) of ePrivacy Directive regulates the storing of and access to information in users' terminal equipment. As was shown, the prevailing methods of user identification used for OBA – HTML cookies and advertising IDs – require AdTech vendors to retrieve data from users' devices.

[113] It is also apparent that OBA data processing is carried out via automated means and does not relate to purely personal or household activity. As the CJEU confirmed in *Lindquist*, the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people cannot be considered a purely personal activity. [CJEU judgment in Case C-101/01 of 6 November 2003, *Göta hovrätt (Sweden)* v *Bodil Lindqvist*, ECLI:EU:C:2003:596, para. 47]

§ 89 (3) of Act No. 127/2005 Coll., Electronic Communications Act.	

Nonetheless, to provide a complete answer as to whether these laws apply to OBA, I must assess in detail the conditions for their applicability and whether they are satisfied in OBA context.

Given the extent and complex nature of data processing occurring in OBA ecosystems, it is not possible for this paper to assess the compliance of OBA with the applicable law in its entirety. Instead, I will be focusing solely on the aspects relevant for answering the outlined research questions.

4. OBA driven by data

4.1. Personal data in OBA

Under GDPR, **personal data** is defined as any *information relating to an identified or identifiable natural person*, that is, a *natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*[114]. It follows that GDPR only applies to data about individuals as opposed to legal entities (such as corporations) or technologies posing as users (such as bots).

As regards the nature and content of the information collected, GDPR does not seem to lay down any limitations[115]. Thus, any information can be personal data if it refers to the identity, characteristics, or behaviour of an individual (the "content" element), is likely to be used to determine or influence the way in which that person is treated (the "purpose" element), evaluated, or otherwise impacted (the "result" element)[116]. Unquestionably, the main reason behind data collection in OBA is to learn about user behaviour and to leverage that information to serve personalized ads. Therefore, in the overwhelming majority of OBA scenarios, all three elements will be present[117] and the user information gathered will constitute personal data, provided that the natural person concerned is **directly or indirectly identifiable**.

[114] Art. 4 (1) GDPR

[115] As early as 2014, CJEU supported the broad interpretation of "personal data" in a case concerning data relating to an applicant for a residence permit contained in the minutes of the relevant administrative office [CJEU judgment in Joined cases C-141/12 and C-372/12 of 17 July 2014, *YS and M, S v Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081]. In *Peter Nowak*, CJEU further confirmed that responses submitted within a professional exam as well as any comments by the examiner also constitute personal data. According to the court, the concept of 'personal data' is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject. [CJEU judgment in Case C-434/16 of 20 December 2017, *Peter Nowak v Data Protection Commissioner (Ireland)*, ECLI:EU:C:2017:994, para. 34]

[116] WP29. *Opinion 4/2007 on the concept of personal data*, 20 June 2007, p. 10

[117] Given the broad definition of personal data, the elements proposed by WP29 are to be understood as alternative rather than cumulative. [*ibid., p. 11*]

4.2. Identifying users

A common misconception is to reduce identification to knowing a person's name. However, this was hardly the intention of EU legislators. In fact, the sole knowledge of someone's name will rarely lead to their reliable identification within the entirety of a country's population, not to say the pool of all internet users. Identification is always context specific – seemingly ancillary pieces of information may enable precise identification if combined with additional information (e.g. an e-mail address combined with the person's age and nationality) or applied in narrowly-defined contexts (e.g. user's unique username on Instagram). By distinguishing between direct and indirect identification, GDPR acknowledges that different identifiers may enable identification with varying accuracy. Hence, identifiability is not limited to the knowledge of dedicated identifiers (such as a name or a passport number) and even *one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity* may serve as indirect identifiers[118]. Simply put, identification must be understood as the ability to recognize an individual and distinguish them from other individuals within a larger dataset, regardless of the identifier or combination of data used.

GDPR recital 30 provides that in digital environments, individuals *may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*. In this way, it is acknowledged that in digital interactions, users manifest themselves through their devices. Therefore, the fact that an identifier is tied to a particular device rather than directly to its user does not generally diminish its usefulness for distinguishing that user. On the internet, even without knowing users' identity in a narrow sense, it is still perfectly possible to recognize, categorize, make inferences about them, or learn about their behaviour[119].

This conclusion is well supported by academics as well as EU courts. For instance, in a case concerning Google's online tracking practices, the question whether a user's internet browsing history tied to a cookie identifier can be considered 'personal data' was assessed by

[118] Art. 4 (1) GDPR.
[119] WP29. *Opinion 4/2007 on the concept of personal data*, 20 June 2007, p. 14

the England and Wales Court of Appeal (Civil Division)[120]. In the proceedings, the plaintiffs claimed that Google violated their privacy by collecting information about their browsing behaviour via cookies without their consent and later using that data for ad targeting within its DoubleClick ad exchange (now Authorized Buyers). Citing the WP29 guidelines as well as the CJEU *Lindquist*[121] judgment, the court held that "*identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the [browser-generated data] does not name the user. The [browser-generated data] singles them out and therefore directly identifies them.*" Rebutting Google's counterargument that users are not identified since one device may be used by multiple users, the court made the following observations: (i) the concept of "multiple users" is, in effect, an outdated one – on average, devices are generally used exclusively by a single individual (smartphones and tablets, to take two examples)[122]; (ii) even if a device has more than one user, by distinguishing between individual browsing sessions and analysing browsing habits, Google is in fact able to differentiate those users. Moreover, CJEU also seems to be on board with the idea of device identifiers as a reliable way to identify individual users. In *Lindquist*, its states that people may be identified "*by other means than their name, for instance* ***by giving their telephone number*** *or information regarding their working conditions and hobbies*" (emphasis added).

In conclusion, unique identifiers used for OBA as well as any user data linked to such identifiers must generally be regarded as personal data if the OBA player is able to connect the identifiers with a particular individual or device. That is especially the case for publishers and advertiser who interact directly with users as they are more likely to associate the identifiers with additional information, such as the data subject's contact data. However, the same logic extends to any AdTech vendor with direct access to the user's device. The term "identifier" must then be understood in a broad sense as including any explicitly assigned client-side identifiers (e.g. cookie IDs, device IDs and advertising IDs), and even probabilistic identifiers such as unique characteristics of the user (e.g. their browsing habits and purchase interests) or

[120] England and Wales Court of Appeal, [2015] EWCA Civ 311 of 27 March 2015, *GOOGLE INC. and Judith Vidal-Hall Robert Hann Marc Bradshaw and the Information Commissioner*, para. 115 *et seq.*

[121] CJEU judgment in Case C-101/01 of 6 November 2003, *Göta hovrätt (Sweden)* v *Bodil Lindqvist*, ECLI:EU:C:2003:596, *Bodil Lindqvist*.

[122] Although the court did not support its reasoning with any empirical findings, the argument seems valid. Where OBA players collect data from millions of devices, they should assume that at least some of those devices are associated with a single user.

their device (e.g. a device fingerprint) if they are sufficiently precise so as to single-out the user[123].

4.2.1. Reasonable identifiability

The situation gets a little more complex when personal data is shared between different parties within RTB ecosystems. As was shown earlier, DMPs often aggregate large pools of user data separated from its original context. When a DMP acquires data from other OBA stakeholders, it usually no longer maintains a direct connection to the user. Since it does not interact directly with the user's browser, it may be unable to associate the processed data with a particular device[124]. Could this mean that the data processed by the DMP is anonymous, and the user no longer identifiable?

GDPR recital 26 explains that "*[to] determine whether a natural person is identifiable, account should be taken of* ***all the means reasonably likely to be used****, such as singling out,* ***either by the controller or by another person*** *to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*." (emphasis added).

Helpful guidance regarding the notion of "means that are reasonably likely to be used" was introduced in *Brayer*[125]. Therein, the CJEU assessed whether an IP address held by a website publisher constitutes personal data. First, it found that in the hands of a publisher, a dynamic IP address does not on its own reveal the user's identity – to identify the user, it would need to be combined with other information, such as the records of assigned IP addresses maintained by the respective internet service provider. Next, the court considered (in line with Recital 26 GDPR) the likelihood that such records could in fact be obtained by the publisher.

[123] According to WP29, unique identifiers such as cookies or device fingerprints *enable data subjects to be "singled out" for the purpose of tracking user behaviour while browsing on different websites and thus qualify as personal data*. See: WP29. *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, 8 December 2011.

[124] For instance, even if the DMP knows what cookie ID has been assigned to a user, it cannot use this knowledge to recognize the user on the web, since the Same Origin Policy will prevent it from reading cookies set by other domains.

[125] CJEU judgment in Case C-582/14 of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

In this regard, it concurred with the Advocate General, that such reasonable likelihood would not exist if acquiring the additional data be "*prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*"[126].

On the facts of the case, the CJEU concluded that it was reasonably likely for the publisher to acquire the additional information held by the data subject's internet service provider. According to the court, "*in the event of cyberattacks legal channels exist so that the* [publisher] *is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.*"[127] It is important to note that in the proceedings, the primary reason given by the publisher for retaining user IP addresses was in fact to enable prosecution of potential "pirates". Therefore, the possibility that the IP address would be used in the context of criminal proceedings was not so remote.

However, even after *Brayer*, the discussion around identifiability is not settled. On the one hand, some DPAs (such as the UK ICO or French CNIL) apply a "risk-based" approach. That is, if – based on the circumstances and the criteria of Recital 26 and *Brayer* – it appears highly unlikely that the data subject could be identified, the data is indeed effectively anonymized. On the other hand, the EDPB (and its predecessor the WP29) adopts a stricter "zero-risk" approach – the data is never fully anonymized unless it is objectively impossible for anyone to re-identify the data subject. According to exhaustive legal research on the concept of identifiability and the different approaches taken by regulatory authorities conducted by prof. Finck and Dr. Ing. Frank Pallas[128], the debate is not yet settled. However, the academics conclude that a risk-based approach aligns better with the *Brayer* ruling and with the rationale of Art. 4 (1) GDPR. Arguably, under a zero-risk approach, the potential for data subject re-identification could never be fully eliminated in light of constant technological developments, which would in effect undermine the concept of anonymization as established under GDPR.

[126] ibid. para. 46
[127] ibid. para. 47
[128] FINCK, Michèle, and Frank PALLAS. They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law* [online]. 2020, 10(1), 11–36 [viewed 18 December 2022]. ISSN 2044-4001. Available from: doi:10.1093/idpl/ipz026

Nonetheless, for the purposes of this research, it is still possible to identify some of the common ideas endorsed by the relevant authorities:

- identifiability must be assessed not only from the perspective of the data controller but also from the perspective of any third party likely to access the data;
- in assessing the likelihood of re-identification, account must be taken to all objective factors, such as the effort required and the available technology;
- the intentions of the data controller towards re-identification are immaterial;
- identifiability encompasses not only the ability to associate records with an individual's name but also to (i) isolate some or all records which identify an individual in the dataset – i.e. to "**single out**" the individual; (ii) **link together** different records relating to an individual; and (iii) **make inferences** about an individual[129]; the purpose of the data processing and its benefits expected by the controller are highly relevant – i.e. if purportedly anonymous data is collected with the view of future re-identification, GDPR will still apply.

4.2.2. Identifiability of users in OBA data processing

However, the question of user identification in OBA is never limited to first-party identifiers. Instead, to successfully deliver targeted ads, OBA players consistently exchange user data and match their IDs. In RTB ecosystems, ID matching is largely facilitated by bid request data. As was demonstrated in previous chapters, bid requests contain various data that could be used to identify users, such as site, app, and device data or user demographics, location, and interests. In addition, DMP services (regardless of whether they are provided by DMPs, other AdTech vendors, or through data partnerships) are used for bid request enrichment and for background data exchange. Thus, the likelihood that users will be identified is significantly expanded. Below, I examine some of the most common scenarios that may arise in RTB[130].

[129] The criteria of singling out, linkability and inference for assessing identifiability were proposed by the WP29 in its guidance on anonymisation. See: WP29, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, p. 11.

[130] Within the discussed scenarios, the term "ID" is used to refer to fixed client-side identifiers such as HTML cookies, device IDs, or dedicated ad IDs as well as other explicitly assigned identifiers such as account identifiers or unique hashes of device fingerprints. However, the term "ID" as used here does not refer to raw data that may potentially be used for identification such as behavioural data or unique user and device characteristics.

<u>Scenario 1</u>: The ID broadcast in a bid request (or otherwise shared) is directly recognizable by the recipient.

Scenario 1 may occur if the shared data is linked to the user through one of these IDs:

- **recipient's own ID** (e.g. a cookie ID set by the AdTech vendor's own domain) – On occasions, SSPs sending bid request may proactively include demand-side IDs from existing ID matching tables (for example, Authorized Buyers automatically retrieves the match data hosted for the relevant Google User ID). Bid request recipients that find their own ID within a bid request (such as if they previously ID-matched with the SSP) will immediately recognize the user and will be able to enrich the bid request with data from its own database.
- **dedicated advertising ID** (e.g. Apple IDFA) – Since ad IDs are universal for all apps, ID matching does not require any additional steps. Although the recipient may not have yet recorded the ad ID for this particular user, once it is collected, they will be able to immediately recognize the user upon next interaction.
- **previously matched third-party ID** – Most bid requests contain the ID assigned to the user by the publisher. As it is transmitted in RTB auctions, other IDs of SSPs, ad exchanges or DSPs may be added to it. Any recipient that has previously ID matched with this one of these IDs will be able to recognize the user.
- **unmatched third-party ID** – Even if the recipient has not previously matched IDs for this user, the advertiser that wins the auction (and its AdTech intermediaries) will be able to ID-match with the bid request sender and set their own cookies. This allows them to measure the ads served and recognize the user in future interactions.

<u>Scenario 1 legal assessment</u>*:*

In all of the above cases, any user data associated with the ID will almost certainly constitute personal data, as it directly identifies the user or the user's device. The associated personal data then "relates to" the user in the sense that it reveals information about them and their online behaviour.

What is more, even one of the device characteristics (such as the user's IP address,) can on its own be a sufficient identifier, where the data controller or a third party disposes with means reasonably likely to be used to identify the data subject. In RTB, the likelihood that the user's IP address could be matched with other data revealing the user's identity is particularly high. Leaving aside fingerprinting options, companies that have previously interacted with the user (mostly publishers and advertisers) will be able to match it with existing user profiles. Thus, even when other IDs are obfuscated, IP address can still be used to connect user data across contexts.

Scenario 2: **Unique data in a bid request (or otherwise shared) may be directly recognizable by the recipient.**

Sometimes, the bid request does not include any explicit IDs – for example, if an Authorized Buyers bid request contains a privacy treatment object, the Google User ID, cookie data obtained through matching, the session ID and device IDs will be redacted. However, the bid request will still contain other site/app data (e.g. URL and content), device data (e.g. device model) or user demographics (age and gender), location (which Google suggests may be fuzzified), and user interests (in Authorized Buyers communicated via publisher verticals). This scenario may also arise when DMPs aggregate user data from multiple sources to create a complex user profile. When such profile is then shared with OBA companies, be it without any explicit identifier, the behavioural or other unique characteristics of the user may suffice to reveal their identity.

Scenario 2 legal assessment:

Depending on the uniqueness of the information shared, the user could be identified through probabilistic methods. In this case, the identifiability of the data subject is largely influenced by statistical and technological considerations. For example, a study from 2008 has shown that 87 % of the US population can be uniquely identified based only on their ZIP code, gender, and date of birth[131]. Device fingerprinting techniques are also increasingly accurate in identifying users. If the data exchange occurs within an RTB auction, there exists a high

[131] SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely [online]. Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper 3., 2000 [viewed 19 December 2022]. Available from: https://dataprivacylab.org/projects/identifiability/paper1.pdf

likelihood that the user's identity will be revealed already with the standard data contained in a bid request without the need for any explicitly assigned IDs, since all leading RTB protocols communicate at least the user's IP address and other device characteristics.

Scenario 3: **Shared data does not allow the recipient to recognize the user; however, it may still be used for identification purposes.**

Although it is rather unlikely to occur within the context of an RTB auction (as explained in Scenarios 1 and 2), this scenario may arise when user data is aggregated by a DMP. In this case, the DMP acquires user data from multiple sources through direct data exchanges. Although this data will generally be linked to an ID assigned by the data provider, the Same Origin Policy will prevent the DMP from recognizing the user when they are again encountered in other contexts. Alternatively, rather than directly sharing their IDs, data providers may encrypt the IDs and only provide their hash.

Scenario 3 legal assessment:

The purpose of the data processing plays an important role in this scenario. Even though many DMPs argue that they are only processing anonymized user data, this will scarcely be the case. In OBA settings, the value of user data is derived from the ability to use this data for user monitoring and ad targeting. In the words of the WP29, "*to argue that individuals are not identifiable, where the purpose of processing is precisely to identify them, would be a sheer contradiction in terms*"[132]. Regardless of whether the DMP itself is able to identify the user, the data will generally still allow for all the functions associated with identifiability – singling out the user, linking their data between datasets and making inferences about them. In the hands of the DMP, the data can only be described as pseudonymous, not anonymous. For example, even if only hashed IDs are shared, when two OBA players use the same hash function to encrypt the same data, the records can still be linked.

In a recent decision, the Belgian DPA[133] found the TC String used in IAB's TCF to constitute "personal data", even though the TC String cookie did not contain any IDs that would directly identify an individual and only recorded binary values denoting the user's consent

[132] WP29. *Opinion 4/2007 on the concept of personal data*, 20 June 2007, p. 16
[133] See the *IAB Ruling*.

granted for individual processing purposes and AdTech vendors. The conclusion was based on two main considerations. Firstly, AdTech vendors engaged in OBA have at their disposal the means to link the TC String to an identifiable individual[134]. From the CMPs perspective, the cookie will always be retrieved together with the user's IP address contained in the same HTTP request. In addition, in Open RTB, the TC String is commonly shared as part of bid request containing additional user data. Secondly, the purpose of the TC String is exactly to single out the data subject in order to communicate its processing preferences[135].

Indeed, it could hardly be argued that the likelihood that the user will be re-identified is fully reduced when it is exactly the potential for future re-identification that gives the data collection in OBA ecosystems its commercial sense. Therefore, such data must also be regarded as personal data.

Scenario 4: The shared data does not allow for the user to be identified due to its generality.

To prevent user identification, OBA players may sometimes only share individual pieces of general information about the user, such as the user's interest in one website or product. For example, Topics[136] – a new targeting method proposed within Google's Privacy Sandbox as an alternative to third-party cookies – determines the user's top interests for the week by studying their browsing history. When the user's browser later requests to load an ad, the only information shared with the advertiser are the user's three random interests from the past three weeks. Other methods do not disclose user data at all, such as targeting based on look-alike audiences.

Scenario 4 legal assessment:

Even if only generic data is shared, the sharing entity cannot automatically assume that the data is not personal data. Even the data cannot by itself identify an individual, attention should be taken to the means that could reasonably be used by other OBA players to connect it

[134] See the *IAB Ruling*, para. 302 *et seq.*
[135] See the *IAB Ruling*, para. 309 *et seq.*
[136] GOEL, Vinay. *Get to know the new Topics API for Privacy Sandbox* [online] Google, Chrome, 25 January 2022 [viewed 19 December 2022]. Available from: https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/

with the person concerned. For example, once topics or look-alike audiences are used to target an ad, the user will then be referred to the advertiser's server, which allows the advertiser to access device and browser data (e.g. IP address), create a device fingerprint and associate the user's behavioural data with that fingerprint, making the user identifiable. Multiple advertisers could then share the acquired data with a DMP to create a comprehensive profile featuring the user's shopping preferences.

Nonetheless, the likelihood of re-identification must always be assessed on a case-by-case basis, considering its statistical probability, the technological tools available, and the uniqueness of the data shared. If we adopt the risk-based approach to identification, it is thus conceivable that once traditional identifiers such as HTML cookies are phased-out and browsers implement enhanced protection against fingerprinting techniques, such re-identification may not be possible. At the moment, however, these tracking technologies are still available and even generic data should thus be treated as personal data, if it is used for OBA targeting.

