Adtech and Real-Time Bidding under European Data Protection Law

Michael Veale, University College London, UK
Frederik Zuiderveen Borgesius, Radboud University, NL

m.veale [at] ucl.ac.uk & *frederikzb [at] cs.ru.nl*

Draft, April 2021

This paper discusses the troubled relationship between contemporary advertising technology (adtech) systems, in particular systems of real-time bidding (RTB, also known as programmatic advertising) underpinning much behavioural targeting on the web and through mobile applications. This paper analyses the extent to which practices of RTB are compatible with the requirements regarding (i) a legal basis for processing, transparency, and security in European data protection law.

We first introduce the technologies at play through explaining and analysing the systems deployed online today. Following that, we turn to the law. Rather than analyse RTB against every provision of the General Data Protection Regulation (GDPR), we consider RTB in the context of the GDPR's requirement of a legal basis for processing and the GDPR's transparency and security requirements. We show, first, that the GDPR requires prior consent of the internet user for RTB, as other legal bases are not appropriate. Second, we show that it is difficult – and perhaps impossible – for website publishers and RTB companies to meet the GDPR's transparency requirements. Third, RTB incentivises insecure data processing.

We conclude that, in concept and in practice, RTB is structurally difficult to reconcile with European data protection law. Therefore, intervention by regulators is necessary.

Keywords: GDPR, e-Privacy Directive, cookie, real-time bidding, RTB, adtech, consent, transparency, security

1 Introduction

This paper discusses the troubled relationship between EU data protection legislation, encompassing the EU General Data Protection Regulation (GDPR) and ePrivacy instruments, and the infrastructures of contemporary behavioural targeting. Behavioural targeting is the monitoring of online behaviour, and the use of this to deliver personalised advertisements. Today, both on the Web and in packaged software, such as mobile apps, a complex, interwoven web of actors and technologies operate in concert to deliver the granular, and often uncanny, tailoring seen today. The paper focuses on the following question:

> To what extent is real-time bidding compatible with EU data protection and privacy law's requirements regarding a legal basis for processing, transparency, and security?

Section 2 introduces advertising technologies in historical and technological context. It outlines the technologies and practices underpinning a main mode of online advertising today, the real-time bidding (RTB) system.

We then turn to the law. We argue that the GDPR generally applies to RTB (section 3). We show that the GDPR requires consent of the internet user as a legal basis for real-time bidding practices, while the ePrivacy Directive also requires consent (section 4). Next, we show that it would be extremely difficult to make RTB comply with the GDPR's transparency requirements (section 5) and security requirements (section 6). We briefly discuss the findings in section 7. In section 8 we conclude: we call upon regulators to enforce the GDPR in the RTB sector.

2 Online advertising, adtech and real-time bidding (RTB)

Real-time bidding is a system where pre-determined advertising space, such as a banner advert on a website, or a splash screen in an app, is allocated through an auction process carried out for each requested impression. The creation of markets does not directly engage privacy concerns. Advertising can be envisaged without the use of personal data. Potential advertising space can be auctioned on the basis of generic data which does not individuate a viewer, such as the time of day, the country of internet access, the content of the page the advert is shown on, and so on.[1]

In practice however, those participating in auctions for online advertising do not only consider characteristics of the property (e.g. the website), but evaluate the personal data of the user. Real-time bidding is heavily entwined with individualised tracking, and cannot be properly understood without it.[2] We therefore explain the underlying infrastructure, before elaborating further on the functioning of the real-time bidding system.

2.1 Online Tracking

Tracking infrastructures can be split into two main types, *explicit* tracking and *inferred* tracking.[3] These terms refer to the role of the user, their device, and unique identifiers, in the tracking process.

[1] Such advertising is often called "contextual advertising".

[2] The real-time bidding industry are uncomfortable with the term tracking (calling its condemnation "facile") but do not deny that it describes the practices they undertake. See Helen Mussard, 'Digital Advertising Industry Warns Against Misguided EU Regulation - IAB Europe' (*Interactive Advertising Bureau*, 29 September 2020) <https://perma.cc/GQ6J-GXVW> accessed 22 January 2021.

[3] Franziska Roesner and others, 'Detecting and Defending Against Third-Party Tracking on the Web' (Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), 2012) 158 <https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner> accessed 8 November 2019.

2.1.1 Explicit tracking

Explicit tracking occurs where a user is identified by a tracking mechanism that assigns a unique identifier per user. A user's device may emit a unique identifier for functional reasons which can be used to track them, or a tracking infrastructure may have caused the device to store and emit an identifier on request.