Scenario 5: **Processing of anonymized data for analytical purposes**.

Occasionally, OBA players only process general or high-level aggregated data, such as when they measure website traffic or engage in market research.

Scenario 5 legal assessment:

Usually, where high-level aggregated data is used in OBA, it is still collected from identifiable individuals, and it is only after the data is aggregated and de-identified that it may cease to be personal data. Therefore, data anonymization should always be conducted in compliance with the high standard required by GDPR[137]. If the relevant guidance is followed, the data will be effectively anonymized (although this will cause it to partially loose its value for OBA purposes).

[137] For example, helpful guidance on anonymization can be found in the WP29, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, or ICO. *Anonymisation, pseudonymisation and privacy enhancing technologies guidance* [online] ICO, 7 September 2022 [viewed 19 December 2022]. Available from: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/

In conclusion, given the inherent focus of OBA on audience monitoring and behavioural ad targeting, all data broadcasted in RTB bid requests as well as any data collected in the course of providing DMP services must be regarded as personal data, unless the likelihood that the user will be identified by companies within the RTB ecosystem is virtually non-existent.

4.3. Sensitive data

To protect individuals' sensitive data, GDPR creates a special regulatory regime for so-called "special categories of personal data" – that is, data *revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*[138]. Such sensitive data may only be processed on an additional stricter legal basis prescribed by Art. 9 GDPR in addition to the legal basis under Art. 6 GDPR. As the CJEU confirmed in *OT v Chief Official Ethics Commission Lithuania*[139], in addition to inherently sensitive data, Art. 9 GDPR also applies to data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing. This was also confirmed in the Norwegian DPA's fine to Grindr. Therein, the DPA found that information that a data subject is a user of the gay dating app is data concerning the data subject's sexual orientation[140].

Other than the explicit user consent required by Art. 9 (2) (a) GDPR, the legal basis under Art. 9 (2) (e) GDPR could potentially be available in OBA context. Art. 9 (2) (e) GDPR allows the processing of sensitive data on the basis that it was manifestly made public by the data subject. Nonetheless, as explained by the EDPB[141], the word "manifestly" implies a high threshold for the application of the exemption. Therefore, even if the information has been published within an app or a social network, its nature as a special category of data cannot be automatically dismissed and account must be taken of the settings of that app regarding the publishing and access to such information.

[138] Art. 9 GDPR.
[139] CJEU judgment in Case C-184/20 of 1 August 2022, *OT v Chief Official Ethics Commission Lithuania*, para. 123.
[140] Datatilsynet decision no. 20/02136-18 of 13. December 2021.
[141] EDPB. *Guidelines 8/2020 on the targeting of social media users*, 13 April 2021, version 2.0, para. 120 *et seq*.

Contrary to consumer's common understanding, the presence of special categories of data in RTB is hardly an exception. For example, the following topics were distinguished within Authorized Buyers publisher verticals or IAB content taxonomies signifying users' purchase interests[142]:

gay life, incest/abuse support, substance abuse, smoking cessation, cancer, depression, right-wing politics, STDs, eating disorders, work & labour issues, poverty & hunger, discrimination.

Yes, these are actual interest categories shared in Authorized Buyers and OpenRTB ecosystems that advertisers may bid on to target their ads.

4.4. Device data in OBA data processing

As opposed to GDPR, which provides a general legal framework for the use of personal data, the regulation that governs the processing of terminal equipment data is much more specific. In fact, Art. 5 (3) ePrivacy Directive only prescribes that *the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller*.

First, ePrivacy Directive applies to both user and subscriber data, where "subscriber" is defined as *any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services*[143]. As opposed to GDPR, the ePrivacy Directive thus applies also to data of legal entities. Second, Art. 5 (3) is technologically neutral and applies to any **storing** and/or **gaining access to** data stored in the user's terminal device through electronic communications networks. In OBA context, "terminal equipment" denotes a user's connected device, such as a computer, tablet, or cell phone. The "electronic communications network" facilitating the transmission is

[142] Authorized Buyers and IAB taxonomies highlighted by Brave privacy advocates are available at: https://brave.com/rtb-evidence/ [viewed 19 December 2022].
[143] Art. 2 (k) of Directive 2002/21/EC.

usually the internet; however, EDPS[144] considers apps that access device data to also fall within the definition, even if the data is not transmitted outside that device[145]. Third, the regime applies to "any information", not only personal data. This is of course without prejudice to the potential simultaneous application of ePrivacy Directive and GDPR[146].

Consequently, it is undisputable that Art. 5 (3) applies to all locally stored identifiers, including cookies, device IDs and advertising IDs as well as any unique device characteristics used for fingerprinting[147]. On the other hand, it does not apply to the use of identifiers independent of the device, such as account identifiers (e.g. a username or e-mail). It must be noted that from the words "*the use of electronic communications to gain access to information stored in the terminal equipment*", it appears that Art. 5 (3) applies only to the act of directly extracting the data from the user's device and does not cover the subsequent use or sharing of the information[148]. As explained by the EDPB, this also includes the gaining of access to information automatically transmitted by the browser within a HTTP request header when the browser requests to load a webpage (or executes an ad tag or ad markup)[149]. However, the rules do not seem to extend to further transmission of such information by the retrieving entity. This means that while fingerprinting based on information from a received HTTP request and canvas fingerprinting (that requires running code directly on the device) falls within the scope, fingerprints based solely on data obtained from another AdTech intermediary without a direct contact with the user – such as the data obtained from a bid request – are excluded from the scope.

[144] EDPS. Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, November 2016., para. 17
[145] For instance, if an app seeks to access the device's advertising ID or location,
[146] EDPB. *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, 12 March 2019.
[147] WP29. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*, 25 November 2014. and WP29. Opinion 04/2012 on Cookie Consent Exemption, 7 June 2012.
[148] This interpretation is also consistent with Recital 24 ePrivacy Directive, which provides that „*Terminal equipment* […] *and any information stored on such equipment are part of the private sphere of the users requiring protection*". The rationale behind Article 5 (3) thus lies not in the protection of information due to its special nature, but in the protection of the device as the user's private sphere.
[149] WP29. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*, 25 November 2014.

5. Responsibility for data protection compliance

While identifying the entity responsible for compliance with Article 5 (3) ePrivacy Directive is fairly straightforward, applying GDPR to the complex RTB ecosystems requires a more in-depth analysis. In terms of responsibility for data processing, GDPR distinguishes between a **data controller** and a **data processor**.

Controller is the person primarily responsible for the data processing and for demonstrating compliance with GDPR[150]. Controller decides on the "why" and "how" of the data processing. Processor is then simply the entity that carries out the processing on behalf of a controller without determining its purposes or means[151]. A processor may carry out processing only on instructions from the controller and cannot process the data for its own purposes[152]. Whether an entity acts as a controller or processor must always be determined *in concreto*, according to the actual activities performed by each entity. The formal designation of an actor as a "controller" or "processor" (e.g. in a contract), though it may be helpful, cannot be considered a decisive factor[153]. Based on such factual analysis, an entity[154] will be considered a controller if it *determines the purposes and means of the processing of personal data*[155].

The requirement of "determination" assumes that the controller exercises a certain level of control over the processing activities. In the CJEU's case-law and authority guidance, the following clarifications have been provided:

- the fact that an entity does not itself have access to the personal data processed does not prevent it from being a data controller[156];
- the exercised control does not need to be carried out by way of written guidelines or instructions; it is enough that the entity exerts influence over the processing for its own purposes[157];

[150] In Art. 5 (2) GDPR described as the principle of „accountability".
[151] Art. 4 (8) GDPR.
[152] Art. 28 (3) (a) GDPR.
[153] EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 July 2021, version 2.0, para. 12.
[154] That is, any natural or legal person, public authority, agency or other body.
[155] Art. 4 (7) GDPR.
[156] CJEU judgment in Case C-210/16 of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, para. 38
[157] CJEU judgment in Case C-25/17 of 10 July 2018, *Jehovah's Witnesses Community*, para. 67 and 68

- for example, as CJEU pointed out in *Jehovah's Witnesses*[158], such influence may take the form of encouragement, organisation, or coordination of the processing activity;
- according to the EDPB, another way a controller may apply its influence without directly processing data is by adjusting the parameters of a service provided by a data processor in such a way that it influences how personal data shall be processed[159];
- the fact that the entity's intervention plays a decisive role in the overall data processing or that it is liable to affect significantly and additionally the data subject's fundamental rights to privacy makes it more likely to be a controller[160].

While the purposes of the processing are always determined by the data controller, when processing activities are outsourced to a data processor, the controller inevitably loses some control over the means of the processing. However, as long as the processor's decision-making discretion remains only ancillary, it will not affect its position under GDPR. In this regard, EDPB proposes to distinguish between essential and non-essential means of processing:

- **essential means** determine whether the processing is lawful, necessary and proportionate and include aspects such as the categories of data subjects, types of data processed, processing duration, and categories of recipients[161];
- **non-essential means** concern mostly practical aspects such as the specific hardware and software used to process the data, or the security measures applied.

5.1. Providers of standardized software as data processors

In digital environments, platforms often allow their business users to exploit their ready-made software tools for personal data processing. Through user settings offered within those tools, business users may then also influence the data processing. In line with the judgment in *Wirtschaftsakademie*, the EDPB recognizes that "*the use of an existing technical system does not exclude joint controllership when users of the system can decide on the processing of*

[158] CJEU judgment in Case C-25/17 of 10 July 2018, Jehovah's Witnesses Community, ECLI:EU:C:2018:551, para. 73
[159] EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 July 2021, version 2.0, para. 45
[160] CJEU judgment in Case C-131/12 of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317, para. 36 and 38
[161] Essential means are mainly those that determine whether the processing is lawful, necessary and proportionate.

personal data to be performed in this context"[162]. From the provider's perspective, even if the way in which the tools are designed pre-determines to some extent the conditions of the data processing, the provider may still preserve its role as the data processor, provided that "*the final decision to actively approve the way the processing is carried out, at least insofar as concerns the essential means of the processing*" is still left to the controller[163]. However, the line between sole and joint controllership may sometimes be rather blurry. On the one hand, the EDPB provides that a cloud storage provider who offers completely standardized services on a "take it or leave it" basis will be considered a processor[164]. Although the service's parameters are pre-defined, the controller still has the final say. On the other hand, in both *Wirtschaftsakademie* and *Fashion ID*, CJEU held that in providing access to its platform, Facebook was acting as a joint controller.

Although neither EDPB nor CJEU provide any further guidance on this issue, it seems the following criteria could be considered when analysing on a case-by-case basis the controller-processor paradigm:

- **provider's own purposes** – whether the provider derives any benefits from the processing beyond merely being paid for services rendered;
- **specificity** – whether the service allows for different types of data processing pursued by the controller or whether it is tailored to perform specific pre-determined processing operations;
- **approval procedure** – whether decisions on all essential means of processing and changes thereto require the controller's prior approval;
- **user controls** – whether the controller is provided with settings that affect the functioning of the service (e.g. to turn on/off certain features, choose data categories, etc.);
- **settings limitations** – whether settings and controls offered to the controller within the service in any way limit their decision-making over the essential means of the processing;

[162] EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 July 2021, version 2.0, para. 65
[163] *ibid*., para. 84
[164] *ibid.*, para. 30

- **bargaining power** – especially in digital advertising where large platforms control a substantial part of the market, it may be relevant whether the service provider is in a position to unilaterally impose terms on controllers due to its commercial power.

5.2. Joint controllership

If multiple data controllers *de facto* together determine both the purposes and the means of the data processing, they are referred to as **joint controllers**[165]. Joint controllers may decide on the purposes and means of the processing together through a **common decision** or alone through individual **converging decisions**. According to the EDPB's interpretation of the CJEU case law, joint controllers determine the conditions of data processing through converging decisions if "*the processing would not be possible without both parties' participation* […] *in the sense that the processing by each party is inseparable, i.e. inextricably linked*"[166].

However, processing activities are often complex and occur in sequences and combinations – a set of operations with a common purpose may as well be perceived as several disconnected processing operations, each with its own narrowly-defined purpose[167]. As explained in *Jehovah's Witnesses*, joint responsibility does not necessarily imply equal responsibility and operators may be involved at different stages and to different degrees[168]. Since an entity may only act as a controller in respect of data processing operations for which it determines the purposes and means, it cannot be considered a joint controller for operations that precede or are subsequent in the overall chain of the processing and which it cannot itself influence[169]. In other words, within an overarching macro-level data processing operation, an entity can only serve as a data controller for those its parts (or the individual micro-level operations from which it is comprised), for which it determines the processing purposes and means.

Joint controllership has been repeatedly addressed in prior case-law. In *Wirtschaftsakademie*, CJEU found Facebook (now Meta) and an administrator of a fan page on

[165] Art. 26 (1) GDPR.
[166] EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 July 2021, version 2.0, para. 55
[167] *ibid*., para. 43
[168] CJEU judgment in Case C-25/17 of 10 July 2018, *Jehovah's Witnesses Community*, EU:C:2018:551, para. 66
[169] CJEU judgment in Case C-40/17 of 29 July 2019, *Fashion ID*, ECLI:EU:C:2019:629, para. 74

Facebook to be joint controllers in relation to the monitoring of page traffic through cookies to generate anonymized statistics about page visitors. While in this case, all data processing was carried out by Facebook, the fan page administrator's contribution consisted in the creation of a specific fan page (targeted at a particular audience) and by adjusting parameters of the required statistics through filters made available to it by Facebook[170].

Another case – *Fashion ID* – concerned a website operator (publisher) who embedded in its website a social plugin (Facebook "like" button) by Facebook (now Meta). When loading the publisher's website, the plugin caused the user's browser to download the plugin from Facebook's servers, allowing Facebook to place its cookie on the user's device and learn that the user has visited the publisher's website. CJEU found Facebook and the publisher to be joint controllers in relation to the collection and transmission of user data to Facebook. However, CJEU also noted that once the data was transmitted, the publisher was not responsible for any subsequent processing carried out by Facebook[171]. The division of responsibilities between joint controllers applies also to the collection of consent. As with other duties under GDPR, each controller collects consent "*only with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means*"[172].

Another recently decided case of joint controllership concerned the TCF's creator IAB Europe. The Belgian DPA assessed whether IAB Europe acts as a data controller in relation to RTB exchanges within OpenRTB when it drafts TCF policies and technical standards. Even though IAB Europe does not itself engage in data processing within OpenRTB (nor does it develop the OpenRTB protocol), the Belgian DPA found it to be a joint controller. According to the DPA, IAB Europe influences TC String processing in the following ways: (i) it stipulates a mandatory list of predefined processing purposes that OpenRTB participants must adhere to[173]; (ii) it defines how CMPs can collect consent from users and generate a TC String; (iii) it designs mandatory specifications of the CMP API through which AdTech vendors access a TC

[170] CJEU judgment in Case C-210/16 of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, para. 36
[171] CJEU judgment in Case C-40/17 of 29 July 2019, *Fashion ID*, ECLI:EU:C:2019:629, para. 76
[172] *ibid*., para. 106
[173] See the *IAB Ruling*, para. 337

String; (iv) by managing the Global Vendor List ("**GVL**") it limits the availability of data processors; and (v) it sets criteria for retention periods[174].

In my view, the decision is encumbered by one major flaw. The DPA failed to consider whether IAB Europe's pre-determination of the conditions of the TCF data processing could be viewed as later approved by data controllers in accordance with the argument proposed by the EDPB in the case of a cloud provider (discussed above). Indeed, it could be argued that rather than itself determining the processing purposes, IAB Europe merely compiled the common purposes already pursued in RTB ecosystems. Given that RTB communications all conform to similar standards, it does not seem impossible for them to follow the same processing patterns or pursue similar purposes. Instead of IAB Europe "limiting the number of available vendors", GVL could be seen as an expression of will by publishers to only transact with certified vendors. However, IAB Europe's exceptional position on the digital advertising market and its significant bargaining power could also be seen as a decisive factor. If it would be shown that decisions on the purposes and essential means of the processing are in effect imposed on OBA players, it would likely justify IAB Europe's position as a data controller exerting a decisive influence over particular questions defining the terms of the data processing.

Upon IAB Europe's appeal against the decision, a preliminary question has now been referred to the CJEU. Should CJEU side with the DPA, the judgment could mean nothing short of a revolution for the AdTech industry. Although the decision is not entirely flawless, CJEU's prior judgments (especially *Jehovah's Witnesses*) hint that the CJEU might support the broad interpretation of the concept of controller as applied by the Belgian DPA.

5.3. Responsibility of parties in RTB ecosystems

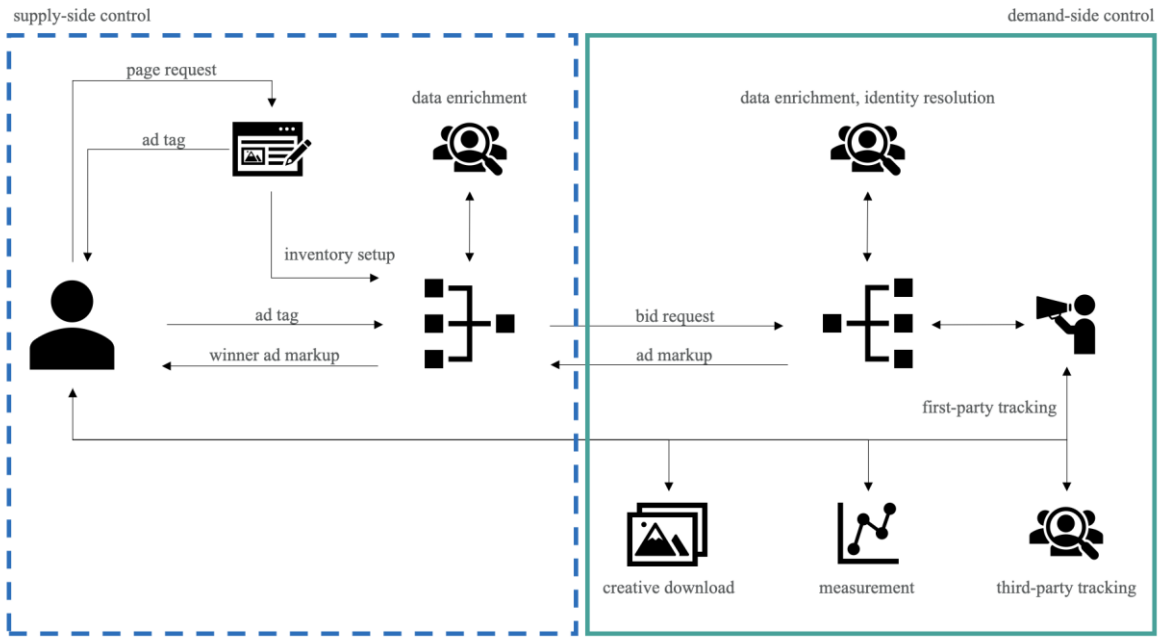
In RTB, the whole process of delivering personalized advertisements from the user's request to load a webpage to the measurement of conversions is complex and comprises of many individual processing operations performed by different parties and AdTech vendors. In view of the law presented in the previous section, it is not possible to determine with finality the roles of different OBA players in the abstract without performing a case-by-case assessment taking into account all the relevant factors and circumstances. However, it may still be possible

[174] See the *IAB Ruling*, para. 360

to highlight some common roles in which OBA players usually appear in relation to RTB data processing.

5.3.1. Publishers and advertisers

Although the processing by publishers and advertisers ultimately advances the same purpose – to deliver a targeted ad to the user – the process occurs in separate phases, whereas each side only influences the means of the processing occurring within the phase in which it is involved. In this regard, it is necessary to distinguish the acts of (i) bid request transmission; and (ii) bid request reception and ad markup delivery. Under Art. 26 GDPR, parties are only considered joint controllers if they determine the purposes and means of the data processing jointly (either through common or converging decisions), not consecutively. In an RTB auction, each side operates within its own sphere of disposition without the ability to determine the processing of data by the other side. In this regard, the process of an RTB auction is different from the situation in *Fashion ID*. In *Fashion ID*, the publisher enabled the data collection by embedding Facebook's code into its website – thus, the means of the data collection and transmission were determined jointly by Facebook (code provision) and the publisher (code implementation). However, in RTB, the publisher generally retains full control over the data transmission (within the boundaries of the selected RTB protocol) as the first contact between the user's browser and the demand side is usually mediated by an SSP or publisher's ad server.



Infographic describing the spheres of control of publishers and advertisers.

Publishers make displaying ads possible by incorporating the necessary code into their websites or apps. In this way, their intervention is indispensable for RTB to take place. They are responsible for the first part of the RTB process – the technical steps that enable the collection of user data and its transmission to the demand side[175]. Publishers pick their SSP and (alone or jointly with supply-side AdTech vendors) define the category of data subjects concerned by tailoring their site to a specific audience, select the ad delivery method and RTB protocol to be used, set the parameters of a bid request and the requirements for a winning bid, provide additional targeting data (e.g. verticals or IDs), and designate the ad exchanges, DSPs or other bid request recipients. Although advertisers express their targeting preferences and by this also narrow down the category of data subjects involved, this reflects merely their preference and cannot, in my view, be construed as a decision on the essential means of the data processing. In reality, the data subjects, the contents of a bid request as well as its recipients are selected exclusively by the publisher and supply-side AdTech vendors (although advertiser preferences affect how impression offers will be distributed).

While publishers control how a bid request is transmitted, after it is received by advertisers, publishers can no longer control the data processing. This conclusion is supported by *Fashion ID*. Therein, the CJEU found that the publisher did not act jointly with Facebook in relation to data processing occurring after the user was redirected to Facebook's servers through a social plugin[176]. In the same manner, I believe that a publisher cannot be held responsible for data processing by advertisers after they receive a bid request. Thus, in the default state, publishers are only liable for the data disclosure related to the targeting of the auctioned impression. Of course, the question must always be assessed on a case-by-case basis as the conclusions will differ according to the ad delivery methods used. For example, joint controllership is more likely to be found in social media advertising, where all the targeting tools are provided by the platform provider, as opposed to open RTB auctions, where targeting is enabled by independent demand-side AdTech intermediaries.

[175] In its opinion on OBA, WP29 notes that „publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their web sites. This is because the publishers facilitate such transfer and co-determine the purposes for which it is carried out, i.e. to serve visitors with tailored adverting." [Working Party 29, WP 171, Opinion 2/2010 on online behavioural advertising, p. 11]

[176] CJEU judgment in Case C-40/17 of 29 July 2019, *Fashion ID*, ECLI:EU:C:2019:629, para. 76

Nonetheless, in providing advertisers with unique user identifiers, publishers anticipate that user's identity may be revealed, and that bid request data may be combined with third-party data. By setting the criteria for a winning bid, they also decide which recipient gets to match IDs following the auction. Therefore, if publishers specifically provide advertisers with additional information to facilitate ID-matching, they may also be considered independently or jointly liable for cross-platform monitoring of user behaviour, as it mostly cannot be assumed that any user identification performed will be limited to the impression auctioned[177]. The EDPB also suggest that ID-matching entails joint controllership of the involved parties[178].

Naturally, if publishers set up their SSP tools so that, after the ad is delivered, subsequent calls to third parties are made for measurement or tracking purposes, they will also be responsible for such data processing.

Advertisers – as independent controllers – are liable for the reception of bid request data and its subsequent processing to evaluate the bid request. They determine the extent, to which bid request data is further processed and combined with additional data to reveal the data subject's identity and learn about their online behaviour for targeting purposes. For some of these operations, such as identity resolution and data enrichment, advertisers employ DMPs or other AdTech intermediaries. Advertisers also determine the contents of the ad markup, including any third-party calls to CDNs, trackers or measurement vendors.

Depending on the circumstances, measurement can be carried out by publishers and advertisers jointly, concurrently or through controller-to-controller data sharing. Finally, both advertisers and publishers are individually responsible for any precedent or subsequent processing of user data, such as the gathering of behavioural data to create user profiles for advertising, data sharing outside RTB auctions and traffic analytics on their websites.

Since the publisher is the only party within the RTB process that interacts directly with the user, it is uniquely positioned to collect any consents necessary for the processing to be lawful and to comply with any transparency obligations. In practice, the required consents are mostly collected by the publisher's CMP on behalf of both the publisher and the advertisers.

[177] In my view, the provision of user identifiers within a bid request necessarily implies that targeting will be based on third-party data in addition to the data contained in a bid request.
[178] EDPB. *Guidelines 8/2020 on the targeting of social media users*, 13 April 2021, version 2.0, para. 56 *et seq.*

Advertiser's generally do not seek to collect any additional consent for their OBA processing. However, it is often overlooked that the publisher and the advertiser are each responsible for different phases of the RTB auction and carry out different processing operations. Each must therefore ensure a valid legal basis for the processing that takes place under its control. While a publisher must ensure the lawfulness of the transmission of the personal data to its recipients (including identifiers shared to enable ID-matching), the advertiser is responsible for any subsequent processing such as the sharing of bid request data with its vendors, combining it with own or third-party data and any further data collection via redirects enabled by the ad markup. Therefore, the legal bases that must be acquired be the involved parties do not necessarily need to fully overlap. It may be the case that the legal basis acquired by the publisher only covers the purpose of targeting of the auctioned impression based on bid request data, without justifying the purposes of ongoing profiling based on third-party data.

Of course, the determination of the parties' roles must always be assessed on a case-by-case basis and depends largely on the tracking and ad delivery methods used. For example, joint controllership is generally more likely to be found on social networks, where platforms directly provide targeting tools, as opposed to open RTB auctions[179].

5.3.2. AdTech vendors

The extent to which AdTech vendors (intermediaries) may be considered joint controllers in respect of RTB data processing largely depends on how the tools they offer are designed. Generally, all AdTech vendors, in developing their tools, make decisions that influence how OBA players may process user data. However, in my view, it must always be distinguished whether they are themselves independently or jointly capable of determining the purposes and means of the processing or whether they are merely making available ready-made data processing tools, whereas the final decision-making power stays with the data controller. Overlooking this distinction would lead to the illogical conclusion that any technology provider, by designing its technology in a certain way or providing its client with only a limited number of data processing controls, assumes the responsibility of a data controller. In this sense, the responsibility of the data controller to only use GDPR-compliant solutions cannot be underestimated.

[179] In its guidance on targeting on social media, EDPB recognized that, in most scenarios, the social network and the targeter are joint controllers. On the other hand, WP29's guidelines on online behavioural advertising

When applying this to **Supply Side Platforms**, the level of independence granted to the SSP within its contractual relationship with publishers must be taken into account. For example, if, after the publisher integrates the SSP's ad tag in its website, the SSP is then free to choose the bid request recipients and the RTB protocol used, it is likely to be considered a controller. On the other hand, if the conditions of the data processing are clearly defined in advance and cannot be altered without the publisher's approval, the SSP can operate as a data processor. The controls offered to publishers are also highly relevant. For example, SSPs may allow publishers to choose which ad networks will be involved, whether some bid request objects will be restricted (e.g. whether user IDs will be provided), or whether additional operations such as data enrichment or identity resolutions should be applied.

The position of **Demand Side Platforms** is similar to that of SSPs. However, in relation to ad delivery, their influence on the processing means is more limited since they generally act as bid request data recipients rather than transmitters. However, they may still exert decisive power over the data processing, especially if they offer highly automated targeting methods such as look-alike audiences.

In OBA, users often consent to data processing through **Consent Management Platform** tools. The available CMP tools differ on how consent is requested, for what purposes, and to which data controllers. Due to their influence on these decisions, CMPs are now increasingly being categorized as data controllers. For example, in the *IAB* ruling, the Belgian DPA considered CMPs' role in TC String processing[180]. Noting that under TCF policies, CMPs are bound to offer by default all TCF-registered AdTech vendors in their interface, it concluded that CMPs may be data controllers if they deviate from TCF policies, such as by imposing pre-selected AdTech vendors on publishers or by denying them the possibility of deviating from the full list of AdTech vendors by default. On the other hand, if CMPs determine the list of recipients in accordance with the publishers' instructions, they act as data processors.

However, the Belgian DPA did not fully consider whether the act undertaken by a publisher consisting in the selection of a particular CMP could be seen as the publisher's instruction to process the data on the terms pre-determined by that CMP. In my view, the fact

[180] See the *IAB Ruling*, para. 372 *et seq*.

that a CMP selects the data recipients for which consent is requested cannot by itself deprive the CMP of its position as a data processer as long as all design choices made by the CMP (and any changes thereto) are clearly laid out in advance and remain subject to the publishers' final approval exercised by the selection of that particular CMP.

Arguably, CMPs are also more likely to be data controllers if they perform additional processing activities, such as incorporating their own trackers, scanning the trackers in use to automatically generate purpose and vendor lists, when they include third-party vendors by default, or if they apply manipulative design strategies in consent pop-ups[181]. Although these arguments are convincing, the responsibility of publishers cannot be left unnoticed. As long as there are enough competing CMP solutions to choose from, publishers are ultimately at fault if they opt for a non-compliant CMP solution or if they fail to make use of provided controls by sticking to the default settings.

It must be pointed out that the above considerations apply only if AdTech vendors act as supply-side or demand-side agents. However, if they process personal data for their own purposes, they must always be considered data controllers. As a result, **Data Management Platforms** operate almost exclusively as data controllers.

Finally, market power is an important factor. Although in theory, businesses are free to choose the AdTech tools they use, in reality, large platforms such as Google or Meta dominate the AdTech market. Thus, to be able to effectively compete on the market, business may be practically forced by commercial reasons to contract with these large platforms to be able to meaningfully advance their economic goals. It is questionable whether in such case data controllers can still be seen as "approving" the pre-determined data processing terms if they are not presented with other commercially viable solutions and thus cannot really influence how data will be processed.

[181] The role of CMPs in OBA data processing has been analysed in detail in SANTOS, Cristiana, et al. Consent Management Platforms Under the GDPR: Processors and/or Controllers? *SSRN Electronic Journal* [online]. 2021 [viewed 18 December 2022]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4205933.

6. Lawfulness of OBA

The most important obligation of OBA participants under both the ePrivacy framework and GDPR is to ensure the lawfulness of data processing. In line with GDPR, personal data may only be processed under one of the legal bases offered by Art. 6 GDPR. In the context of OBA, the following legal bases could potentially apply[182]:

- Art. 6 (1) a) – the data subject's **specific and informed consent**;
- Art. 6 (1) b) – the **performance of a contract** to which the data subject is party; or
- Art. 6 (1) f) – the **legitimate interests pursued by the controller** or by a third party unless they are overridden by the interests or fundamental rights and freedoms of the data subject.

To be considered lawful, processing must fall under one of these legal bases. Generally, more legal bases cannot be used simultaneously to justify the same processing activity. For example, if the controller processes data on the basis of a freely given consent, they should not continue to process the data after consent is withdrawn, claiming that the processing is also justified by contract performance. As the WP29 explains, "*Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals*" and "*Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is*."[183] However, it may be possible to alternate legal bases for processing of the same personal data for different purposes. For example, even after consent is withdrawn, personal data may be further processed to comply with a statutory obligation requiring the data controller to retain the data.

[182] These three legal bases are consistently recognized as those that may potentially apply to OBA. For example, they have been identified in UK Competition & Markets Authority. *Online platforms and digital advertising. Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, para. 4.38

[183] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 123

6.1. Legal basis under ePrivacy Directive

In addition, the rules of ePrivacy Directive apply as *lex specialis* to GDPR. Consequently, even if processing of personal data is justified under Art. 6 GDPR (for example, based on the data controller's legitimate interests), to store or access information in the user's terminal equipment (device), the data controller will still need to obtain the user's informed **consent** under Art. 5 (3) ePrivacy Directive.

The concept of informed consent under ePrivacy Directive is aligned with that of Art. 6 (1) (a) GDPR. Art. 5 (3) ePrivacy Directive provides that processing is justified if the user has granted "*consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC*". Under Art. 94 GDPR, all references to the repealed Directive 95/46/EC are replaced by references to GDPR. It ensues that consent under Art. 5 (3) ePrivacy Directive must also meet the requirements of Art. 7 GDPR[184]. Moreover, although the consent requirements under ePrivacy Directive and GDPR are concurrent and both may be simultaneously applicable, the two types of consent can be merged in practice, provided that the user is made unambiguously aware of what he is consenting to[185].

The WP29 has also clarified that the user's consent to store a cookie may also entail their acceptance for the subsequent readings of the cookie, and hence for the monitoring of their internet browsing[186]. Thus, it is not necessary to ask users for additional consent each time a cookie is accessed.

As an alternative to user consent, ePrivacy Directive provides for two exemptions that can also justify the processing of device data:

- the storage or access is carried out **for the sole purpose of carrying out a transmission of a communication over an electronic communications network**; or

[184] Even though Art. 95 GDPR provides that GDPR does not create additional rules for publicly available electronic communications services that are already subject to specific obligations under ePrivacy Directive, EDPB explains that the requirements for consent under the GDPR are not considered to be an 'additional obligation'. From the reference to Directive 95/46/EC in Art. 5 (3) ePrivacy Directive, the legislators' intention to align the requirements for consent within the two pieces of law is also apparent. See: EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 6
[185] WP29. *Opinion 02/2013 on apps on smart devices, 27 February* 2013, para. 3.4.1
[186] WP29. *Opinion 2/2010 on online behavioural advertising*, 22 June 2010, p. 3

- the storage or access is strictly necessary **to provide an information society service explicitly requested by the subscriber or user**.

As the WP29 noted in its guidance on cookies[187] and device fingerprinting[188], both exemptions are unlikely to apply to processing for OBA purposes. Since the purpose of OBA data processing is never merely to carry out a data transmission, the first exemption is self-evidently out of question.

For the second exception to apply, the access to device data (e.g. reading a cookie) would have to be "strictly necessary" to provide a requested information society service, i.e. to enable a specific functionality that would not otherwise work[189]. The main benefit of relying on the second exemption is that, apart from the user's explicit consent, there are other ways to obtain "explicit request" of a functionality. In essence, any positive action to request a service with a clearly defined perimeter such as creating an account on a website or selecting a preferred language counts as an explicit request. Naturally, the obligations cannot be avoided merely by bundling cookies together. If multipurpose tracking technologies are used (e.g. cookies that serve merely as an identifier), the exemption applies only to those processing activities that fulfil the prescribed conditions.

According to the WP29, the second exemption may justify the following use-cases of tracking technologies:

- **remembering user input** such as the selection of items across several webpages to add them to a virtual shopping cart;
- **user authentication** such as to recognize a logged-in user across webpages (conversely, the use of persistent cookies to recognize the user as they are browsing the web falls outside of the exemption);
- **user-centric security** such as features that prevent user accounts from cyber-attackers;
- **multimedia player session cookies** such as flash cookies that enable video playback;
- **user interface customization** such as the selection of language or display preferences;

[187] WP29. *Opinion 04/2012 on Cookie Consent Exemption*, 7 June 2012.
[188] WP29. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*, 25 November 2014
[189] WP29. *Opinion 04/2012 on Cookie Consent Exemption*, 7 June 2012, para. 2.2

- **social media plugins** that are session-based and only used for logged-in social media users.

On the other hand, social plugin, tracking technologies, or advertising trackers for OBA purposes are not exempt and always require explicit and informed consent[190], because turning off tracking does not generally affect the provider's technical ability to provide the requested services. Curiously, the EDPS proposes that exceptionally, the requirement of prior consent can be skipped in the case of first-party cookies used for anonymous, aggregate statistics under specific assumptions and safeguards[191]. The WP29 is more reserved in this regard – although it recognizes that first-party analytics are not likely to create a high privacy risk, it concludes that (*de lege lata*) neither of the Art. 5 (3) exemptions can be applied in such case. However, both supervisory authorities agree that adopting a more lenient regime for first-party analytics is the right way forward.

It seems that these calls for deregulation of first-party analytics have persuaded the EU's legislators. The latest draft of ePrivacy Regulation – currently subject to trialogue negotiations – proposes in Art. 8 (1) (d) an exception for processing of device data that "*is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the end user, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested*"[192].

All in all, there are currently no exemptions under ePrivacy Directive that would justify the collection of device data without user consent. While the strict regulation of OBA does not seem to be going anywhere, the position could soon change for first-party analytics. Even now, data controllers that take a risk-based approach and perform limited first-party analytics without user consent are likely to avoid major sanctions.

[190] *ibid*., para. 4.2
[191] EDPS. *Guidelines on the protection of personal data processed through web services provided by EU institutions*, November 2016, para. 29
[192] Latest draft of ePrivacy Regulation as of October 2022, pre-approved by the Council is available at: COUNCIL OF THE EUROPEAN UNION. Interinstitutional file 2017/0003(COD), Council of the European Union mandate ST 6087 2021 INIT of 10 February 2021, available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

6.2. Legal basis under GDPR – necessity for contract performance

Turning to GDPR, many data controllers argue that OBA processing is necessary to perform a contract with the data subject under Art. 6 (1) (b) GDPR. Although advertising is usually ancillary to the main content of a website, and as such it is rarely directly requested by users, it allows publishers to finance their business in the attention economy. If services are provided free of charge and the publisher is only able to maintain such business model thanks to advertising revenue, OBA could potentially be seen as necessary in a broader sense for the performance of a contract with the user.

Unfortunately, such reasoning is hard to align with the concept of contractual necessity established in GDPR. According to CJEU's settled case law (largely borrowed from the ECtHR[193]), any limitation of fundamental rights and freedoms must be interpreted restrictively. It follows that the term "necessary" in Art 6 GDPR must as well be understood to require a "strict necessity"[194].

Therefore, to successfully rely on Art. 6 (1) b) GDPR to justify processing for OBA purposes, AdTech vendors must establish that:

1) a contract was concluded with the data subject; and
2) the processing is strictly necessary to perform that contract.

6.2.1. Conclusion of a contract

In OBA context, even the first condition may cause difficulties. Firstly, the contract must be validly concluded under the laws of the respective EU member state. While Czech law generally recognized the validity of click-wrap contracts[195] – contracts where the acceptor agrees to the terms by clicking a button or checking a box – the validity of browse-wrap

[193] "*The cardinal issue that arises is whether the interference so found is justifiable under paragraph 2 of Article 8. That paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be interpreted narrowly. While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*" See: European Court of Human Rights, *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V, para. 47, emphasis added.
[194] CJEU judgment in Case C-13/16 of 4 May 2017, *Rīgas satiksme*, ECLI:EU:C:2017:336para. 30.
[195] For example, see judgment of the Supreme Court of the Czech Republic no. 8 Tdo 307/2020-873 of 24 March 2020 or judgment of the Regional court in Ústí nad Labem no. 45 ICm 4182/2014-35 of 30 October 2015.

contracts – where the user agrees merely by browsing a website or using a service – is questionable in most jurisdictions. In the Czech Republic, contract formation requires both parties to unambiguously express their will to be bound by the agreed terms, whereas silence or inactivity generally do not represent acceptance[196]. Since, in many cases, ads are shown even to unregistered users merely browsing a website, it may be difficult for OBA players to prove that the user willingly accepted their T&C and was fully aware of their content.

Secondly, potential application of Art. 6 (1) (b) GDPR to AdTech vendors is further limited by the fact that AdTech vendors usually do not directly engage with users – generally, users only interact with publisher or advertiser websites. For this reason, only those AdTech vendors, whose data processing activities are closely tied to a specific service provided by the publisher or advertiser that contracts with a user could potentially rely on contract performance (for example, a subcontractor of a publisher that facilitates an authentication function could fit under the provision of a login service enabled by the publisher's T&Cs).