On the Web, cookies are one of the main methods used in explicit tracking. Cookies were invented in 1994 to provide an ability to retain state to the stateless HTTP protocol, and '[give] the Web a memory'.[4] They consist of text, often encoded or even encrypted,[5] that can be placed by a server in a user's browser, and examined later by a server. Cookies have a range of useful functions: without some ability for a website to store information in a browser, for example, login status could not be reliably remembered the next time a user visits a site. It would also be challenging for e-commerce applications, such as retaining items in a basket online. However, the seamless and silent nature of cookies has also meant cookies can be used in ways that go beyond users' expectations.

In the early days of the Internet (when nobody knew which users were dogs[6]) content on webpages usually only came from a single source. Netscape Navigator 2.0 introduced the function of rendering two HTML files in a single browsing window in 1996 through *frames*, and so security features were needed to determine which frame could access which information in the browser. The *Same Origin Policy*, broadly put, means that documents in the browser, such as cookies, can only be accessed by servers sharing their protocol (e.g. HTTP, HTTPS), domain, and port.[7] The intention for this was so that if one party places a cookie, another party cannot read it.

Driven by a desire to establish cross-site, tracking, the advertising industry sought to circumvent the effects of the Same Origin Policy. Cookies that are not placed by the website publisher itself, but by third parties, are often called 'third party cookies'. Say that somebody visits a website, www.A.com. It may seem that each element on that website comes from A.com. In reality, however, different elements of the website are often sourced from other domains. For example, a website may have a box for advertisements, or for recommended articles elsewhere on the web. In most cases, ads are shown on a website not by the website publisher itself (A, in our example) but by third parties. Those third parties can also place and read their own cookies, third party cookies. The website visitor usually does not see that his or her browser contacts these different

[4] John Schwartz, 'Giving the Web a Memory Cost Its Users Privacy', *New York Times* (4 September 2001).

[5] For example, IAB cookies relating to real-time bidding are often placed as concatenated, sequential bits that are then encoded using the base64 method.

[6] See generally Glenn Fleishman, 'Cartoon Captures Spirit of the Internet', *The New York Times* (14 December 2000) <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html> accessed 8 November 2019.

[7] See generally Frederik Braun, 'Origin Policy Enforcement in Modern Browsers' (Diploma Thesis, Ruhr Universität Bochum 2012).

domains; for the website visitor it seems like one website is being loaded from one domain. While a user may only see one URL in the address bar, visiting almost any site now entails querying tens or hundreds of other servers.

Some firms have spread their own tracking code with resounding success: Google calls home with unique identifiers for at least 28% of *all* web page loads, while Facebook does the same for approximately 15%.[8] The proportion is significantly higher in certain sectors, such as news, compared to others, such as banking. Trackers also differ by country — UK users are tracked more in this manner than Chinese web users, for example.[9]

Yet firms with less infrastructure also established means to track users more broadly by using loopholes in the Same Origin Policy to combine the reach of their tracking. The prime mechanism this is carried out is through cookie syncing, also called cookie matching. In its most basic form, this involves a third-party with a cookie (TRACKER1) making a user's browser query a second third-party (TRACKER2) with a URL which includes TRACKER1's identifier.[10] Because the user's browser is querying TRACKER2, TRACKER2 is able to look at its own cookies on the site. As the query includes the ID that Tracker1 just saw from its own cookies, this has the effect of enabling TRACKER2 to possess both identifiers at once, associating their own cookie ID with TRACKER1's cookie ID. The two organisations can share data through a back-channel ('server-to-server transfer'[11]) to connect the profiles they have built so far.

This *cookie syncing* (or cookie matching) significantly widens the scope of tracked activity online by pooling the reach of multiple trackers.[12] Even under conservative estimates of server-to-server transfers, based only on *observed* cookie syncing, 53 firms observe more than 91% of users' browsing behaviour.[13] This figure is likely an underestimation — a recent study found evidence that as many as 27% of advertiser-tracker relationships may be undetectable through cookie-syncing analysis.[14]

More recently, trackers have sought to evade restrictions on third party cookies in a number of newer ways. In particular, they have been encouraging sites to edit their Domain Name System (DNS) records to effectively deliver third-party tracker resources from the same domain that is serving the website, making effectively blocking trackers without breaking the website a trickier task. This also

[8] Arjaldo Karaj and others, 'WhoTracks.Me: Shedding Light on the Opaque World of Online Tracking' [2018] arXiv:180408959, 8.

[9] X Hu and others, 'Multi-Country Study of Third Party Trackers from Real Browser Histories' (2020) 2020 IEEE European Symposium on Security and Privacy (EuroS&P) 70.

[10] For example, a query might look like http://tracker2.com?tracker1cookieID=j9240.

[11] See generally Muhammad Ahmad Bashir and Christo Wilson, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) 2018 Proceedings on Privacy Enhancing Technologies 85.

[12] Google call this 'cookie matching'. See generally Jane Wakefield, 'Google's "secret Web Tracking Pages" Explained' (9 May 2019) <https://www.bbc.com/news/technology-49593830> accessed 8 November 2019.

[13] Bashir and Wilson (n 11).

[14] John Cook and others, 'Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem Using Header Bidding' (2020) 2020 Proceedings on Privacy Enhancing Technologies 65.

creates a range of serious security risks, as first-party cookies often include cookies designed to log a user in to a website, and such configurations can mean that these cookies can be read by and sent to a third party other than the website operator.[15] As a result, the terms 'first-party' and 'third-party' cookies have less meaning in a legal context — a case-by-case analysis will be required to understand which actors are involved in any particular cookie, as the domain name–based identity of the server laying it may not be the same as the organisation utilising its tracking potential across websites.

On mobile devices, app developers, which are analogous to website publishers, have more freedom to execute arbitrary code. As the Web is accessed through a browser, the browser has power to limit the ways a website can function. In contrast, app developers can specify the way their software works without requiring to cede rendering and execution decisions to the browser. Instead, looser limits are applied at the level of the mobile operating system (e.g. limiting access to sensors such as the camera or GPS) and through any conditions placed upon apps allowed to be distributed through official channels such as Apple's App Store and Alphabet's Play Store, which for most users will be the only way they install custom software.

The fact that app developers have more freedom than Web developers to determine who is able to track individuals means that active tracking, rather than passive tracking, is the main issue in the mobile sphere. Third-party services are integrated in apps for a variety of purposes, including crash reporting, to provide usage or engagement analytics, to integrate agile development methods such as A/B testing, to integrate with other services such as social networks, and to deliver advertising. Almost all of these services, with the exception of advertising services, *only operate in the background* of applications, and users are in general unable to detect and understand the extent to which the app is communicating with both the developer's server (the 'first-party') or third-party servers.

Empirical studies into tracking apps are challenging, and are mostly limited to the Android platform due to the inability to examine the innards of the heavily restrictive Apple iOS system. Studies seeking to survey app tracking at scale take a few different approaches.[16] Some researchers intercept traffic from hundreds of thousands of apps which are being either interacted with automatically by bots

[15] Yana Dimova and others, 'The CNAME of the Game: Large-Scale Analysis of DNS-Based Tracking Evasion' [2021] arXiv:210209301 [cs].

[16] For an assessment of the comparative merits of these approaches, see Abbas Razaghpanah and others, 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem' (The Network and Distributed System Security Symposium (NDSS 2018), San Diego, CA, USA, 18 February 2018) 13–14 <http://eprints.networks.imdea.org/1744/> accessed 8 November 2019.

synthesising real user input in a sandbox on a server,[17] or by using real user interactions, with traffic captured via user-installed VPNs.[18]

One recent study identified 2,121 separate advertising tracking services in apps in the Android ecosystem, which can be grouped by ownership into approximately 292 parent organisations.[19] Another study found that 88.4% of apps contained a tracker owned by Alphabet (Google), 42.6% by Facebook, 33.9% by Twitter, 26.3% by Verizon and 22.2% by Microsoft.[20] 30% of News apps, 28% of Family apps, and 25% of Gaming & Entertainment apps contain trackers from more than ten distinct tracker companies.[21]

Mobile devices hold a variety of unique identifiers tied to their software and hardware with different levels of permanence, such as the IMEI, IMSI and SIM number, operating system number, phone number, device ID, MAC address, and operating system specific advertising identifiers.[22] Third-party plug-ins have a variety of direct and indirect ways to access these identifiers, and in practice access and transmit a wide variety of them.[23] Such identifiers are also linked through a variety of means to track individuals across different devices, although exactly how this occurs in-the-wild is unclear.[24]

2.1.2 Inferred tracking

Inferred tracking seeks to identify or profile an individual from observing their digital traces online, and re-identifying a user through primarily probabilistic means. Unlike explicit tracking, these approaches are 'stateless' — they do not change the behaviour of user's devices, nor store information on them directly. Inferred tracking is therefore substantially more challenging for an individual or device to defend against.

'Fingerprinting' is a core approach for inferred tracking. Early documentation of fingerprinting was provided by analysis from the Electronic Frontier Foundation's *Panopticlick* tool, which uses modern fingerprinting techniques to

[17] See e.g. Haojian Jin and others, 'Why Are They Collecting My Data?: Inferring the Purposes of Network Traffic in Mobile Apps' (2018) 2 Proc ACM Interact Mob Wearable Ubiquitous Technol 173:1.