Additionally, when processing data on the basis of a contract with a consumer, controllers must be mindful of the requirements prescribed by consumer-protection laws. For example, under Council Directive 93/13/EEC ("**Unfair Contract Terms Directive**"), standard form contracts (which represent the norm in online contracting) cannot contain unfair terms that cause a significant imbalance in the parties' rights and obligations to the detriment of the consumer[197]. Through this optic, contract terms that seek to justify excessive data processing, which could not be reasonably expected by the consumer, could be deemed unenforceable under Art. 6 (1) Unfair Contract Terms Directive. Furthermore, Art. 5 Unfair Contract Terms Directive provides that ambiguous terms in consumer contracts will be interpreted in favour of the consumer. To fully capture the versatility of their products, online service providers often use very broad and vague language when describing their data processing practices. One can often encounter processing purposes described in a broad manner, such as "*provision and improvement of our products*", "*promoting safety, security and integrity*" or "*research and innovation for social good*"[198]. Should a dispute arise over the meaning of the terms, Unfair

[196] Sec. 1740 of Act No. 89/2012 Coll., the Civil Code.
[197] In the Czech Republic, Art. 3 (1) Unfair Contract Terms Directive is implemented in Sec. 1813 of the Civil Code and applies to all consumer contracts regardless of whether they have been individually negotiated. Additionally, under Sec. 1798 et. seq. of the Civil Code, the protection against unfair terms in standard form contracts is further extended to business-to-business relationships.
[198] The terms are excerpted from Meta's privacy policy effective from 26 July 2022 available at: https://www.facebook.com/privacy/policy/?section_id=2-HowDoWeUse

Contract Terms Directive mandates they be construed to the consumers' benefit. As a result, their actual scope can turn out to be much narrower than the service provider originally intended.

6.2.2. Strict necessity

As per the second condition, data processing must be strictly necessary to provide a service under the contract. To satisfy this condition, merely mentioning a processing activity in the T&Cs is hardly sufficient. The data controllers must ask themselves to what extent the processing is objectively and genuinely necessary to deliver the service, considering the exact objectives of the contract[199]. Conversely, if they find that the data processing is in fact necessary, they should be able to explain how the contract's subject-matter could not be performed without the data processing. Within this exercise, the EDPB advises controllers to consider *inter alia* the nature of the service provided, the rationale of the contract, its essential elements, the mutual understanding of the parties and the reasonable expectations of data subjects.

When looking at a contract in its entirety, the necessity assessment must be performed for each service separately. Otherwise, controllers could bundle services together to artificially inflate the scope of the permitted processing. In my view, such counterbalancing works both ways. After analysing each processing activity separately, the sum of all individual services performed should again be measured against the objectives of the whole contract. This would prevent controllers from disguising unnecessary data processing as ancillary features that offer little added value for the data subject. Such interpretation is coherent with the principle of "privacy by design and default" enshrined in Art. 25 GDPR, which encourages providers to design their services in a way that favours user privacy. Relevant aspects of this principle include differentiation between processing activities, limitation of processing, purpose orientation and data subject autonomy[200]. Keeping Art. 25 in mind, controllers should not bundle unrelated services. Instead, users can be provided with a basic version of the service and be allowed to opt in for additional features.

[199] EDPB. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019, version 2.0, p. 9
[200] EDPB. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 20 October 2020, Version 2.0

6.2.3. OBA based on contract performance

In its guidance, the EDPB sharply rejects the arguments that Art. 6 (1) (b) GDPR could apply to OBA data processing where it is necessary to support an ad-based business model[201]. In the EDPB's view, the requirement of "strict necessity" cannot be fulfilled in case of OBA, since the controller is generally contracted to deliver its service rather than to serve personalized advertisements and it would be hard to argue that disabling ads objectively prevents the controller from providing the service[202]. More generally, the EDPB does not consider personal data to be a tradeable commodity, arguing that while "*data subject can agree to the processing of personal data, they cannot trade away their fundamental rights through this agreement.*" The same understanding of "necessity" is advanced when the EDPB addresses conditionality of consent under Art. 7 (4) GDPR. The EDPB provides that "*GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract*"[203] and that "*there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service*"[204].

I agree with EDPB that Art. 6 (1) (b) cannot generally justify extensive personal data exchanges in RTB auctions. In most scenarios, such processing is neither strictly necessary to provide a service, nor is it based on a valid contract concluded with the user. On this, national DPAs also seem to agree. For example, in the *IAB* ruling, the Belgian DPA concluded that Art. 6 (1) (b) GDPR could not justify the processing of a TC String because "*even if there were a contractual relationship between the users and the publisher, the data processing involved under the TCF would still not meet the requirement of objective necessity for the provision of online services by the publishers to the users concerned (in particular for processing for the purposes of personalisation of content and for advertising based on surfing behaviour)*"[205]. Similarly, the Irish DPC recently issued a € 405 million fine to Meta, finding *inter alia* that

---

[201] "*Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue*". See: EDPB. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019, version 2.0, para. 53

[202] *ibid*., para. 51 *et seq.*

[203] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 26

[204] ibid., para. 27

[205] See the *IAB Ruling*, para. 408.

acceptance of Instagram T&Cs did not provide a sufficient legal basis for the processing of children's contact details on Instagram business accounts[206].

Nonetheless, it does not seem right to me to *a priori* assume that Art. 6 (1) (b) cannot be used to justify OBA. Furthermore, contrary to EDPB's belief, I do not find the CJEU's case law to be so categorically opposed to the idea that processing would be justified by necessity for contract in a broader economic sense rather than a strictly causal sense. While it is true that according to the CJEU's settled case law, "*derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*"[207], this requirement of necessity arises from the more general assessment of proportionality that any interference with the fundamental right to privacy must satisfy[208]. It is not clear to me why the requirement of proportionality – based on the rationale of the contract and circumstances of the resulting data processing – could not in any case be satisfied if the processing is not causally necessary to provide the service (i.e. that without the processing, the provider would be physically precluded from providing the service) but rather necessary to sustain the business model of the provider and uphold the commercial viability of the contract. In this regard, the EDPB's reading of the case law seems overly protective.

On the one hand, I sympathize with the EDPB's concerns that commoditization of personal data could pose a serious threat to the fundamental right of privacy and its firm position that fundamental rights cannot be traded away. On the other hand, I can foresee a situation in which a user could freely decide to limit their fundamental rights to allow fair and proportionate processing of their personal data in exchange for a fulfilment from the data controller. It is important to note that the right to privacy is not absolute and may be limited by the data subject's own actions. For example, as the ECtHR considered in a personality protection dispute[209], the right to privacy "*cannot be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions*". On the facts of this case, when the actor concerned "*revealed details about his private life in a number of interviews […] he had*

[206] Irish DPC decision of 2 September 2022, Inquiry Reference: IN-20-7-4
[207] CJEU judgment in Case C-13/16 of 4 May 2017, *Rīgas satiksme*, ECLI:EU:C:2017:336, para. 30.
[208] "*In that regard, according to the settled case-law of the Court, the principle of proportionality requires that* [interference with the right to privacy] *be appropriate for attaining the legitimate objectives pursued* […] *and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*." See: CJEU judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238, para. 46
[209] ECtHR (GC) judgment of 7 February 2012 on Application no. 39954/08, *Axel Springer AG v. Germany*

[…] actively sought the limelight, so that, having regard to the degree to which he was known to the public, his "legitimate expectation" that his private life would be effectively protected was henceforth reduced"[210]. Similar to an actor who actively seeks out attention of the press and thereby reduces his legitimate expectations of privacy, a user that in full knowledge of the consequences of his or her actions accepts a contract that requires them to endure certain processing of their data in exchange for a particular benefit (e.g. access to a service) may be understood as merely exercising their right to self-determination. After all, the benefit of access to an array of freely accessible content and services could greatly outweigh the detriment caused by a limited data processing of data for advertising purposes, if it is not disproportionate and fully complies with GDPR's principles. If personality rights may be restricted by one's own actions or even partially limited as counter-performance (such as when a celebrity's image is used to promote a product under an endorsement contract), why data protection rights cannot?

Within the realm of consent under Art. 6 (1) (a) GDPR, the practice of trading consent for a certain incentive already seems to be accepted. According to Art. 7 (4) GDPR as reformulated in Recital 42 GDPR, consent is not freely given if the data subject is unable to refuse consent without detriment. As the EDPB rightly points out, "*GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances*"[211]. While the EDPB does not approve of data being used as counter-performance in any context, some DPA's seem to disagree. For example, the Austrian DPA[212] once concluded that consent is not conditional if the controller implements a so-called "pay-or-okay" mechanism, whereunder users are asked to either consent to data processing for OBA purposes and receive a free service or to pay for a subscription. In subsequently released FAQs, the DPA clarified that "pay-or-okay" is permissible only if fair price is charged for the private alternative and if the service provider does not enjoy a monopolistic position or provide a public utility service[213]. In its guidance on cookie walls, the French CNIL expressed similar views[214].

---

[210] *ibid*., para. 101
[211] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 48
[212] Datenschutzbehörde decision of 30 November 2018, no. DSB-D122.931/0003-DSB/2018
[213] DATENSCHUTZBEHÖRDE. FAQ zum Thema Cookies und Datenschutz [online]. 25 May 2022 [viewed 19 December 2022]. Available from: https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html#Frage_6
[214] CNIL. Cookie walls: la CNIL publie des premiers critères d'évaluation [online]. 16 May 2022 [viewed 19 December 2022]. Available from: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation

In my view, the fact that a user may be refused access to an ad-funded service does not automatically means that they suffered a detriment. In general, data subjects cannot legitimately expect that a business will provide them with free services. Therefore, the finding of detriment in such cases should only be reserved to situations, in which access to the service is closer to being necessary for the data subject rather than merely useful (such as due to the widespread reliance on the services or due to it being a public utility service). Notably, consent presented as a "take it or leave it" choice will as well likely not be valid if the controller enjoys a dominant position or if the data subject is caught in a lock-in situation due to their previous use of the service[215].

While the practice of "pay-or-okay" attempts to bridge the divide between the leading interpretation of Art. 7 (4) GDPR and the widespread advertising practice, it is not a perfect solution. In my opinion, the discussion around "pay-or-okay" reveals fundamental flaws in the general prohibition of personal data as counter-performance. For instance, one could ask the following questions. Can providers be forced to provide a subscription-based alternative even if it does not make commercial sense for them to do so? Could this discriminate against low-income individuals, who cannot afford the privacy-preserving alternative? If payment is charged for enhanced privacy, isn't this just another form of privacy commoditization? Given the positive externalities of ad-funded economies, could such preference of subscription-based business models negatively affect businesses with price-sensitive customers or new market entrants and thereby decrease competition in the market?

To say the least, this is a question that has not yet been sufficiently explored in the CJEU's case law. While in *Planet49*[216], the CJEU came close to addressing the problem once it was presented with a situation where the provision of data for advertising purposes was made a prerequisite to participation in a promotional lottery, it refused to provide its insights since the question was not raised by the referring court.

In the light of the above, I propose an alternative interpretation of Art. 6 (1) (b) GDPR, whereby the legal basis does not apply only to processing that is causally necessary to perform a contract but also that is strictly necessary to preserve the commercial viability of the contract

[215] ZUIDERVEEN BORGESIUS, Frederik J., et al. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review* [online]. 2017, 3(3), 353–368 [viewed 19 December 2022]. ISSN 2364-284X. Available from: doi:10.21552/edpl/2017/3/9, para. VII 1.
[216] CJEU judgment in Case C-673/17 of 1 October 2019, *Planet49 GmbH*, ECLI:EU:C:2019:801, para. 64

provided that alternative business models are not available or significantly less effective and where the resulting processing is fair, transparent, and generally proportionate. While even this interpretation clearly cannot justify the processing undertaken by OBA players under the leading RTB protocols, it could potentially justify emerging alternative OBA mechanisms. For example, the privacy-oriented browser Brave allows users to enrol into its Brave Rewards programme to be directly compensated (with tradeable tokens) for seeing a limited number of behavioural ads subject to additional privacy-enhancing measures[217]. In cases such as this one, reliance on contract performance as a legal basis seems appropriate and in line with GDPR's principles.

6.3. Legal basis under GDPR – legitimate interest

The legitimate interests of the data controller represent another potential legal basis for OBA. In line with Art. 6 (1) (f) GDPR, data processing is lawful if it is necessary[218] for the purposes of the legitimate interests pursued by the controller or by a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject. According to recital 47 GDPR, the existence of a legitimate interest requires a careful assessment including whether a data subject can reasonably expect that processing for that purpose may take place. The assessment that a controller must carry out to find out whether it may rely on Art. 6 (1) (f) involves the following three steps[219]:

1) **Purpose test:** are you pursuing a legitimate interest?
2) **Necessity test:** is the processing necessary for that purpose?
3) **Balancing test:** do the individual's interests override the legitimate interest?

Examination of legitimate interests must always be conducted from the perspective of the data controller. As CJEU confirmed in *Fashion ID*[220], to successfully rely on Art. 6 (1) (f)

[217] Brave Browser Privacy Policy [online]. Brave Software, Inc., 12 December 2022 [viewed 19 December 2022]. Available from: https://brave.com/privacy/browser/
[218] In the sense of a strict necessity as explained above.
[219] For a summary of the requirements see: ICO. What is the 'legitimate interests' basis? Guide to the General Data Protection Regulation (GDPR) [online] [viewed 19 December 2022]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test
[220] *CJEU judgment in Case C-40/17 of 29 July 2019, Fashion ID, ECLI:EU:C:2019:629*, para. 96

in advertising context, it is necessary that each of the controllers involved should pursue a legitimate interest.

In case of OBA, satisfying the first condition is not so problematic. Recital 47 GDPR lists direct marketing as an example of a legitimate interest a data controller may have. The WP29 adds that this extends also to other forms of marketing or advertising and that "*controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers and* [that legitimate interest] *may be an appropriate legal ground to be used for some types of marketing*"[221]. In a letter sent to the Dutch DPA[222], the European Commission as well argues that the concept of legitimate interest under GDPR does not exclude purely commercial interests of the data controller.

The second condition poses a more significant obstacle. Given the restrictive interpretation of "necessity" under GDPR, controller cannot justify its data processing by legitimate interests if less invasive means are available to serve the same end[223]. As Advocate General Rantos points out in his opinion in *Meta Platforms v Bundeskartellamt*[224], in the context of OBA, the "*question therefore arises as to the 'degree of personalisation' of the advertising objectively necessary*". Indeed, the scope and nature of the processing greatly influence the results of the legitimate interest assessment. If, for instance, a publisher would be able to generate similar ad revenue from non-personalised ads based on contextual targeting or by relying on innovative privacy-oriented technologies, it may not be possible for them to invoke Art. 6 (1) (f) to justify large-scale behavioural profiling. To quote prof. Zuiderveen Borgesius[225], "*it seems questionable whether tracking people's browsing behaviour is the least intrusive manner for the ad network to enable advertisers to promote their products*" and since "*behavioural targeting would be possible without large-scale data collection, it could be seen as disproportionate if companies collect large amounts of personal data for behavioural targeting*".

---

[221] WP29. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, p. 25
[222] EUROPEAN COMMISSION. Letter to the Dutch DPA of 6 March 2020, Ref. Ares(2020)1417369
[223] WP29. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, p. 29
[224] Opinion of Advocate General Rantos of 20 September 2022 in Case C-252/21, *Meta Platforms v Bundeskartellamt*, para. 64
[225] ZUIDERVEEN BORGESIUS, Frederik J. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* [online]. 2015, 5(3), 163–176 [viewed 18 December 2022]. ISSN 2044-4001. Available from: doi:10.1093/idpl/ipv011, p. 168

The last condition requires controllers to perform a complex balancing exercise to assess proportionality of the data processing to the potential impact that it may have on the data subjects. According to the WP29, the key factors to consider when assessing the impact of the processing include (i) the potential consequences of the processing for the data subject and the likelihood they will materialise; (ii) the nature of the data and of the processing activities performed; and (iii) the reasonable expectations of the data subject[226].

One of the main factors that weighs against the proportionality of OBA is that the leading RTB protocols do not contain any effective safeguards to ensure that the principle of purpose limitation is observed. Once data contained in a bid request is disseminated to the demand side, there are no technical measures in place that would prevent misuse of the acquired data for additional purposes and preclude further sharing with third parties. Privacy advocacy groups consistently challenge the common misconception among consumers that the primary negative consequences of OBA data processing take the form of the nuisance caused by seeing too many pervasive ads or the discomfort experienced when one is confronted with creepy ads adapted to browsing behaviour. In fact, when data is shared with thousands of parties without effective controls against function creep, there is much more at stake[227].

Bid requests exchanged in RTB ecosystems contain information that may itself have value independent of the advertising context in which it is communicated, such as online identifiers that allow ISSPs to recognize users across networks, the data subject's location or their topics of interest. In addition, raw data may be combined and analysed to make more general inferences about the data subject and learn about their personality and behaviour. Studies have shown that using only Facebook "likes", it is possible to predict with surprisingly high accuracy a range of highly sensitive personal attributes about a data subject (e.g. their sexual orientation, ethnicity, intelligence, happiness or use of addictive substances)[228] or to

[226] WP29. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, p. 36 *et seq.*

[227] For non-exhaustive list of risks associated with RTB see: CHRISTL, Wolfie and SPIEKERMANN, Sarah. *Networks of control a report on corporate surveillance, Digital Tracking, Big Data & Privacy*. Wien: facultas [online]. January 2016. ISBN: 978-3-7089-1473-2., p. 81

[228] KOSINSKI, Michal, STILLWELL, David and GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior [online]. Proceedings of the National Academy of Sciences, April 2013, Volume 110, Issue 15, 5802–5805. DOI: 10.1073/pnas.1218772110. Available from: https://www.pnas.org/doi/10.1073/pnas.1218772110

predict their personality better than the person's friends and family[229]. It is easy to imagine countless ways in which such information could be abused. For instance, the story of the infamous Cambridge Analytica taught us how psychological profiles inferred from seemingly insignificant data about people's interests on a social network can be abused to manipulate voters in an attempt to influence the results of democratic elections[230].

In extreme cases, data leaks from RTB networks may have immediate and direct effects on the affected data subjects' lives. Estimates about personality and behaviour are already used to make automated decisions about data subjects, such as to predict their creditworthiness when evaluating their application for a loan[231]. Some reports even suggest that location data exchanged in RTB may have been repeatedly accessed by US state authorities posing as advertisers and used to track down illegal immigrants[232].

Another factor to consider is the nature of the personal data processed. It was demonstrated that bid requests may contain special categories of personal data. Additionally, seemingly neutral data may be used to make inferences about sensitive aspects of data subjects' lives. In *Meta Platforms v Bundeskartellamt*, Advocate General Rantons expressed the views that even if behavioural data is not sensitive *per se*, it should be covered by Art. 9 GDPR, if the data "*considered in isolation or aggregated, make it possible to profile users on the basis of the categories that emerge from the listing in that provision of types of sensitive personal data*"[233]. Given the CJEU's prior case law such as *OT v Chief Official Ethics Commission Lithuania*, it is likely that in its ruling, the CJEU will uphold the AG's interpretation.

---

[229] YOUYOU, Wu, KOSINSKI, Michal and STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans [online]. Proceedings of the National Academy of Sciences, January 2015. 112 (4), 1036–1040. DOI: 10.1073/pnas.1418680112. Available from: https://www.pnas.org/doi/10.1073/pnas.1418680112

[230] For an overview of the Cambridge Analytica case together with other notable examples of threats presented by big data see CHRISTL, Wolfie and SPIEKERMANN, Sarah. *Networks of control a report on corporate surveillance, Digital Tracking, Big Data & Privacy*. Wien: facultas [online]. January 2016. ISBN: 978-3-7089-1473-2.