[18] See e.g. Razaghpanah and others (n 16); Anastasia Shuba and others, 'AntMonitor: A System for On-Device Mobile Network Monitoring and Its Applications' [2016] arXiv:161104268 [cs]; Yihang Song and Urs Hengartner, 'PrivacyGuard: A VPN-Based Platform to Detect Information Leakage on Android Devices' in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* (SPSM '15, New York, NY, USA, ACM 2015).

[19] Razaghpanah and others (n 16).

[20] Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem' in *Proceedings of the 10th ACM Conference on Web Science* (WebSci '18, New York, NY, USA, ACM 2018) 27. The sixth most prevalent tracker was LinkedIn, which has since been purchased by the fifth most prevalent tracker, Microsoft.

[21] ibid 28.

[22] Razaghpanah and others (n 16) 3.

[23] ibid 7.

[24] See generally Sebastian Zimmeck and others, 'A Privacy Analysis of Cross-Device Tracking' (26th USENIX Security Symposium (USENIX Security 17), 2017) <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/zimmeck> accessed 8 November 2019.

determine how unique, and therefore how fingerprint-able, your browser is.[25] Browser fingerprinting is a moving target, as sophisticated techniques can circumvent proxies, reveal the particular version of a browser, and repurpose new Web technologies for fingerprinting as they emerge.[26] Research has found evidence of fingerprinting on at least 4.4%–5.5% of top websites, although these should be taken as lower bounds due to the difficult-to-observe nature of fingerprinting techniques.[27] These methods interplay with explicit tracking mechanisms — if the user clears their cookies, for example, fingerprinting approaches can be used to re-establish ('respawn') deleted identifiers.[28]

Inferred tracking also plays an important role in cross-device tracking. Simulated cross-device tracking studies have estimated a significant ability to follow users from their mobiles to their desktops, even if they are not logged in to the same service (e.g., if they are connected to the same router). Many companies advertise probabilistic cross-device tracking as a reason to install and use their trackers.[29]

Despite scholarly interest, the covert, stateless nature of fingerprinting and inferred tracking makes its prevalence, scope and impact unclear.[30]

2.2 RTB and programmatic advertising

Real-time bidding (RTB) is a form of *programmatic advertising*, where advertising placements are determined by algorithmic systems, rather than in human-mediated ways, such as through traditional negotiation and contracts. With RTB, advertisers (or their intermediaries) bid on an automated auction for the chance to target an ad to a specific internet user. RTB is also called 'audience selling' or 'audience buying'.

While early display advertising (the sale of 'properties' such as banners, pop-ups or video segments) was largely conducted through manual deals, advertising

[25] See Peter Eckersley, 'How Unique Is Your Web Browser?' in Mikhail J Atallah and Nicholas J Hopper (eds), *Privacy Enhancing Technologies*, vol 6205 (Springer Berlin Heidelberg 2010). You can test your own browser at https://panopticlick.eff.org.

[26] See generally Nick Nikiforakis and others, 'Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting' (May 2013) 2013 IEEE Symposium on Security and Privacy 541; Łukasz Olejnik and others, 'The Leaking Battery' in *Data Privacy Management, and Security Assurance* (Lecture Notes in Computer Science, Joaquin Garcia-Alfaro and others eds, Springer International Publishing 2016).

[27] Gunes Acar and others, 'FPDetective: Dusting the Web for Fingerprinters' in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (CCS '13, New York, NY, USA, ACM 2013); Gunes Acar and others, 'The Web Never Forgets: Persistent Tracking Mechanisms in the Wild' in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (CCS '14, New York, NY, USA, ACM 2014).

[28] Ashkan Soltani and others, 'Flash Cookies and Privacy' (23 March 2010) 2010 AAAI Spring Symposium Series; Mika D Ayenson and others, 'Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning' (SSRN Scholarly Paper, 29 July 2011); Acar and others (n 27).

[29] Zimmeck and others (n 24).

[30] A useful review of knowledge on fingerprinting is Pierre Laperdrix and others, 'Browser Fingerprinting: A Survey' [2019] arXiv:190501051 [cs].

is now predominately allocated automatically through programmatic methods, of which real-time bidding is the prime system.[31]

Real time bidding is a complicated system, with many different types of players. Below, we give a brief introduction to RTB. The reader might be a tad overwhelmed, but such a reaction is understandable. We return to the complexity and the opaqueness of RTB in section 5.

In brief, real time bidding works as follows (and is illustrated in the companion Figure 1): A website or app (publisher) has a range of slots that it wishes to sell to advertisers, known in the industry as their 'inventory'. Advertisers to fill these slots are sought through one or more supply-side platforms (SSPs) the publisher deals with.[32] Supply-side platforms are technical intermediaries for publishers to work with complex advertising auction markets: the advertising exchanges (ADXs) which serve as auction-houses for real-time bidding. Demand-side platforms (DSPs) are the technical intermediaries that represent advertisers. Such demand-side platforms place bids on advertising exchanges.

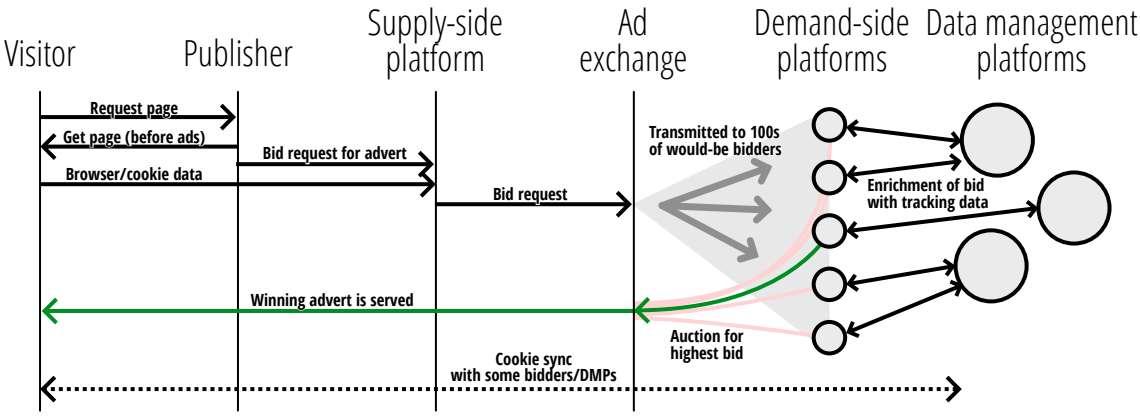

Figure 1. Main actors and processes in RTB (diagram by authors).

These demand-side platforms will be given a copy of the bid request, which represents information about the user to whom the advert will be delivered. This

[31] Competitions and Markets Authority, 'Online Platforms and Digital Advertising' (Market Study Interim Report, 2019) para 2.41.

[32] In the past, a publisher would work with a single SSP. However, as are several AdXs, publishers often found themselves locked into a 'waterfall' process whereby, in practice, Google's exchange would get the first attempt to bid for inventory, and if it met the minimum specifications (e.g. a price threshold) of publishers, it would be the ad that was served. Only if this failed would the same ad be offered to other ad exchanges, in a 'waterfall'–like sequence. In some cases, these other exchanges may have offered a higher price, but the publisher would never have known. Consequently, in recent years, a process called *header bidding* emerged, where the publisher themselves (in the HTML header of the website) would query many exchanges simultaneously rather than sequentially, through multiple SSPs, and on their end (or the server of yet another intermediary) evaluate the different offers and choose between them. See generally Michalis Pachilakis and others, 'No More Chasing Waterfalls: A Measurement Study of the Header Bidding Ad-Ecosystem' in *Proceedings of the Internet Measurement Conference* (IMC '19, New York, NY, USA, ACM 2019).

information varies slightly depending on the specification. On the Web, the contents of this 'bid request' is determined by one of two specifications. The first is *Authorized Buyers*, a specification determined by Google. The second is *OpenRTB/AdCOM*, maintained by the technology division of the Interactive Advertising Bureau (IAB), a membership organisation of large and small advertising firms ranging from Google, Facebook and Twitter down to smaller actors.

A bid request contains a broad array of data about an individual, their device and the website there are visiting. Some of the data in *Authorized Buyers* and *OpenRTB* bid requests relevant to our regulatory discussion include:

- **Site**
  - URL of the site being visited
  - Site category or topic
- **Device**
  - Operating system
  - Browser software and version
  - Device manufacturer, model
  - Mobile provider
  - Screen dimensions
- **User**
  - Unique identifiers set by vendor and/or buyer.
    - *Advertising exchange's unique person identifier, often from the advertising exchange's cookie.*
    - *A demand-side platform's user identifier, often taken from the cookie of the advertising exchange which has been cookie-synced with a cookie from the demand-side platform's domain.*
  - Year of Birth
  - Gender
  - Interests
  - Metadata reporting on consent provided
- **Geography**
  - Longitude and latitude
  - Postal/ZIP code

Bid requests with some of all of this information have the potential to directly target individuals in quite granular ways. However, the economic incentives of an auction mean that demand-side platforms with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The demand-side platform enlists a final actor, the data management platform (DMP). demand-side platforms send bid requests to data management platforms, who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser

(e.g. customer relationship databases), collected from other sources (e.g. a list from another company), or bought from data brokers. Cambridge Analytica was a notorious data management platform, for example, although companies like Google also run data management platforms.