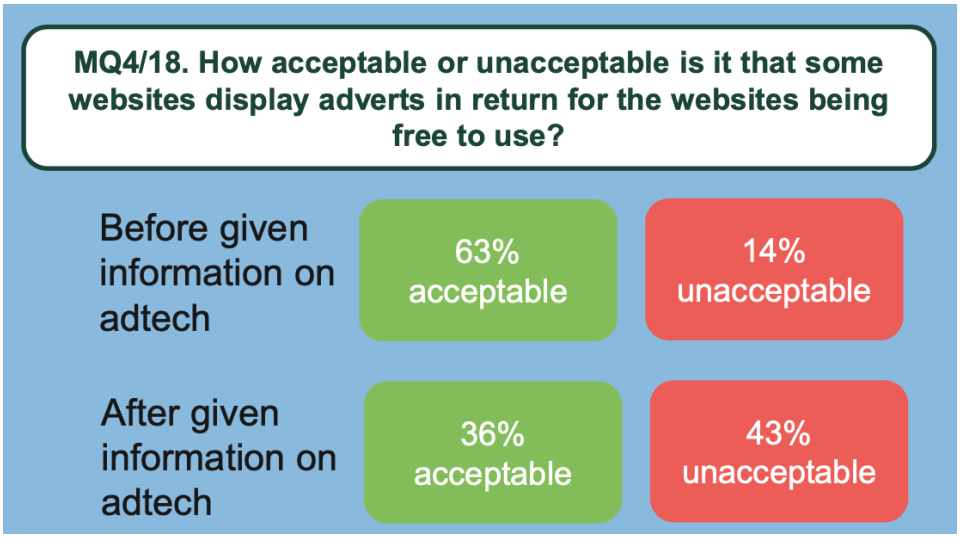
[231] For examples of credit scoring based on web searches, smartphone use or location data see: *ibid*., Chapter 3.2.

[232] Links to the relevant news sources are compiled in LEMOINE, Laureline et al. *Targeted Online – An industry broken by design and by default* [online]. Brussels: European Digital Rights (EDRi), 9 March, 2021. [viewed 19 December 2022]. Available from: https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf, p. 39

[233] Opinion of the CJEU Advocate General Rantos of 20 September 2022 in Case C-252/21, *Meta Platforms v Bundeskartellamt*, para. 46

Other issues relate to the nature of the data processing. Apart from the massive scale of data processing carried out within RTB ecosystems, it is relevant that the principle of privacy by default is not always observed allowing personal data to be disclosed to bid request recipients even where the user does not consent to the data processing.

Finally, as regards the reasonable expectations of the data subjects, market research shows that consumers are drastically underinformed about the functioning of RTB ecosystems and the potential consequences of OBA data processing. In market research commissioned by the UK ICO[234], respondents were asked to evaluate how acceptable they find that some websites display adverts in return for the websites being free to use. While initially, 63 % of respondents stated that they find this acceptable, after they were explained how OBA processes work, the number significantly dropped:



Considering all its aspects, it is therefore highly unlikely for data processing occurring in today's leading RTB exchanges to be justified by legitimate interests of the participating companies. This is a view shared by both scholars[235] and supervising authorities. In its guidelines on Art. 6 (1) (f) GDPR, the WP29 provides that where controllers process personal

[234] WORLEDGE, Michael and Mike BAMFORD. Adtech Market Research Repor [online]. ICO, March 2019 [viewed 19 December 2022]. Available from: https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

[235] For example, see ZUIDERVEEN BORGESIUS, Frederik J. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* [online]. 2015, 5(3), 163–176 [viewed 18 December 2022]. ISSN 2044-4001. Available from: doi:10.1093/idpl/ipv011, p. 170: "*under current law, personal data processing for behavioural targeting, in particular if it involves tracking people over multiple websites or Internet services, generally cannot be based on necessity for the legitimate interests of the controller*".

data to "*unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences without their knowledge [, such] a profiling activity is likely to present a significant intrusion into the privacy of the customer [and] the controller's interest would be overridden by the interests and rights of the data subject*"[236]. Similarly, the EDPB concludes that advertisers may not rely on legitimate interests to use data acquired through purchases for retargeting, since this would not reasonably be expected by the data subject[237].

Nonetheless, it cannot be ruled out that legitimate interest could be used as a legal basis for less intrusive forms of OBA. Provided that the principles of GDPR are duly observed and processing is limited only to what is strictly necessary, I can imagine that Art (1) (f) could be relied on especially for certain incidental processing operations performed in OBA context that do not pose additional privacy risks and can reasonably be expected by the data subjects, such the basic process of reception and evaluation of a bid request and bid submission, or the recording of the data subject's processing preferences by a CMP.

6.4. Legal basis under GDPR – consent

The best fitting legal basis for most processing operations occurring in RTB auctions is the data subjects' freely given consent. Besides the fact that other legal bases may not be available given the context of the processing, in most scenarios, the data processed will also represent "device data" under ePrivacy Directive. Under ePrivacy Directive, at least the OBA players that directly interact with the user's device will always be required to collect consent[238].

Art. 4 GDPR defines consent as any (i) *freely given*, (ii) *specific*, (iii) *informed*, and (iv) *unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. Additionally, consent must also be "explicit" if it is used to process special categories

[236] WP29. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, p. 26
[237] EDPB. *Guidelines 8/2020 on the targeting of social media users*, 13 April 2021, version 2.0, para. 59
[238] As was explained above, the exemptions from consent under ePrivacy will likely not apply to OBA.

of data[239] or for processing involving automated decision-making[240]. When collecting consent in online environments, this will require the controller to exert increased effort to draw the data subject's attention to the consent request and the potential consequences of the resulting data processing.

It is not the purpose of this paper to comprehensively describe the requirements for each element of a GDPR-compliant consent[241]. Instead, I would like to explore aspects that appear to cause the most problems when consent is sought for OBA purposes. I will not separately consider the concept of freely given consent (as opposed to conditional) as this aspect has already been addressed above in connection with processing based on contract performance.

6.4.1. Specific and granular consent

Consent must always be provided for a clearly defined and specific purpose[242]. Where consent is sought to justify multiple processing operations, the design of the consent form must distinguish between processing operations carried out for different purposes and allow for a separate consent (opt-in) to be granted for each processing purpose[243]. Since specificity and granularity of consent must always be assessed on a case-by-case basis, it may be difficult for controllers to determine how broadly or narrowly the consent must be defined and whether the carried-out processing operations may still fall under the declared purpose.

In this regard, controllers should keep in mind the guidance that GDPR provides in relation to the purpose limitation principle. In line with Art. 6 (4) GDPR, when ascertaining whether processing for another purpose is compatible with the original purpose for which data was collected, controllers must consider inter alia: a) any link between the purposes; b) the context in which the personal data was collected; c) the nature of the personal data; d) the possible consequences of the intended further processing for data subjects; and e) the existence of appropriate safeguards. The information provided to the data subjects and their reasonable expectations also plays an important role.

---

[239] Art. 9 (2) (a) GDPR.
[240] Art. 22 (2) (c) GDPR.
[241] For a complete explanation of GDPR's consent requirements see: EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1.
[242] Art. 6 (1) (a) GDPR.
[243] In addition to Art. 6 (1) (a) GDPR, the requirement of specificity and granularity is also acknowledged in Recitals 32 and 42 GDPR.

Applying these principles, OBA players should carefully examine all the intended processing activities and identify a common overarching processing purpose that sufficiently explains the carried-out processing to the data subjects. In turn, activities that appear too remote from such initial purpose should be considered as a new purpose. On the one hand, a narrowly defined purpose (e.g. "sharing data with the publisher's SSP") could not be understood as comprising other operations that may occur in OBA such the sharing of data with advertisers, tracking users or behavioural profiling. On the other hand, if the purpose is defined too broadly (e.g. "advertising") it would not be specific enough and would not allow the data subject granting the consent to understand the extent of the processing and its potential consequences. Therefore, controllers should always search for the right balance.

6.4.2. Acquiring consent online

In online environments, consent is mostly acquired through consent forms implemented by the service provider. The active confirmation of such forms may be designed in many ways, including swiping a bar on a screen[244], ticking an opt-in checkbox, clicking a button, choosing from yes/no options, or adjusting technical settings or preference dashboard settings[245]. On the other hand, silence, inactivity, or lack of opt-out do not constitute consent[246] as well as any actions that are not clearly distinguishable and unambiguous such as such as scrolling or swiping through a webpage[247]. In *Planet49*[248], CJEU ruled that the requirement of "indication" of the data subject's wishes clearly points to active rather than passive behaviour and that preselected tick in a checkbox does not meet the requirement, since in such case, it would not be inconceivable "*that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited*"[249].

[244] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 85
[245] ICO. How should we obtain, record and manage consent? *Guide to the General Data Protection Regulation (GDPR)* [online] [viewed 19 December 2022]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/#how1
[246] Recital 32 GDPR.
[247] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 86
[248] CJEU judgment in Case C-673/17 of 1 October 2019, *Planet49 GmbH*, ECLI:EU:C:2019:801, para. 52
[249] *ibid*., para. 55

It was previously debated whether the reference to consent granted via "technical settings for information society services" in GDPR[250] and "appropriate settings of a browser or other application" in ePrivacy Directive[251] could mean that users consent to the collection of cookies for OBA purposes merely by not switching off cookie collection in their browser settings and stick with the default setup. Any doubt regarding this question was effectively dispersed by CJEU in *Planet49*. Therein, the court observed that following the adoption of GDPR and of Directive 2009/136/EC amending ePrivacy Directive, user consent may no longer be presumed but must be the result of active behaviour on the part of the user[252]. Even prior to GDPR, WP29 considered consent through browser settings to be valid only if the browser rejected cookies by default and the data subjects were required to "*engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites*"[253].

Of course, that does not mean that consent cannot be provided via technical settings at all. On the contrary, transparent controls provided on browser or application level can be an effective tool to allow users to influence the collection of data about their browsing behaviour. However, it appears that generally, these controls are not currently available in RTB ecosystems. For user-side controls to be an effective way to grant consent for OBA data processing, standardization is needed to ensure that the tools may be relied on by all participating OBA players across all contexts.

6.4.3. Informed consent

When considering whether processing activities are justified by consent, it is also important to look at the information provided to the data subject at the time the consent was granted. Art. 12 to 14 GDPR provide a list of the required disclosures[254]. Furthermore, it is not only relevant what information is provided but also how it is provided. Under Art. 7 (2) GDPR, a request for consent must be distinguished from other communications and provided in intelligible and easily accessible form, using clear and plain language. Consequently, valid

[250] Recital 32 GDPR.
[251] Recital 66 of Directive 2009/136/EC amending ePrivacy Directive.
[252] CJEU judgment in Case C-673/17 of 1 October 2019, *Planet49 GmbH*, ECLI:EU:C:2019:801, para. 56
[253] WP29. *Opinion 2/2010 on online behavioural advertising*, 22 June 2010, p. 14
[254] In CJEU judgment in Case C-673/17 of 1 October 2019, *Planet49 GmbH*, ECLI:EU:C:2019:801, para. 81, the CJEU ads that if consent is collected for the use of advertising cookies, users must also be informed about the duration of the operation of cookies and whether they may be shared with third parties.

consent cannot be obtained merely by reference to the service provider's T&Cs. The consent request must be more prominently brought to the users' attention.

The aim of these rules is to alert the data subject to the fact that they are consenting to data processing and allow them to easily recognize the extent of the processing and its consequences so that they can make an informed decision[255]. Among the prescribed information requirements, Recital 42 stresses the importance of disclosing the identity of the data controller and describing the purposes of the processing.

In OBA, this gives rise to another significant issue. Commonly, the only point of contact for users exposed to OBA is the publisher of the website where ads are displayed. Nonetheless, if consent is to also serve as a legal basis for other RTB participants to which data is transmitted by that publisher, all of them should be named in the consent request. Otherwise, they would not be allowed to rely on the consent. On top of that, the consent must cover all purposes pursued be each of the stakeholders involved.

To this end, the need to obtain a legal basis for each data controller involved cannot be easily bypassed by contractual frameworks between OBA players as is often asserted by AdTech vendors. For example, Google's Authorized Buyers Program Guidelines[256] make advertisers solely responsible for data protection compliance. However, if advertisers have no direct contact with the user but still need to rely on consent to justify their processing, the requirement is effectively impossible to comply with. The CNIL's fine to Vectuary serves as an example of the likely extent of such lawless processing and its potential consequences for AdTech vendors[257]. After Vectuary – a DSP that processed data acquired from OpenRTB bid requests – failed to demonstrate that consents had been granted by the affected data subjects, it was ordered to delete all the acquired data. Notably, CNIL also considered that Art. 6 GDPR was not complied by Vectury merely by relying on contractual assurances that valid consents had been collected by other AdTech vendors in previous stages of RTB auctions.

Due to these complexities of RTB, where data is shared in complex networks with thousands of participants all of which seek to rely on consent to justify their processing,

[255] *ibid*., para. 74
[256] GOOGLE. The Privacy Sandbox [online]. 28 March 2022 [viewed 19 December 2022]. Available from: https://www.google.com/doubleclick/adxbuyer/guidelines/
[257] Commission Nationale de l'Informatique et des Libertés decision No. MED-2018-042 of 30 October 2018

obtaining informed consent is especially difficult. The EDPB recognizes that in this manner, the obligations prescribed by GDPR are two-fold, requiring disclosures that are precise and complete on the one hand and understandable on the other hand[258]. As a solution, the EDPB proposes a "layered" approach to accommodate for small screens or situations with restricted room for information and to not overwhelm users with excessive information. In EDPB's view, informed consent can still exist even if not all required disclosures are presented in the first layer – the consent banner – but are explained in a linked-to privacy policy. If necessary, even the consent banner may be differentiated into several layers that users may explore.

Unfortunately for AdTech, if processing is too extensive, even a layered approach may not be acceptable. Hiding information under several layers that user needs to click through can again infringe the Art. 7 (2) element of easily accessible and clear information.

6.4.4. Privacy fatigue

Experts also warn about another aspect that hinders the exercise of informational self-determination by internet users – the so-called "privacy fatigue". Being exposed to that much information when browsing the web causes users to become numb to privacy notices and blindly accept all consent requests[259]. Such attitude is understandable. According to researchers[260], it would take a person approximately 201 hours per year to read all privacy statements for the websites he or she visits. Consequently, only a minority of consumers actively tries to influence how their personal data is processed since most of them lack the knowledge necessary to identify threats to their privacy and actively overcome them[261].

User attitudes towards OBA were also explored in detail in a market study conducted by the UK CMA [262]. Therein, the CMA identified several challenges for user privacy in online advertising, including:

---

[258] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1, para. 69
[259] Literature and research on this subject have been comprehensively described in BOERMAN, Sophie C., Sanne KRUIKEMEIER, and Frederik J. ZUIDERVEEN BORGESIUS. Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising* [online]. 2017, 46(3), 363–376 [viewed 18 December 2022]. ISSN 1557-7805. Available from: doi:10.1080/00913367.2017.1339368
[260] *ibid*., p. 367
[261] *ibid*., p. 368
[262] UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, para. 4.43 *et seq*.

- Privacy paradox: The CMA points to a "privacy paradox" observed when users decide whether to allow data processing as a trade-off for receiving a service. Even though users claim to be concerned about their privacy, they behave in a way that contradicts this clearly stated preference by not making use of the offered privacy controls. This may be because users are forced to make snap judgments despite being unable to assess the long-term consequences of their choice. Other research suggests that users may be averse to the additional inconvenience connected with the enforcement of their privacy (e.g. less smooth user experience) or that, if they are presented with a "take it or leave it" choice concerning a service that is considered a "must have", they feel that they are left with no other choice than to accept.

- Insufficient knowledge: Although users are generally aware that their data is used to power OBA, research show that only few are aware of the true scale of the data processing involved. Furthermore, user concerns tend to increase as they learn more about OBA data-handling practices. As their concerns increase, they are less willing to receive personalized advertisements.

- Perceived loss of control: Consumer surveys show that most users feel that they have little or no control over the processing of their data online.

- Lack of user engagement: Surveys found that only a small number of users engages with privacy policies and settings on a regular basis or even opens policies presented to them online before accepting them. According to data provided by Google, 85% of visits to its privacy policy last shorter than 10 seconds. The data also revealed inefficiencies of the layered approach, since 75 % of users visiting the privacy policy did not click on any links provided therein.

- Accepting default settings: According to data submitted by Google and Facebook, less than 5% of users interact with privacy settings at the time of sign-up as well as during regular use.

In this manner, the GDPR's concept of consent is built on the flawed premise that, if provided with sufficient information, data subjects are capable of making a rational decision. However, this consent model does not take into account the inherent limits of human cognitive capabilities – once the processing is complex enough, it may well be impossible for data subjects to comprehend the vast amounts of information presented, all the more anticipate the potential consequences of the processing. Evidence shows that in practice, biases and behavioural tendencies lead users towards wrong decisions about the use of their data. Some authors argue that these challenges could be partially offset by privacy-enhancing choice architectures of user interfaces – the so-called "privacy nudges"[263]. Privacy nudges steer users into making privacy-conscious decisions and involve soft paternalism measures such as alerting users to high-risk processing or regularly notifying users to make sure that they are aware of available privacy controls. In my view, implementing privacy nudges may be a great way for controllers to ensure that they collect free and informed consent and comply with the privacy-by-design obligation.

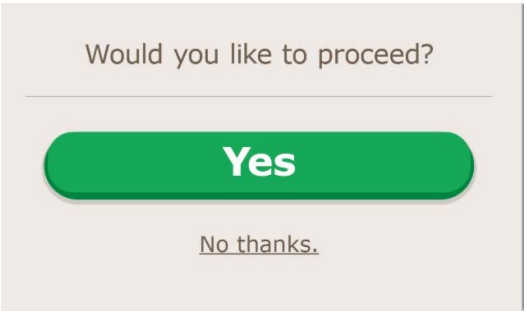
6.4.5. Dark patterns

Another significant threat to user privacy online are dark patterns. Dark patterns are basically the opposite of privacy nudges. Dr Leiser[264] describes dark patterns as "*interface design choices that benefit an online service by coercing, steering, and/or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make*". Many companies deliberately implement dark patterns to shift consumers towards behaviours favourable to data collection and to impede users from limiting the scope of data processing for OBA purposes[265]. Given the inherent value of data, AdTech companies have a considerable economic incentive to maximize their data collection by steering users into accepting more intrusive data processing practices. In its report, the CMA expressed the view that the recorded low levels of actual consumer engagement could be partially caused by the prevalence of influencing choice architecture.

[263] The academic literature on privacy nudges has been explored in detail in SOH, S. Y. Privacy Nudges. *European Data Protection Law Review* [online]. 2019, 5(1), 65–74 [viewed 18 December 2022]. ISSN 2364-284X. Available from: doi:10.21552/edpl/2019/1/10

[264] LEISER, Dr Mark. 'Dark Patterns': The Case for Regulatory Pluralism. *SSRN Electronic Journal* [online]. 2020 [viewed 18 December 2022]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.3625637

[265] UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study, para. 4.168



Example of a dark practice provided in the CMO report, para. 4.201. The "Yes" option is presented more prominently to steer users into accepting the data processing.

Although dark patterns are not explicitly regulated by GDPR, they are likely to contravene GDPR rules, such as the concept of freely given, specific, and informed consent, the principles of lawfulness, fairness and transparency, the obligation of privacy-by-design and privacy-by-default, or communication of request for consent in intelligible and easily accessible form, using clear and plain language.

Recently, regulators have started to acknowledge the danger of dark patters. In March 2022, the EDPB issued guidelines on dark patterns, where it provides an overview of the most common manipulative practices and explains how such practices interfere with GDPR rules[266]. In May 2022, the guidance was followed by a behavioural study on dark patterns and unfair commercial practices published by the European Commission. Dark patterns have also entered the spotlight of supervising authorities. In fact, two of the largest GDPR fines to date were issued for a dark pattern. In early 2022, CNIL issued a € 150 million fine to Google and a € 60 million fine to Facebook for designing their layered consent form in such a way, that users were able to accept the cookie processing with a single click in the first layer, whereas the refusal button was moved to the second layer. CNIL took into account relevant research from Cambridge University and MIT, showing that that 93.1% of Internet users faced with cookie banners stop at the first layer and that relegating the opt-out button to the second layer increases consent rate by more than 20 % on average[267]. CNIL thus considered that Google's and Facebook's consent design deliberately manipulated users into consenting.

[266] EDPB. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, 14 March 2022
[267] Commission Nationale de l'Informatique et des Libertés decision restricted committee No. SAN-2021-024 of 31 December 2021 concerning Facebook Ireland Limited, para. 98

6.4.6. Justifying OBA by user consent

Considering the legal pre-conditions for a GDPR-compliant consent, it is very hard for AdTech vendors to collect valid consent with targeted advertising. Given the enormous scale of the processing, it seems impossible to provide users with comprehensive information about the data processing without overwhelming them and thus failing to provide the information in a user-friendly way. Research further shows that data subjects are not familiar with the pitfalls of online advertising and are easily influenced by dark patterns.

The current state of play also poses regulatory risks to AdTech vendors. Since most of them do not directly interact with users and only receive data from RTB networks, they may not be able to demonstrate valid consent for the processing operations they carry out. Recent GDPR enforcement, in particular the *IAB* and *Vectuary* cases, reveals how deeply rooted the problem may be. In the *IAB* ruling[268], the Belgian DPA acknowledged this issue, stating that in RTB, the "*recipients for whom consent is obtained are so numerous that users would need a disproportionate amount of time to read this information, which means that their consent can rarely be sufficiently informed*" and that the "*information CMPs provide to users remains too general to reflect the specific processing operations of each vendor*". Moreover, "*enrichment of the data in a bid request with personal data already held by the adtech vendors and the relevant Data Management Platforms means that users cannot possibly be properly informed*".

In my view, it is important to recall that provisions of GDPR are built on the foundations of Art. 8 of the European Convention on Human Rights and that even under GDPR, data processing can only be justified so long as it is proportionate. Thus, AdTech vendors cannot expect consent to serve as a universal waiver to justify any processing that they might intend to pursue. There must be a situation in which the envisaged processing is so extensive and complex that it can no longer be justified by simply clicking an "accept" button (the more when it can no longer be easily explained in plain language). If the data subjects fail to grasp the true nature of the data processing, how can they consent to it? And if they do, can this still be regarded as an expression of informational self-determination?

[268] *IAB ruling*, para. 435 *et seq*.

It appears that in this age of attention economy and big data, the data processing occurring in the AdTech sector and especially processing related to RTB has grown into a massive scale that may no longer be supported by user consent. A 2020 report prepared by the Irish DPC shows that out of 38 examined controllers including most well-known organisations engaged in user tracking online, the majority were found to have potential compliance issues, particularly in relation to reliance on implied consent[269].

AdTech vendors should keep in mind that where they act as data controllers, they are still responsible for compliance, even if they receive data from well-known tools such as RTB networks. The principle of accountability under Art. 24 GDPR provides that it is always the data controller, who is responsible for ensuring and demonstrating that processing is performed in accordance with GDPR.

[269] IRISH DPC. Report by the Data Protection Commission on the use of cookies and other tracking technologies [online]. Data Protection Commission, 6 April 2020 [viewed 19 December 2022]. Available from: https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf.

"*What we found during our ongoing adtech work is that companies are collecting and sharing a person's information with hundreds, if not thousands of companies, about what that person is doing and looking at online in order to show targeted ads or content. Most of the time, individuals are not aware that this is happening or have not given their explicit consent. This must change.*"

Elizabeth Denham, the UK's Information Commissioner[270].

"*Privacy shouldn't be a matter of personal responsibility. It's not your job to obsess over the latest technologies that can secretly monitor you, and you shouldn't have to read through a quarter million words of privacy-policy legalese to understand how your phone shares data. Privacy should be a right, not a privilege for the well-educated and those flush with spare time. Everyone deserves to live in a world—online and offline—that respects their privacy.*"

The Electronic Frontier Foundation[271].

[270] ICO. *ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry* [online]. ICO, 25 November 2021 [viewed 19 December 2022]. Available from: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/

[271] GEBHART, Bennett Cyphers and Gennie, 2021, Behind the one-way mirror: A deep dive into the technology of Corporate Surveillance. *Electronic Frontier Foundation* [online]. 10 February 2021. [viewed 19 December 2022]. Available from: https://www.eff.org/wp/behind-the-one-way-mirror

Conclusions

The conducted research largely confirms the existence of the presupposed privacy deficit in OBA markets. Even though RTB data exchanges mostly fall under the scope of ePrivacy Directive and GDPR, user data is often shared among thousands of parties without effective safeguards to ensure lawfulness of the processing. Internet users are not informed about the extent and potential consequences of the processing and are unable to exercise their right to informational self-determination. Due to the extensive nature of the performed data processing and lack of necessary safeguards, controllers participating in OBA likely cannot rely on contract performance or legitimate interests and reliance on user consent is problematic at best. Therefore, data processing in current RTB ecosystem may be largely taking place without an appropriate legal basis under both ePrivacy Directive and GDPR.

Why am I seeing this ad?

In this paper, I have carefully examined the functioning of current RTB ecosystems, the methods that AdTech companies use to track our browsing behaviour, and the protocols that decide which ads will be displayed to us based on that behaviour. It was established that programmatic methods of ad buying based on real-time analysis of user data account for the majority of online display advertising. These methods of ad delivery often involve the cooperation of thousands of parties forming complex advertising ecosystems. Within the AdTech industry, OBA players are commonly distinguished according to their role within the ad supply chain. Since programmatic methods are software-based, AdTech vendors providing such software play a crucial part in the process. On the supply side, publishers enter ad exchanges thorough their supply side platforms to offer their free ad space for sale. On the demand side, advertisers receive bid requests through demand side platforms and bid on available advertising space to deliver ads to users. To enhance the accuracy of ad targeting, both sides often enrich the information learned from RTB transactions with additional user data acquired from data management platforms. Identifying users and collecting their data is required not only for targeting, but also to effectively measure ad performance and combat ad fraud. In this manner, tracking helps preserve the fairness of RTB exchanges.

Next, I have explored how users are tracked in online environments to learn about their browsing behaviour and ultimately about their buying interests and preferences. As a general

note, it was considered that the inherent properties of the internet pose a challenge for online service providers, who usually cannot simply identify and repeatedly recognize users that visit their online environments. To overcome this, they need to employ some of the available tracking technologies. Currently, the advertising market still relies on third-party cookies as the primary tool for identifying and tracking users browsing the web. On mobile devices, advertising IDs implemented by device manufactures are widely leveraged for their universal availability. Nonetheless, probabilistic methods such as canvas fingerprinting show that when enough data is communicated with the service provider, they can use inferences to distinguish users with surprising accuracy.

From the technological perspective, the AdTech industry is currently experiencing a revolution. Due to the increasing demand for user privacy, large platforms have now turned their back on cookies and are on the lookout for less intrusive alternatives. While the majority of commercial browsers has already abandoned or at least significantly limited third-party cookies, the effects have not yet been fully experienced by the AdTech industry given that Google's Chrome browser – accounting for the majority of the worldwide browsing activity – is yet to take that step. Nevertheless, Google is working hard on its Privacy Sandbox initiative, which is expected to come up with a proposal for the new market standard for privacy-preserving OBA. Taking into account these recent technological changes, I believe it is now the best time for AdTech companies to take an honest look at their data-handling practices and measure them against the stringent requirements of EU's privacy laws.

Is bid request data protected by law?

Looking at the structure and contents of bid requests communicated in Authorized Buyers and OpenRTB protocols and considering the overall purpose of the processing, it is evident that most data processed within RTB constitutes "personal data" under GDPR. In addition, when the data is collected from the user's device, such as by inducing the browser to make a HTTP request to an ad server, it must also be considered "terminal equipment information" under ePrivacy Directive. In line with the concept of "reasonable identifiability" maintained by case law of the CJEU (*Brayer* in particular), it was demonstrated that the fact that data is compiled outside of RTB context or the fact that the AdTech vendor performing the processing is itself unable to tie the data to a specific individual will rarely suffice to achieve

true anonymization. Under GDPR, "identifiability" must be interpreted very broadly as including any potential to single-out a person from the crowd (even if their name is not known). In this sense, even the unique characteristics of the user or their behaviour can serve as probabilistic identifiers. In the AdTech business, the ability to identify the data subject and make inferences about them is what gives data its value. Thus, companies collecting data for targeting purposes will generally be unable to claim that they only process anonymous data.

Who is responsible for the data processing?

Once I had established that ePrivacy Directive and GDPR apply, it was necessary to determine to what extent the individual actors involved in RTB may be responsible for the data processing taking place. Under the ePrivacy Directive, identifying the responsible party is fairly simple. In RTB, only those parties that directly interact with the user's device can fall under the scope of the directive. In this regard, an important clarification to make is that according to the WP29, this also includes parties that do not themselves collect data, but that nonetheless deliberately make data collection possible by introducing code into their services that induces the user's device to transmit data to AdTech vendors.

Under GDPR, I have analysed the concepts of "controller", "processor" and "joint-controller" as explained in the CJEU's case law laid out in particular in *Wirtschaftsakademie* and *Fashion ID*. While it is impossible to provide a brief answer as to the extent of responsibility of the individual parties involved in RTB data processing, it is possible to arrive at some overall observations. When examining the RTB ad delivery chain, it is necessary to distinguish between data processing essential to the RTB auction and additional processing performed by each of the RTB participants for their own purposes. In general, publishers and SSPs exercise control over the contents of a bid request, its dissemination to advertisers, and its subsequent evaluation. Advertisers and DSPs decide on the processing carried out for bidding purposes (including any additional processing to improve ad targeting) and to deliver the ad. Depending on the modalities of each advertising ecosystem, I believe that it is even possible for publishers and advertisers in programmatic systems to act as independent data controllers, given their involvement in different stages of the ad delivery process.

Determining the role of AdTech intermediaries turned out to be a more challenging task. When drawing a line between mere data processing and joint controllership, the existing decision-making practice does not properly take into account the specific nature of data processing carried out by business users through standardized software products. On the one hand, it may seem that by making choices regarding the design of such software, its developers necessarily influence the way in which data will be processed. On the other hand, it is not clear whether the business users of such software could be deliberately affirming the data processing choices imprinted therein by making use of the software on pre-defined terms. In my view, to not completely erode the GDPR's concept of "controller", it is necessary to define a clear threshold for the acceptable extent to which an AdTech vendor can be involved in the decision-making concerning the means of data processing without it losing its data processor status. Until more guidance is available, I have proposed some non-exhaustive considerations that may be taken into account when determining the role of providers of standardized software tools.

Can device data be collected without consent?

The conducted review of Art. 5 (3) ePrivacy Directive has revealed that there is very limited potential to rely on exemptions from consent when collecting device data for OBA purposes. Unfortunately, the current wording of ePrivacy Directive does not allow for first-party analytics to be performed under an exemption. Nonetheless this deficit has been acknowledged and will likely be remedied in Art. 8 ePrivacy Regulation, which is planned to include an exemption for audience measuring and fraud prevention.

Is OBA necessary for contract performance?

As regards lawfulness of RTB data processing under GDPR, the concept of "strict necessity" mostly prevents data controllers from claiming that data processing for OBA purposes is necessary to perform a contract with the data subject. According to the majority view, Art. 6 (1) (b) GDPR requires a close proximity to exist between the objectives of the contract and the data processing performed. Such an immediate link is not present if the processing of personal data to enable behaviourally targeted advertising is merely necessary in a general sense to support the business model of the data controller.

I have partially challenged the rationale of such a narrow interpretation of Art. 6 (1) (b) GDPR. Of course, not every processing can be justified by contract performance and proportionality must always be sought. Nonetheless, I believe that in principle, the restrictive approach overlooks the indisputable additional value that ad-funded services generate for consumers. In my view, acknowledging this value and allowing consumers to consciously limit their right to privacy in exchange for free services would better reflect the reality of the transactions that occur in online environments. Conversely, when one recalls the inherent deficiencies of consent, the tendency to push service providers towards collecting consents no longer seems so well justified. In addition, in situations where for some reason a subscription-based business model is not a viable option (e.g. if it would clearly disadvantage the provider against its competitors), the requirement of consent forces providers to resort to dark patterns, since failure to acquire consents could effectively drive them out of business. Ultimately, privacy is not the only value that is at stake. In my view, DPA's sometimes tend to forget that they are not the ones best positioned to decide, whether the consumer will benefit more from a higher level of privacy or from the access to free services that can otherwise improve the consumer's life.

Additional authority guidance on Art. 6 (1) (b) is expected to come in 2023. In addition to the CJEU's upcoming judgment in *Meta Platforms v Bundeskartellamt*, on 6 December 2022, the EDPB adopted three binding decisions under the Art. 65 dispute-resolution meachanism concerning the lawfulness of processing for OBA purposes on Facebook, Instagram, and WhatsApp. According to news reports[272], the final decision to be delivered by the Irish DPC could set a record in GDPR fine size.

Is OBA necessary for legitimate interests?

Considering that Art. 6 (1) (f) GDPR requires the controller to perform a balancing test on a case-by-case basis, there is no straightforward answer to this question. Nonetheless, in view of the enormous scale of the data sharing involved and the potential serious consequences

[272] SCHECHNER, Sam. Meta's targeted ad model faces restrictions in Europe [online]. The Wall Street Journal, 6 December 2022 [viewed 19 December 2022. Available from: https://www.wsj.com/articles/metas-targeted-ad-model-faces-restrictions-in-europe-11670335772

of the processing, the lack of safeguards against function creep, the nature and extent of the data collected, and the insufficient understanding of the processing on the side of consumers, the processing of personal data carried out in RTB ecosystems does not seem to be proportionate.

Yet, that does not mean that no form of OBA can be justified by legitimate interests. For example, a minimalistic version of RTB that would not allow advertisers to identify the data subject, would carefully observe the principles of data minimization and purpose limitation and ensure a sufficient level of transparency and user control could theoretically pass the balancing test. Furthermore, legitimate interests could potentially justify some of the less problematic processing operations ancillary to RTB such as the recording of user consent by CMPs, measuring ad performance, ad fraud prevention, or the sole act of bidding on impressions (provided that no additional processing of the bid request data is involved).

Does user consent justify OBA?

While consent is commonly regarded as the most appropriate legal basis for OBA under both GDPR end ePrivacy Directive, upon a closer look at the requirements prescribed by Art. 4 and 7 GDPR, it appears that in practice, even consent may cause problems. In particular, data controllers engaged in OBA often fail to consider that the requirements for consent expand hand in hand with the extent of the processing. The more intrusive the processing is, the more effort is required from the controller to alert the data subjects to its potential consequences and assist them with exercising effective control over their personal data. In line with the principle of privacy-by-design, controllers that wish to rely on consent to justify high-risk data processing could even be required to implement "privacy nudges" to compensate for users' negative behavioural tendencies, biases, and inherent incapacity to make rational choices when asked for consent in online environments.

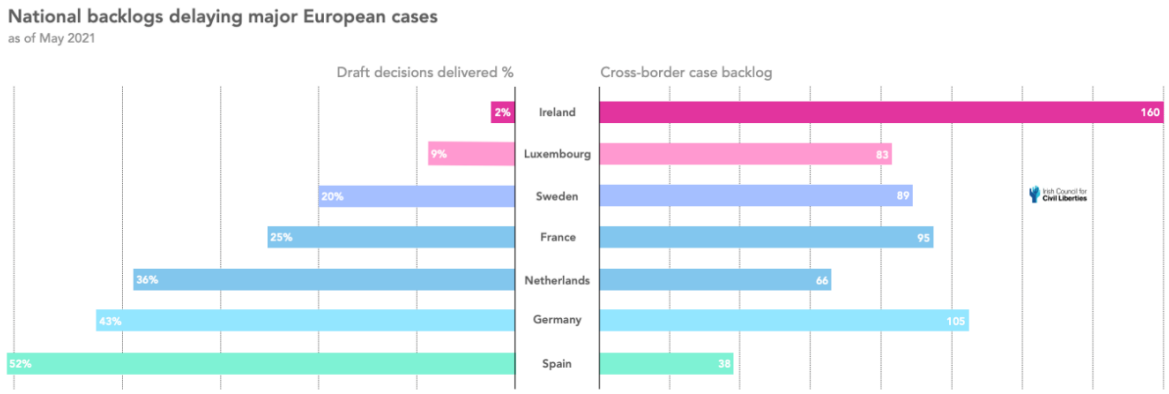
It is also important to note that the responsibility for compliance always sits with the controller. Therefore, controllers that receive data from RTB exchanges without directly interacting with the user should not expect to rely on contractual guarantees provided by other OBA players. In case of an inspection or an action brought by a data subject, they will be the

ones that need to demonstrate a valid consent covering all the data processing activities performed.

What are the broader implications?

The likely root of the problem is that AdTech vendors are economically incentivized to engage in intrusive data processing and cannot afford to downsize their data processing without endangering their economic goals. To avoid the costs associated with privacy compliance, they instead wilfully blind themselves to the fact that the processing may no longer be compatible with internet user's fundamental rights.

Unfortunately, this has been in part possible due to leniency in GDPR enforcement. In particular, the Irish DPC – the lead supervising authority for some of the Europe's largest advertising companies including Google and Meta – is often criticised for its lack of action against blatant infringements in the AdTech sector[273]. In its 2021 report titled "Europe's enforcement paralysis", the ICCL warns that some of the EU's DPA's are consistently falling behind on their enforcement duties[274].



The graph provided in the ICCL report compares the number of decisions delivered by the 7 EU DPA's that most frequently receive cross-border referrals under the GDPR's one-stop-shop mechanism against the number of referrals submitted to those authorities[275]*. The main*

[273] In its report, ICCL informs that in 2021, almost all (98%) major GDPR cases referred to the Irish DPC still remained unresolved
[274] RYAN, Dr Johnny and TONER, Alan, 2021, Europe's enforcement paralysis: ICCL's 2021 GDPR Report on the enforcement capacity of data protection authorities. *Irish Council for Civil Liberties* [online]. 13 April 2022. [viewed 19 December 2022]. Available from: https://www.iccl.ie/digital-data/2021-gdpr-report/
[275] *ibid*., p. 6

takeaway is that, as of May 2021, the Irish DPC has addressed only 2% of its cross-border case backlog.

As demonstrated by the above graph, the GDPR's one-stop-shop mechanism further amplifies the gap in enforcement. Since investigations into data-handling practices of large AdTech companies may only be carried out by their lead supervising authority, large-scale infringements may be swept under the carpet if these authorities fail to act. For this reason, data protection is becoming an increasing focus of anti-trust authorities that are not bound by the same restrictions and operate independently in each member state. For instance, in 2019. the German Bundeskartellamt prohibited Meta from compiling data gathered from Facebook, Instagram and WhatsApp mainly on the grounds that Meta failed to acquire a sufficient legal basis for the processing under GDPR[276]. The Bundeskartellamt considered that, while it was not competent to issue corrective measures under the GDPR, the practice also constituted a breach of German laws against the abuse of dominant position. The UK CMA's extensive investigation into OBA also hints that the CMA is also about to take a stance against malpractice in the AdTech sector[277]. After Meta's appeal, the main questions of the Bundeskartellamt ruling have now been referred to the CJEU. If the CJEU decides to follow the opinion of Advocate General Rantons issued in September 2022, a second line of data protection enforcement could be established under national competition rules[278].

It appears that the AdTech sector has skipped its classes on privacy compliance for far too long. As a result, the privacy deficiencies are deeply rooted in RTB systems and correcting the shortcomings will take nothing less than a complete overhaul of current digital advertising ecosystems. This considered, introducing real privacy compliance into OBA will be an extremely laboursome and complicated task that will require various contradictory values to be weighed against each other. On the one hand, there is urgent for consumer protection. On the other hand, any action against RTB is bound to impact thousands of companies around the world and create significant negative economic externalities.

[276] German Bundeskartellamt decision no. B6-22/16 of 6 February 2019.
[277] UK Competition & Markets Authority. *Online platforms and digital advertising. Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[278] Opinion of the CJEU Advocate General Rantos of 20 September 2022 in Case C-252/21, *Meta Platforms v Bundeskartellamt*

One thing is certain – the time to act is now. With the turmoil caused by the phase-out of third-party cookies, OBA players are currently rethinking their advertising strategies and looking out for new technologies that will support their goals while ensuring privacy compliance. As the UK ICO rightly points out, these "*new proposals need to be designed with data protection by design and default considerations from the beginning [and] need to reconcile the objectives of advertising and measurement with an approach that reduces the privacy risks and harms to user*"[279]. Clearly, there is no simple remedy to achieve the ambitious goal of efficient but privacy-focused online advertising. To support the AdTech industry's journey towards privacy compliance there is urgent need for technological advancement, clarification of disputed aspects of the existing law as well as its more vigilant enforcement by supervising authorities.