The demand-side platform with the highest bid not only wins the right to deliver the ad, through the supply-side platform, to the individual. The demand-side platform also wins the right to cookie sync its own cookies with the ad exchange (see section 2.1.1), to more easily be able to link data and profile the user in the future.[33]

3 The GDPR applies to RTB

The GDPR applies to activities that fall within both its material and territorial scope. The GDPR 'applies to the processing of personal data wholly or partly by automated means.'[34] There are exemptions which self-evidently do not apply in the case of RTB, such as whether the activity if processed 'by a natural person in the course of a purely personal or household activity'.[35] Therefore the discussion of whether real-time bidding falls within the material scope of the GDPR centres on the GDPR's definition of personal data, relevant case law, and applicable guidance from the European Data Protection Board, where Data Protection Authorities (DPAs) from the 27 EU Member States cooperate. Processing includes almost everything that can be done with personal data,[36] and the definition is so wide that it rarely leads to discussion.

As noted, the main relevant question for material scope is whether RTB involves the use of 'personal data'. Personal data means

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an *identification number, location data, an online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37]

[33] See generally Muhammad Ahmad Bashir, 'On the Privacy Implications of Real Time Bidding' (PhD, Northeastern University 2019) 16–17. Note that the type of sync depends on the AdX; some only provide DSP-specific hashes of the cookies to the DSP, limiting the ability to use this mechanism to link data between DSPs and DMPs, while others provide a common AdX identifier which can make it significantly easier to connect data about the same user.

[34] GDPR, art 2(1).

[35] GDPR, art 2(2).

[36] GDPR, art 4(2).

[37] GDPR, art 4(1), emphasis added.

Scholarly work already exists explaining why behavioural advertising constitutes personal data processing under the GDPR, and will only be summarised here rather than repeated.[38]

Bid requests contain enough data to identify an individual or a device — in practice devices are now primarily individual and not shared — in a number of ways. They generally contain unique identifiers that relate to the ad exchange, which in turn are connected to different identifiers set by tracking infrastructure run by numerous adtech vendors. Indeed, the winner of a bid can, by design of the protocol, cookie sync and connect their own set of identifiers to the ad exchange's.[39] It is additionally a common practice to cookie sync with other tracking firms outside of the real-time bidding protocol.[40] Furthermore, the bid request contains such as wide array of personal data beyond explicit identifiers that it is likely to be unique in and of itself, and can serve to fingerprint users.[41] This is even more apparent given the way that industry players collate bid request data.[42]

Even if it requires multiple actors such as publishers, demand-side platforms, ad exchanges and supply-side platforms to do so, data processing in real-time bidding is designed to identify and profile individual users, and that brings it within the scope of data protection. The Court of Justice of the European Union (CJEU) determined in *Breyer* that the data necessary to identify a user need not all be in the hands of the same actor,[43] and that data would not be personal data only if it met the high barrier that 'the identification of the data subject was 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.'[44] In the case of adtech, that seems unlikely to apply, particularly given the ways that industry players rely on 'contractual controls' between hundreds of entities,[45] as well as the prevalence of server-to-server data transfers between players which makes connecting data the norm, rather than the exception.[46]

[38] See Frederik J Zuiderveen Borgesius, 'Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 Computer Law & Security Review 256.

[39] Panagiotis Papadopoulos and others, 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask' [2018] arXiv:180510505 [cs]; Tobias Urban and others, 'The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR' [2018] arXiv:181108660 [cs].

[40] Papadopoulos and others (n 39); Urban and others (n 39).

[41] See section 2.1.

[42] See Rebecca Hill, 'French Data Watchdog Withdraws Probe from Location Data Guzzling Adtech Biz Vectaury', *The Register* (27 February 2019) <https://www.theregister.co.uk/2019/02/27/cnil_gdpr_vectaury/> accessed 20 June 2019.

[43] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779 [44].

[44] ibid [46].

[45] Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (*Information Commissioner's Office*, 20 June 2019) 21 <https://perma.cc/X7PX-EL3L> accessed 20 June 2019.

[46] Bashir and Wilson (n 11).

Furthermore, it is worth adding that some courts have utilised a further test to firmly ground such data as that processed in RTB as personal. The Court of Appeal in England and Wales notes that such 'browser generated information' serves to 'individuate' the user, in the sense they are singled out, proposing a route to determining whether information is personal data that sits alongside the above linkability analysis by the CJEU in *Breyer*.[47] The CJEU has not needed to consider this type of argument yet, but it is worth noting that 'singling out' has entered EU law in the recitals to the GDPR.[48]

The GDPR therefore applies to real-time bidding. It is not the only regime to do so — the ePrivacy Directive has specific rules for tracking technologies, which we will discuss further in section 4.1.4.[49] As the GDPR applies, we must turn to what it requires of those processing personal data to make such activities lawful.