Finally, AdTech companies deciding on the next steps in their privacy compliance strategy must realize that the potential cost for disregarding user privacy is not limited to sanctions imposed by supervising authorities. According to recent studies[280], consumers react negatively to excessive surveillance, resulting in their unwillingness to disclose data or engage with privacy-intrusive ads. Thus, by improving ad effectiveness and general brand perception, respecting user privacy could result in positive outcomes not only for the fundamental rights of the people concerned but also for the economic interests of advertisers.

[279] ICO. *Data protection and privacy expectations for online advertising proposals* [online] 25 November 2021. Available from: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf

[280] KIM, Tami, Kate BARASZ, and Leslie JOHN. Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness [online]. Journal of Consumer Research, February 2019, 45, no. 5, 906–932 [viewed 19 December 2022]. Available from: https://dash.harvard.edu/handle/1/41971554

List of abbreviations

AG	Advocate General
API	application programming interface
ATD	agency trading desk
ATT	Apple's App Tracking Transparency framework
CDN	content delivery network
CJEU	the Court of Justice of the European Union
CMA	the UK's Competition and Markets Authority
CMP	consent management platform
CNIL	the French Commission Nationale de l'Informatique et des Libertes
DMP	data management platform
DPA	data protection authority
DPC	the Irish Data Protection Commission
DSP	demand side platform
ECtHR	the European Court of Human Rights
EDPB	the European Data Protection Board
EDPS	the European Data Protection Supervisor
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
ePrivacy Regulation	COM (2017) 10: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
GVL	the TCF Global Vendor List

IAB	the Interactive Advertising Bureau
IAB Ruling	decision 21/2022 of the Belgian DPA of 2 February 2022
ICCL	the Irish Council for Civil Liberties
ICO	the UK's Information Commissioner's Office
IP	Internet Protocol
ISSP	information society services provider
OBA	online behavioural advertising
RTB	real-time bidding
SDK	software developer kit
SSP	supply-side platform
TCF	IAB Europe's Transparency and Consent Framework
UK	The United Kingdom of Great Briton and Northern Ireland
Unfair Contract Terms Directive	Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
WP29	the Article 29 Working Party

Additional terms commonly used in the AdTech industry are explained in Chapter 1.2 hereof.

List of sources

EU LAWS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
- Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
- COUNCIL OF THE EUROPEAN UNION. Interinstitutional file 2017/0003(COD), Council of the European Union mandate ST 6087 2021 INIT of 10 February 2021, available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

CZECH LAWS

- Charter of Fundamental Rights and Freedoms of the Czech Republic.
- Act No. 127/2005 Coll., Electronic Communications Act.
- Act No. 89/2012 Coll., the Civil Code.

OTHER LAWS

- Charter of Fundamental Rights of the European Union.
- European Convention on Human Rights.

EU CASE LAW

- CJEU judgment in Case C-131/12 of 13 May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317.
- CJEU judgment in Case C-101/01 of 6 November 2003, *Göta hovrätt (Sweden)* v *Bodil Lindqvist*, ECLI:EU:C:2003:596.
- CJEU judgment in Joined cases C-141/12 and C-372/12 of 17 July 2014, *YS and M, S v Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081.
- CJEU judgment in Case C-434/16 of 20 December 2017, *Peter Nowak v Data Protection Commissioner (Ireland)*, ECLI:EU:C:2017:994.
- CJEU judgment in Case C-582/14 of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
- CJEU judgment in Case C-184/20 of 1 August 2022, *OT v Chief Official Ethics Commission Lithuania*, ECLI:EU:C:2022:601.
- CJEU judgment in Case C-210/16 of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.

- CJEU judgment in Case C-25/17 of 10 July 2018, *Jehovah's Witnesses Community*, ECLI:EU:C:2018:551.
- CJEU judgment in Case C-40/17 of 29 July 2019, *Fashion ID*, ECLI:EU:C:2019:629.
- CJEU judgment in Case C-13/16 of 4 May 2017, *Rīgas satiksme*, ECLI:EU:C:2017:336.
- CJEU judgment in Joined Cases C-293/12 and C-594/12 of 8 April 2014, *Digital Rights Ireland*, ECLI:EU:C:2014:238.
- CJEU judgment in Case C-673/17 of 1 October 2019, *Planet49 GmbH*, ECLI:EU:C:2019:801.
- Opinion of the CJEU Advocate General Rantos of 20 September 2022 in Case C-252/21, *Meta Platforms v Bundeskartellamt.*

OTHER CASE LAW

- European Court of Human Rights (GC), *Rotaru v. Romania*, no. 28341/95, ECHR 2000-V.
- European Court of Human Rights (GC) judgment of 7 February 2012 on Application no. 39954/08, *Axel Springer AG v. Germany*
- Czech Constitutional Court judgment No. Pl. ÚS 24/10 of 22 March 2011.
- Judgment of the Supreme Court of the Czech Republic no. 8 Tdo 307/2020-873 of 24 March 2020
- Judgment of the Regional court in Ústí nad Labem no. 45 ICm 4182/2014-35 of 30 October 2015
- England and Wales Court of Appeal, [2015] EWCA Civ 311 of 27 March 2015, *GOOGLE INC. and Judith Vidal-Hall Robert Hann Marc Bradshaw and the Information Commissioner.*

DPA DECISIONS

- Autorité de protection des données Gegevensbeschermingsautoriteitesicion decision 21/2022 of 2 February 2022, Case No. DOS-2019-01377.
- Commission Nationale de l'Informatique et des Libertés decision No. MED-2018-042 of 30 October 2018.
- Commission Nationale de l'Informatique et des Libertés decision restricted committee No. SAN-2021-024 of 31 December 2021 concerning Facebook Ireland Limited
- Datatilsynet decision no. 20/02136-18 of 13. December 2021.
- Irish DPC decision of 2 September 2022, Inquiry Reference: IN-20-7-4.
- Datenschutzbehörde decision of 30 November 2018, no. DSB-D122.931/0003-DSB/2018.
- German Bundeskartellamt decision no. B6-22/16 of 6 February 2019.

AUTHORITY GUIDANCE

- EUROPEAN COMMISSION. Commission Staff Working Document, Impact Assessment, SWD(2017) 3 final, 10 January 2017, Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:bb21abb2-d809-11e6-ad7c-01aa75ed71a1.0001.02/DOC_1&format=PDF
- EUROPEAN COMMISSION. Letter to the Dutch DPA of 6 March 2020, Ref. Ares(2020)1417369
- EDPB. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, 14 March 2022, version 1.0.
- EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 July 2021, version 2.0.
- EDPB. *Guidelines 8/2020 on the targeting of social media users*, 13 April 2021, version 2.0.

- EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020, version 1.1.
- EDPB. *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, 12 March 2019.
- EDPB. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 20 October 2020, Version 2.0.
- EDPB. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019, version 2.0.
- WP29. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, 3 October 2017.
- WP29. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*, 25 November 2014.
- WP29. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014.
- WP29, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014.
- WP29. *Opinion 02/2013 on apps on smart devices, 27 February* 2013.
- WP29. *Opinion 04/2012 on Cookie Consent Exemption*, 7 June 2012.
- WP29. *Opinion 2/2010 on online behavioural advertising*, 22 June 2010.
- WP29. *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, 8 December 2011.
- WP29. *Opinion 4/2007 on the concept of personal data*, 20 June 2007.
- EDPS. *Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions*, November 2016.
- EDPS. *Guidelines on the protection of personal data processed through web services provided by EU institutions*, November 2016.

- ICO. *Data protection and privacy expectations for online advertising proposals* [online] 25 November 2021. Available from: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf
- ICO. *Update report into adtech and real time bidding* [online]. 20 June 2019. Available from: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
- ICO. *Summary report of adtech Fact Finding Forum, held 6 March 2019* [online]. ICO, 2019 [viewed 19 December 2022]. Available from: https://ico.org.uk/about-the-ico/research-and-reports/adtech-fact-finding-forum/
- ICO. *ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry* [online]. ICO, 25 November 2021 [viewed 19 December 2022]. Available from: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/
- ICO. *Anonymisation, pseudonymisation and privacy enhancing technologies guidance* [online] ICO, 7 September 2022 [viewed 19 December 2022]. Available from: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/
- ICO. What is the 'legitimate interests' basis? *Guide to the General Data Protection Regulation (GDPR)* [online] [viewed 19 December 2022]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test
- ICO. How should we obtain, record and manage consent? *Guide to the General Data Protection Regulation (GDPR)* [online] [viewed 19 December 2022]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/#how1

- UK Competition & Markets Authority. *Online platforms and digital advertising*. *Market study final report.* 1 July 2020. Available from: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
- ECtHR. Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence [online]. 31 August 2021. Available from: https://www.echr.coe.int/documents/guide_art_8_eng.pdf
- OECD. *Competition in digital advertising markets* [online]. OECD, 2022. [viewed 19 December 2022]. Available from: https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf
- DATENSCHUTZBEHÖRDE. FAQ zum Thema Cookies und Datenschutz [online]. 25 May 2022 [viewed 19 December 2022]. Available from: https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html#Frage_6
- CNIL. Cookie walls: la CNIL publie des premiers critères d'évaluation [online]. 16 May 2022 [viewed 19 December 2022]. Available from: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation
- IRISH DPC. Report by the Data Protection Commission on the use of cookies and other tracking technologies [online]. Data Protection Commission, 6 April 2020 [viewed 19 December 2022]. Available from: https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf

EMPIRICAL RESEARCH

- CLEARCODE. *The AdTech Book* [online]. Katowice: Clearcode S.A., February 2022 [viewed 23 August 2022]. Available from: https://adtechbook.clearcode.cc/
- BASHIR, Muhammad Ahmad, and Christo WILSON. Diffusion of User Tracking Data in the Online Advertising Ecosystem. *Proceedings on Privacy Enhancing Technologies* [online]. 2018, 2018(4), 85–103 [viewed 19 December 2022]. ISSN 2299-0984. Available from: doi:10.1515/popets-2018-0033

- BASHIR, Muhammad Admad. *On the privacy implications of Real time bidding* [online]. Northeastern University, Boston, Massachusetts, August 2019 [viewed 19 December 2022]. DOI 10.17760/d20321280. Available from: https://www.ccs.neu.edu/home/ahmad/publications/bashir-thesis.pdf

- BASHIR, Muhammad Ahmad, et al. Tracing Information Flows Between Ad Exchanges Using Retargeted Ads [online]. In: Proceedings of the 25th USENIX Security Symposium, 10-12 August 2016, Austin, TX. Austin, Texas: USENIX, August 2016. ISBN 978-1-931971-32-4. Available from: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_bashir.pdf

- WANG, Jun, Weinan ZHANG, and Shuai YUAN. Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting. *Foundations and Trends® in Information Retrieval* [online]. 2017, 11(4-5), 297–435 [viewed 19 December 2022]. ISSN 1554-0677. Available from: doi:10.1561/1500000049

- PAPADOPOULOS, Panagiotis, KOURTELLIS, Nicolas and MARKATOS, Evangelos, 2019, Cookie synchronization: Everything you always wanted to know but were afraid to ask [online]. Proceedings of the 2018 World Wide Web Conference (WWW'19) [viewed 19 December 2022]. DOI 10.1145/3308558.3313542. Available from: https://arxiv.org/abs/1805.10505

- BINNS, Reuben, LYNGS, Ulrik, VAN KLEEK, Max, ZHAO, Jun, LIBERT, Timothy and SHADBOLT, Nigel, 2018, Third party tracking in the mobile ecosystem [online]. *Proceedings of the 10th ACM Conference on Web Science*. 2018. DOI 10.1145/3201064.3201089. Available from: https://arxiv.org/pdf/1804.03603.pdf

- BUSCH, Oliver, ed. *Programmatic Advertising* [online]. Cham: Springer International Publishing, 2022 [viewed 18 December 2022]. ISBN 9783319250212. Available from: doi:10.1007/978-3-319-25023-6

- EVANS, David S. The Economics of Attention Markets [online]. *SSRN Electronic Journal*, April 2020. Available at SSRN: https://ssrn.com/abstract=3044858

- KARAJ, Arjaldo, Sam MACBETH, Rémi BERSON and Josep M. PUJOL. *WhoTracks.Me: Shedding light on the opaque world of online tracking* [online].

Computers and Society, arXiv:1804.08959, 25 April 2019. Available from: https://arxiv.org/abs/1804.08959

- VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden) [online]. Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284

- WEFERS BETTINK, W., VAN EIJK, R., & WAGNER, F. Strictly Speaking: Cookies, Consent and Compliance. Europe Data Protection congress [presentation]. Brussels: IAPP, 2012. as cited in VAN EIJK, Rob. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden). Amsterdam: Ipskamp Printing, 29 January 2019. ISBN 978 94 028 1323 4, 2019, Available at SSRN: https://ssrn.com/abstract=3319284

- JANC, Artur and Michal ZALEWSKI. Technical analysis of client identification mechanisms [online]. The Chromium Projects, wiki page [viewed 7 September 2022]. Available from: https://www.chromium.org/Home/chromium-security/client-identification-mechanisms/#explicitly-assigned-client-side-identifiers

- SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely [online]. Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper 3., 2000 [viewed 19 December 2022]. Available from: https://dataprivacylab.org/projects/identifiability/paper1.pdf

- KOSINSKI, Michal, STILLWELL, David and GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior [online]. Proceedings of the National Academy of Sciences, April 2013, 110 (15), 5802–5805. DOI: 10.1073/pnas.1218772110. Available from: https://www.pnas.org/doi/10.1073/pnas.1218772110

- YOUYOU, Wu, KOSINSKI, Michal and STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans [online]. Proceedings of the National Academy of Sciences, January 2015. 112 (4), 1036–1040. DOI: 10.1073/pnas.1418680112. Available from: https://www.pnas.org/doi/10.1073/pnas.1418680112

- KIM, Tami, Kate BARASZ, and Leslie JOHN. Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness [online]. Journal of Consumer Research, February 2019, 45, no. 5, 906–932 [viewed 19 December 2022]. Available from: https://dash.harvard.edu/handle/1/41971554

LEGAL BOOKS AND JOURNALS

- ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.
- VEALE, Michael and ZUIDERVEEN BORGESIUS, Frederik, 2022, Adtech and Real-Time Bidding under European Data Protection Law [online]. *German Law Journal*. 2022. Vol. 23, no. 2p. 226–256. DOI 10.1017/glj.2022.18.
- LEISER, Dr Mark. 'Dark Patterns': The Case for Regulatory Pluralism. *SSRN Electronic Journal* [online]. 2020 [viewed 18 December 2022]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.3625637
- BOERMAN, Sophie C., Sanne KRUIKEMEIER, and Frederik J. ZUIDERVEEN BORGESIUS. Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising* [online]. 2017, 46(3), 363–376 [viewed 18 December 2022]. ISSN 1557-7805. Available from: doi:10.1080/00913367.2017.1339368
- DOCKSEY, C., and H. HIJMANS. The Court of Justice as a Key Player in Privacy and Data Protection. *European Data Protection Law Review* [online]. 2019, 5(3), 300–316 [viewed 18 December 2022]. ISSN 2364-284X. Available from: doi:10.21552/edpl/2019/3/6
- SANTOS, Cristiana, et al. Consent Management Platforms Under the GDPR: Processors and/or Controllers? *SSRN Electronic Journal* [online]. 2021 [viewed 18 December 2022]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4205933
- NIKIFORAKIS, N., KAPRAVELOS, A., JOOSEN, W., KRUEGEL, C., PIESSENS, F. and VIGNA, G., 2013, Cookieless Monster: Exploring the ecosystem of web-based device fingerprinting [online]. *2013 IEEE Symposium on Security and Privacy*. 2013. DOI 10.1109/sp.2013.43.

- ZUIDERVEEN BORGESIUS, Frederik J. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* [online]. 2015, 5(3), 163–176 [viewed 18 December 2022]. ISSN 2044-4001. Available from: doi:10.1093/idpl/ipv011

- ZUIDERVEEN BORGESIUS, Frederik J., et al. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review* [online]. 2017, 3(3), 353–368 [viewed 19 December 2022]. ISSN 2364-284X. Available from: doi:10.21552/edpl/2017/3/9

- CHRISTL, Wolfie and SPIEKERMANN, Sarah. *Networks of control a report on corporate surveillance, Digital Tracking, Big Data & Privacy*. Wien: facultas [online]. January 2016. ISBN: 978-3-7089-1473-2.

- LAUX, Johann, Sandra WACHTER, and Brent MITTELSTADT. Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review* [online]. 2021, 58(Issue 3), 719–750 [viewed 18 December 2022]. ISSN 0165-0750. Available from: doi:10.54648/cola2021048

- FINCK, Michèle, and Frank PALLAS. They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law* [online]. 2020, 10(1), 11–36 [viewed 18 December 2022]. ISSN 2044-4001. Available from: doi:10.1093/idpl/ipz026

- SOH, S. Y. Privacy Nudges. *European Data Protection Law Review* [online]. 2019, 5(1), 65–74 [viewed 18 December 2022]. ISSN 2364-284X. Available from: doi:10.21552/edpl/2019/1/10

- ZUIDERVEEN BORGESIUS, Frederik J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review* [online]. 2016, 32(2), 256–271 [viewed 18 December 2022]. ISSN 0267-3649. Available from: doi:10.1016/j.clsr.2015.12.013

- GERADIN, Damien and Dimitrios KATSIFIS. An EU Competition law Analysis of Online Display Advertising in the Programmatic Age [online]. TILEC Discussion Paper No. DP2019-031, 12 December 2018 [viewed 19 December 2022]. Available at SSRN: https://ssrn.com/abstract=3299931 or http://dx.doi.org/10.2139/ssrn.3299931

OTHER PUBLICATIONS

- RYAN, Dr Johnny. *RTB Header Bidder Evidence – Explanatory Document* [online]. Brave Software, Inc., 2 September 2019. [viewed 19 December 2022]. Available from: https://brave.com/static-assets/files/explanatory_note_google_RTB_and_push_pages.pdf

- RYAN, Dr Johnny. *Report from Dr Johnny Ryan – Behavioural advertising and personal data* [online]. Brave Software, Inc., 5 September 2018. [viewed 19 December 2022]. Available from: https://brave.com/static-assets/files/Behavioural-advertising-and-personal-data.pdf

- AMNESTY INTERNATIONAL LTD. *Surveillance giants: How the business model of Google and Facebook threatens human rights* [online]. London: Amnesty International, November 2019. [viewed 19 December 2022]. Index: POL 30/1404/2019.

- RYAN, Dr Johnny and TONER, Alan, 2021, Europe's enforcement paralysis: ICCL's 2021 GDPR Report on the enforcement capacity of data protection authorities. *Irish Council for Civil Liberties* [online]. 13 April 2022. [viewed 19 December 2022]. Available from: https://www.iccl.ie/digital-data/2021-gdpr-report/

- ARGENTESI, Elena, Paolo BUCCIROSSI, Emilio CALVANO, Tomaso DUSO, Alessia MARRAZZO, and Salvatore NAVA. *Ex-post assessment of merger control decisions in digital markets* [online]. Rome: Lear, 9 May 2019. [viewed 19 December 2022]. Available from: https://www.learlab.com/publication/ex-post-assessment-of-merger-control-decisions-in-digital-markets/

- LEMOINE, Laureline et al. *Targeted Online – An industry broken by design and by default* [online]. Brussels: European Digital Rights (EDRi), 9 March, 2021. [viewed 19 December 2022]. Available from: https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf

- MYRSTAD, Finn and Ingvar TJØSTHEIM. *Time to ban surveillance-based advertising. The case against commercial surveillance online* [online]. Oslo: Forbrukerrådet, June 2021. [viewed 19 December 2022]. Available from:

https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.

- DENTSU et al. *Unlocking the new currency of Attention* [online]. United Kingdom: dentsu, 12 May 2021. [viewed 19 December 2022]. Available from: https://www.dentsu.com/uk/en/our-latest-thinking/unlocking-the-new-currency-of-attention

- KEPIOS, WE ARE SOCIAL, and HOOTSUITE. *Digital 2022 Global Overview Report* [online]. 2022. [viewed 19 December 2022]. Available from: https://www.hootsuite.com/resources/digital-trends

- IAB EUROPE. *ADEX Benchmark 2021 Report* [online]. IAB Europe, June 2022. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2022/06/IAB-Europe_AdEx-Benchmark-2021_REPORT.pdf

- IHS MARKIT. *The economic value of behavioural targeting in digital advertising* [online]. IHS Markit, September 2017. [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2019/08/BehaviouralTargeting_FINAL.pdf

- INTEGRAL AD SCIENCE. *Media Quality Report, 16th Edition* [online]. Integral Ad Science, March 2022. [viewed 19 December 2022]. Available from: https://integralads.com/insider/media-quality-report-16th-edition/

- LUMA PARTNERS LLC. *Display LUMAscape* [online]. Luma Partners LLC, 2022. [viewed 30 August 2022]. Available from: https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/

- PRICEWATERHOUSECOOPERS LLP. *Programmatic Supply Chain Transparency Study* [online]. London: The Incorporated Society of British Advertisers Ltd, May 2020 [viewed 19 December 2022]. Available from: https://www.isba.org.uk/system/files?file=media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf

- IAB EUROPE. *What would an internet without targeted ads look like?* [online]. IAB Europe, March 2021 [viewed 19 December 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2021/04/IAB-Europe_What-Would-an-Internet-Without-Targeted-Ads-Look-Like_April-2021.pdf

- GFK. *Europe online: an experience driven by advertising* [online]. GfK, September 2017 [viewed 19 December 2022]. Available from: https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf
- GREENWICH CAPITAL GROUP. *Industry Update. Adtech & Marketing Services Q4 2021* [online]. 2022 [viewed 19 December 2022]. Available from: https://greenwichgp.com/wp-content/uploads/2022/03/AdTech-and-Marketing-Services-Industry-Update-Q4-2021.pdf
- KREIKEN, Floris. *Transparent Consumers. Data brokers and profiling in the Netherlands* [online]. Amsterdam: Stichting Bits of Freedom, 4 February 2016 [viewed 19 December 2021]. Available from: https://www.edri.org/files/transparent-consumers-bits-of-freedom.pdf
- LUPIÁÑEZ-VILLANUEVA, Francisco et al. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation* [online]. Brussels: European Innovation Council and SMEs Executive Agency (EISMEA), European Commission, April 2022. Available from: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418
- BRAVE. Google publisher verticals marked-up [online]. Brave Software, Inc. [viewed 19 December 2021]. Available from: https://brave.com/static-assets/files/Google-publisher-verticals-marked-up.pdf
- RAVICHANDRAN, Deepak and Nitish KORULA. *Effect of disabling third-party cookies on publisher revenue* [online]. Google Inc., 27 August 2019 [viewed 19 December 2021]. Available from: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf
- GOOGLE. Authorized Buyers Real-time Bidding Proto [online]. Google, 2022 [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide

- GOOGLE. Authorized Buyers Help [online] [viewed 28 August 2022]. Available from: https://support.google.com/authorizedbuyers/?visit_id=637985105897694840-1257107195&hl=en&rd=1#topic=22149
- GOOGLE. Cookie Matching. *Authorized Buyers*. [online] [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/cookie-guide#bidder-initiated:-bidirectional-cookie-matching
- GOOGLE. The Privacy Sandbox [online]. 28 March 2022 [viewed 19 December 2022]. Available from: https://www.google.com/doubleclick/adxbuyer/guidelines/
- GOOGLE. Authorized Buyers Program Guidelines [online] [viewed 19 December 2022]. Available from: https://privacysandbox.com/intl/en_us/
- IAB TECH LAB. OpenRTB Version 2.6 [online]. IAB Technology Laboratory, April 2022 [viewed 28 August 2022]. Available from: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide
- IAB TECH LAB. Content Taxonomy [online]. IAB Technology Laboratory [viewed 28 August 2022]. Available from: https://iabtechlab.com/standards/content-taxonomy/
- IAB EUROPE. Consent Management Platform API. *IAB Europe Transparency & Consent Framework* [online]. IAB Europe, September 2021 [viewed 28 August 2022]. Available from: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20CMP%20API%20v2.md
- IAB EUROPE. *The IAB Europe Guide to Ad Fraud* [online]. IAB Europe, December 2020 [viewed 28 August 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2020/12/IAB-Europe-Guide-to-Ad-Fraud-1.pdf
- IAB EUROPE. *The IAB Europe Guide to Brand Safety and Suitability* [online]. IAB Europe, December 2020 [viewed 28 August 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2020/07/IAB-Europe-Brand-Safety-and-Brand-Suitability-Guide_July-2020.pdf

- IAB EUROPE. *The IAB Europe Guide to Quality* [online]. IAB Europe, December 2020 [viewed 28 August 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2021/09/IAB-Europe-Guide-to-Quality-September-2021.pdf
- IAB EUROPE. *GDPR Guidance: Legitimate Interests Assessments (LIA) for Digital Advertising* [online]. IAB Europe, December 2020 [viewed 28 August 2022]. Available from: https://iabeurope.eu/wp-content/uploads/2021/03/IAB-Europe-GDPR-Guidance-Legitimate-Interests-Assessments-LIA-for-Digital-Advertising-March-2021.pdf
- IRISH COUNCIL FOR CIVIL LIBERTIES. *The Biggest Data Breach* [online]. Dublin: 16 May 2022 [viewed 19 December 2022]. Available from: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
- GEBHART, Bennett Cyphers and Gennie, 2021, Behind the one-way mirror: A deep dive into the technology of Corporate Surveillance. *Electronic Frontier Foundation* [online]. 10 February 2021. [viewed 19 December 2022]. Available from: https://www.eff.org/wp/behind-the-one-way-mirror
- FOU, Augustine. *Impact of Loss of 3P Cookies on Publishers' Ad Revenue* [online]. Medium, 30 April 2021 [viewed 19 December 2022]. Available from: https://acfou.medium.com/abstract-2fefd374edb2
- EPSILON. Preparing for a world without third-party cookies [online]. Epsilon Data Management, LLC, 27 October 2020 [viewed 19 December 2022]. Available from: https://www.epsilon.com/us/insights/resources/research-preparing-for-a-world-without-third-party-cookies
- WORLEDGE, Michael and Mike BAMFORD. Adtech Market Research Repor [online]. ICO, March 2019 [viewed 19 December 2022]. Available from: https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

INTERNET ARTICLES AND WEBSITES

- ARRIETA, Andrés. Facebook's Laughable Campaign Against Apple Is Really Against Users and Small Businesses [online]. 18 December 2020 [viewed 19 December 2022]. Available from: https://www.eff.org/deeplinks/2020/12/facebooks-laughable-campaign-against-apple-really-against-users-and-small

- BRAVE SOFTWARE and Dr Johhny RYAN. New evidence to regulators: IAB documents reveal that it knew that real-time bidding would be "incompatible with consent under GDPR". *Brave Browser* [online]. 20 February 2019 [viewed 19 December 2022]. Available from: https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/

- HUNTON ANDREWS KURTH LLP. *CNIL Proposes 60 Million Euros Fine Against French AdTech Company For Non-Compliance with GDPR* [online]. Hunton Andrews Kurth LLP, 17 August 2022 [viewed 19 December 2022]. Available from: https://www.huntonprivacyblog.com/2022/08/17/cnil-proposes-60-million-euros-fine-against-french-adtech-company-for-non-compliance-with-gdpr/

- DATA PROTECTION COMMISSION. *Data Protection Commission opens statutory inquiry into Google Ireland Limited* [online]. 22 May 2019 [viewed 19 December 2022]. Available from: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited

- IRISH COUNCIL FOR CIVIL LIBERTIES. *ACTION FILE: RTB online ad auctions* [online][viewed 19 December 2022]. Available from: https://www.iccl.ie/rtb/

- BRAVE. *RTB evidence* [online][viewed 19 December 2022]. Available from: https://brave.com/rtb-evidence/

- FIX ADTECH. *Appendix on market saturation of the systems* [online]. 4 February 2019 [viewed 19 December 2022]. Available from: https://fixad.tech/wp-content/uploads/2019/02/4-appendix-on-market-saturation-of-the-systems.pdf

- FIX ADTECH. *Ad Tech GDPR complaint is extended to four more European regulators* [online]. 20 May 2019 [viewed 19 December 2022]. Available from: https://fixad.tech/ad-tech-gdpr-complaint-is-extended-to-five-more-european-regulators/

- WIGGERS, Kyle. Google delays move away from cookies in Chrome to [online]. 27 July 2022 [viewed 19 December 2022]. Available from: https://techcrunch.com/2022/07/27/google-delays-move-away-from-cookies-in-chrome-to-2024/
- GOOGLE. *About automated bidding* [online] [viewed 19 December 2022]. Available from: https://support.google.com/google-ads/answer/2979071?hl=en&ref_topic=6294205
- GOOGLE. *Display Network: Definition* [online] [viewed 19 December 2022]. Available from: https://support.google.com/google-ads/answer/117120?hl=en
- GOOGLE. *About data collection controls (Beta)* [online] [viewed 19 December 2022]. Available from: https://support.google.com/google-ads/answer/117120?hl=en
- GOOGLE. *Google Marketing Platform Academy* [online] [viewed 30 August 2022]. Available from: https://support.google.com/admanager/answer/11956152
- GOEL, Vinay. *Get to know the new Topics API for Privacy Sandbox* [online] Google, Chrome, 25 January 2022 [viewed 19 December 2022]. Available from: https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/
- ADBUTLER. *Types of Programmatic Advertising: Deals & Formats Explained* [online]. 9 March 2021 [viewed 19 December 2022]. Available from: https://www.adbutler.com/blog/article/types-of-programmatic-advertising-deals-and-formats-explained
- LOMAS, Natasha. Even the IAB warned Adtech risks EU Privacy Rules [online]. TechCrunch. 21 February 2019. [viewed 19 December 2021]. Available from: https://techcrunch.com/2019/02/21/even-the-iab-warned-adtech-risks-eu-privacy-rules/?guccounter=1
- HA, Anthony. Facebook highlights small businesses as it ramps up Apple criticism [online]. TechCrunch. 16 December 2020. [viewed 19 December 2021]. Available from: https://techcrunch.com/2020/12/16/facebook-apple-small-business/
- Cryptographic hash function [online]. Wikipedia [viewed 19 December 2022]. Available from: https://en.wikipedia.org/wiki/Cryptographic_hash_function

- FRANCESCHI-BICCHIERAI, Lorenzo. *Facebook doesn't know what it does with your data, or where it goes: Leaked document* [online]. *VICE*, 26 April 2022 [viewed 19 December 2022]. Available from: https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

- LARDINOIS, Frederic, 2022, *Google kills off Floc, replaces it with topics* [online]. TechCrunch, 25 January 2022. [viewed 19 December 2022]. Available from: https://techcrunch.com/2022/01/25/google-kills-off-floc-replaces-it-with-topics/

- SWEENEY, Michael and Natalia FIGAS. Google Chrome's Topics API Explained + FAQS [online]. Clearcode, 5 April 2022. [viewed 19 December 2022]. Available from: https://clearcode.cc/blog/google-chrome-topics-explained/

- RYAN, Dr Johnny. Google and IAB's inadequate proposals to reform RTB [online]. 21 January 2020 [viewed 19 December 2022]. Available from: https://brave.com/google-iab-reform/

- SWEENEY, Michael. How Google Chrome's Privacy Sandbox Will Work + Possible Solutions for AdTech [online]. Clearcode, 27 July 2022. [viewed 19 December 2022]. Available from: https://clearcode.cc/blog/chrome-privacy-sandbox-explained/

- RIVERO, Nicolás. The digital ad industry is rewriting the bargain at the center of the internet [online]. Quartz, 25 April 2021 [viewed 19 December 2022]. Available from: https://qz.com/2000490/the-death-of-third-party-cookies-will-reshape-digital-advertising

- THE MEDIAGRID. The publisher brief: OpenRTB 2.6 and the addressable future of CTV [online]. the mediagrid [viewed 19 December 2022]. Available from: https://blog.themediagrid.com/the-publisher-brief-openrtb-2.6-and-the-addressable-future-of-ctv

- ADGUARD. You can hide, but you can't escape: how fingerprinting revolutionized online tracking [online]. AdGuard, 17 August 2022 [viewed 19 December 2022]. Available from: https://adguard.com/en/blog/browser-fingerprinting-gpu.html

- HUGHES, Karl. Fingerprinting in the Modern Browser: Are Privacy Updates Making It Harder to Prevent Fraud? [online]. Chicago: Fingerprint, 25 May 2021 [viewed 19

December 2022]. Available from: https://fingerprint.com/blog/browser-fingerprinting-privacy/

- APPLE INC. About privacy and Location Services in iOS and iPadOS [online] [viewed 19 December 2022]. Available from: https://support.apple.com/en-us/HT203033#:~:text=You%20can%20turn%20Location%20Services,access%20to%20Location%20Services%20data
- APPLE INC. If an app asks to track your activity [online] [viewed 19 December 2022]. Available from: https://support.apple.com/en-us/HT212025
- GHOSTERY GMBH. Doubleclick. *Whotracks.me* [online]. Ghostery GmbH [viewed 19 December 2022] Available from: https://whotracks.me/trackers/doubleclick.html
- HERN, Alex. Cambridge Analytica: how did it turn clicks into votes? [online]. The Guardian, 6 May 2018 [viewed 19 December 2022]. Available from: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
- VON HOFFMAN, Constantine. A statistical picture of the cost of digital advertising fraud [online]. Third Door Media, Inc., MarTech, 9 May 2022 [viewed 19 December 2022]. Available from: https://martech.org/a-statistical-picture-of-the-cost-of-digital-advertising-fraud/
- Brave Browser Privacy Policy [online]. Brave Software, Inc., 12 December 2022 [viewed 19 December 2022]. Available from: https://brave.com/privacy/browser/
- SCHECHNER, Sam. Meta's targeted ad model faces restrictions in Europe [online]. The Wall Street Journal, 6 December 2022 [viewed 19 December 2022. Available from: https://www.wsj.com/articles/metas-targeted-ad-model-faces-restrictions-in-europe-11670335772

Právní aspekty online behaviorální reklamy

Abstrakt

V roce 2022 se reklamní průmysl nachází na pokraji významných změn. Kromě technologických změn spojených s plánovaným zablokováním cookies třetích stran internetovými prohlížeči jsou technologie používané pro online behaviorální reklamu (OBA) stále častěji terčem ostré kritiky ze strany spotřebitelských organizací. Obavy z nedostatečné ochrany soukromí uživatelů při cílení online reklamy se v poslední době začínají promítat také do činnosti dozorových úřadů. V únoru 2022 belgický úřad pro ochranu osobních údajů rozhodl o nezákonnosti zpracování osobních údajů prováděného organizací IAB Europe, která stojí za jedním z největších evropských ekosystémů pro cílení online reklamy. Cílem této práce je posoudit, jaká pravidla stanoví platná právní úprava na ochranu soukromí uživatelů v rámci online behaviorální reklamy, a zhodnotit, zda jsou tato pravidla v praxi dodržována.

Před posouzením jejich právních aspektů bylo nejprve třeba prozkoumat systémy online reklamy z technologického hlediska. První část práce poskytuje úvod do světa reklamních technologií a popisuje fungování real-time bidding (RTB) systémů pro dražby reklamního prostoru v reálném čase, postavení médií, inzerentů a technologických zprostředkovatelů, průběh programatických aukcí, zpracovávané údaje a procesy pro sdílení dat mezi zúčastněnými osobami. Druhá část se zaměřuje na nástroje používané v reklamě k identifikaci a sledování uživatelů online, včetně fixních identifikátorů (jako jsou cookies třetích stran) a metod založených na pravděpodobnosti (jako jsou fingerprinty zařízení).

Následně jsou empirická zjištění poměřena s požadavky GDPR a směrnice ePrivacy. Jako první je posuzována otázka, zda se na data sdílená v RTB vztahuje právní úprava ochrany soukromí. Koncept „přiměřené identifikovatelnosti“ prosazovaný v judikatuře SDEU je přitom aplikován na běžné scénáře online behaviorální reklamy. Dále autor zvažuje, do jaké míry mohou být účastníci RTB procesů odpovědní za zajištění souladu s příslušnými přepisy. Za tímto účelem jsou podrobně zkoumány pojmy „správce“, „zpracovatel“ a „společní správci“, přičemž zvláštní pozornost je věnována roli zprostředkovatelů poskytujících standardizované softwarové nástroje.

V poslední části práce je posuzována otázka zákonnosti prováděného zpracování. Po krátkém představení výjimek dle čl. 5 (3) směrnice ePrivacy se autor podrobně věnuje právním důvodům zpracování dle čl. 6 GDPR. Postupně jsou rozebrány tři právní důvody zpracování, které se potenciálně mohou uplatnit v kontextu online cílené reklamy: plnění smlouvy, oprávněné zájmy a souhlas. V souvislosti s právním důvodem zpracování nezbytného pro plnění smlouvy autor navrhuje alternativní výklad ve vztahu k otázce platby osobními údaji. Závěrem je zpochybněn praktický přínos požadavku na souhlas pro soukromí uživatelů, a to zejména s ohledem na studie poukazující na nedostatečnou informovanost spotřebitelů a rozsáhlé užívání manipulativních uživatelských rozhraní.

Klíčová slova: online behaviorální reklama, real-time bidding, programatická reklama, soukromí uživatelů, GDPR, ePrivacy, ochrana osobních údajů

Legal aspects of Online Behavioural Advertising

Abstract

In 2022, the AdTech industry is on the verge of a significant makeover. In addition to technological changes caused by the phasing out of third-party cookies, real-time bidding systems used for online behavioural advertising (OBA) are subject to fierce criticism by privacy advocacy groups. Moreover, the concerns about privacy deficits in advertising ecosystems are starting to translate into regulatory attention. In February 2022, the Belgian data protection authority sanctioned IAB Europe – the ambassador of one of the largest real-time bidding ecosystems in Europe – for failure to ensure lawful data processing. Considering the recent developments, this paper aims to ascertain how online behavioural advertising is governed by current privacy laws and verify whether the prescribed legal requirements are observed in practice.

Before assessing its legal aspects, it was first necessary to examine online advertising from a technological perspective. The first part of this paper provides an introduction into AdTech and describes the functioning of real-time bidding (RTB) ecosystems, the roles played by publishers, advertisers and AdTech intermediaries, the programmatic bidding process, the data processed and how the data is exchanged between the involved parties. The second part focuses on practices used in advertising to identify and monitor users online, including deterministic methods (such as third-party cookies) and probabilistic methods (such as device fingerprinting).

Subsequently, the empirical findings are contrasted with the requirements of GDPR and ePrivacy Directive. First, it is considered whether data communicated in real-time bidding auctions falls within the protected scope. In this regard, the concept of "reasonable identifiability" promoted by the CJEU is applied to scenarios commonly occurring in online behavioural advertising. Second, the author considers to what extent parties involved in RTB may be responsible for ensuring compliance. The notions of "controller", "processor" and "joint controller" are explored, paying special attention to the role of intermediaries providing standardized software tools.

Finally, the lawfulness of OBA is put to test. After a brief consideration of the exemptions offered by Art. 5 (3) ePrivacy Directive, the author addresses in detail the three legal bases potentially applicable to OBA under GDPR – performance of contract, legitimate interests, and consent. In relation to contract performance, the author proposes an alternative to the current approach of firm rejection of data commoditization. At the end, the practical benefits of consent for user privacy are questioned in view of evidence pointing to a lack of understanding by consumers and prevalence of dark patterns.

Keywords: online behavioural advertising, real-time bidding, programmatic advertising, user privacy, GDPR, ePrivacy, personal data protection