4 Legal basis

In this section, we show that European data protection law requires consent of the internet user as a legal basis for real-time bidding practices.[50]

4.1 The GDPR's requirement for a legal basis for processing

Under the Charter of Fundamental Rights of the European Union, processing personal data is only allowed on the basis of the consent of the data subject or another legal basis laid down by law.[51] The GDPR elaborates, and exhaustively lists six possible legal bases.[52] A data controller (an organisation using personal data[53]) may *only* process personal data on the basis of the data subject's consent, or on one of the other five legal bases. The six legal bases were copied from the 1995 Data Protection Directive with only minor amendments.[54] Hence, the requirement for a legal basis is a key part of EU data protection law for twenty-five years.

For the private sector, three legal bases are most relevant: (a) consent, (b) necessity for contractual performance, and (f) the legitimate interests provision.

[47] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 [115] et seq. The Court further developed this strand of case-law, applying it to transient images in facial recognition systems, in *R (on the Application of Bridges) v South Wales Police* [2020] EWCA Civ 1058 [46].

[48] GDPR, recital 26.

[49] 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) OJ L 201 (2002) art 5(3).

[50] This section is partly based on, and includes sentences from Frederik J Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163.

[51] Charter, art 8(2).

[52] GDPR, art 6(1). See also Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* ECLI:EU:C:2017:336 [25]; *Breyer* (n 43) [57]: 'Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful'

[53] See for a more precise description: section 4.2.1.

[54] See Data Protection Directive, art 7.

We discuss each of those legal bases in turn, and show that generally, only the data subject's consent can provide a legal basis for personal data processing for RTB.

4.1.1 Consent

The GDPR states: 'Processing shall be lawful only if and to the extent that at least one of the following applies: (…) the data subject has given consent to the processing of his or her personal data for one or more specific purposes'.[55]

The requirements for valid consent are strict under the GDPR. The GDPR's consent definition says that '"consent" of the data subject means any freely given, specific, informed and 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'.[56] Article 7, on 'conditions for consent' makes the requirements for valid consent even stricter.

The following elements can be deduced from the GDPR's consent definition: valid consent requires (i) an indication of wishes, which is (ii) specific and informed, and (iii) freely given. We discuss each element in turn.

4.1.1.1 Indication of wishes

The most important requirement for valid consent is that a data subject gives an unambiguous indication of his or her wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.[57] The GDPR's preamble gives, not exhaustively, examples of how a data subject can give an indication of wishes: 'a written statement, including by electronic means, or an oral statement.'[58] The preamble adds that an indication of wishes 'could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.'[59]

[55] GDPR, art 6(1)(a).
[56] GDPR, art 4(11).
[57] ibid.
[58] GDPR, recital 32.
The 'preamble' of EU legislation is a kind of introductory text, consisting of 'recitals' which give additional explanations. The Court of Justice of the European Union sometimes refer to recitals in data protection cases. See e.g. Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.; See generally on the role of recitals Todas Klimas and Jurate Vaiciukaite, 'The Law of Recitals In European Community Legislation' (2008) 15 ILSA Journal of International & Comparative Law 61.
[59] The phrase 'information society services' refers, roughly summarised, to internet services. Hence, in principle people can indicate their wishes by choosing technical settings for an internet service. To illustrate: a system like Do Not Track could be developed that enables people to give and withhold consent to online tracking. However, such consent through technical settings must, of course, comply with all the GDPR's requirements for valid consent.

Under the 1995 Data Protection Directive, data controllers sometimes assumed that a data subject consented if he or she failed to object: an opt-out system. However, an opt-out system could generally not lead to a valid indication of wishes and could thus not lead to valid consent under the Data Protection Directive.[60] The GDPR's consent definition is more explicit than the directive's, as the GDPR requires an 'a statement or (…) a clear affirmative action' for valid consent.[61] Mere inactivity is not an indication of wishes.

In a case about cookies, the CJEU confirmed in 2019 that the GDPR 'expressly precludes "silence, pre-ticked boxes or inactivity" from constituting consent.'[62] Other CJEU case law affirms that controllers cannot easily assume consent.[63] To sum up: opt-out systems cannot be used to obtain valid consent; consent requires a clear expression of will.

4.1.1.2 Specific and informed

The GDPR's consent definition also requires that consent is 'specific'; and 'informed'. These two elements are largely overlapping.[64] Article 7 gives additional requirements. It is not acceptable to hide a consent request in the small print of a contract, privacy notice, or other document. The 'request for consent shall be presented in a manner which is clearly distinguishable from the other matters.'[65] Article 7 also requires that a consent request is presented 'in an intelligible and easily accessible form, using clear and plain language.'[66] Furthermore, consent must be 'informed' be valid. A to consent request must, at a minimum, disclose the controller's identity, and the processing purpose.[67]

The GDPR's preamble adds about the specificity requirement: '[c]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.'[68]

[60] Eleni Kosta, 'Construing the Meaning of Opt-Out - An Analysis of the European, U.K. and German Data Protection Legislation' (2015) 1 Eur Data Prot L Rev 16.

[61] GDPR, art 4(11).

[62] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände—Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801 [62].

[63] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:662 [63]. See also, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:353, Opinion of AG Sharpston [79].

[64] Kosta suggests that 'specific' and 'informed' are largely overlapping, and that the requirement of specificity may be superfluous. Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013) 224.

[65] GDPR, art 7(2).

[66] Ibid. That requirement applies 'if the data subject's consent is given in the context of a written declaration which also concerns other matters'. Presumably, in other situations a consent request must also be 'intelligible', and must also use 'clear and plain language.' Recital 32 adds that in the online context, a consent request must be straightforward and succinct. The recital says that '[i]f the data subject's consent is to be given following a request by electronic means, the request must be clear [and] concise.'

[67] GDPR, recital 42.

[68] GDPR, recital 32.

Case law says about the specificity requirement that 'consent must be specific, that is to say, connected with a processing operation (or series of processing operations) for precise purposes.'[69] In the context of cookies, the CJEU says that 'specific' means that consent 'must relate specifically to the processing of the data in question'.[70] Moreover, the information provided by the controller must ensure that the 'user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed.'[71]

4.1.1.3 Freely given

Only 'freely given', thus voluntary, consent can be valid. Consent is only 'freely given' if the data subject has a genuine choice. Article 7(4) gives guidance regarding the 'freely given' requirement: 'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'[72]

In short, a take-it-or-leave-it choice regarding personal data processing can make consent involuntary and thus invalid. A typical example of such a take-it-or-leave-it choice is a tracking wall, a barrier that visitors can only pass if they consent to tracking by third parties. In the spring of 2020, the European Data Protection Board clarified that tracking walls make consent involuntary and therefore invalid:

> In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls).[73]

To summarise: companies can obtain a legal basis for personal data processing if a data subject gives valid consent. In the following two sections, we show that a data controller cannot rely on other legal bases for RTB.

[69] Case T-343/13, *CN v Parliament*, ECLI:EU:T:2015:926 [61]. The case concerned Regulation 2001/45; that regulation uses a similar consent definition as the GDPR.

[70] *Planet49* (n 62) [58].

[71] ibid [74].

[72] The GDPR's preamble makes the requirements for 'freely given' consent even stricter: 'Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment', recital 42. See also recital 43.

[73] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.0', Brussels, 4 May 2020, p. 11. And Web-wide tracking is not *necessary* for providing a website. See Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (2 April 2013) WP 203, 46; Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC' (9 April 2014) WP 217, 47.

4.1.2 Necessity for contract performance

Another legal basis in the GDPR is necessity for contract performance. Sometimes a controller can have a legal basis for processing if the processing is necessary for performing a contract.[74] In the words of the GDPR, a data controller can have a legal basis for personal data processing if 'processing is necessary for the performance of a contract to which the data subject is party (…)'.[75]

For example, a newspaper publisher does not need to obtain consent to process the name and address of a subscriber, as far as these personal data are required to deliver the newspaper at the subscriber's home. The personal data are 'necessary' to deliver the newspaper to the subscribers and thus to fulfil the contract.

Can a contract provide a legal basis for personal data processing for RTB? Almost certainly not. For this provision to apply, the processing must be genuinely 'necessary' for performing the contract. CJEU case law shows the word 'necessary' must be interpreted narrowly, in favour of the data subject.

> As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[76]

The 'necessary' requirement is related to proportionality, as confirmed in CJEU case law.[77] The CJEU has said that 'the principle of proportionality requires that [measures] 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.'[78] In sum, one should not too easily assume that data collection for RTB and targeted advertising is 'necessary' for performing a contract.

[74] GDPR, recital 44.

[75] GDPR, art 6.

[76] *Rīgas satiksme* (n 52) [30]: 'As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.' See also Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* ECLI:EU:C:2014:238 [50]: 'according to the Court'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*.'

[77] See Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970 [96]: 'Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (…)'; Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* ECLI:EU:C:2017:725 [111]–[2]: 'It is (...) for the referring court to determine whether the establishment of the contested list is necessary for the performance of the tasks carried out in the public interest at issue (...) It is important, in that regard, to ensure that the principle of proportionality is respected. The protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations be carried out within the limits of what is strictly necessary'. See on proportionality and data protection law also Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 147–50. See *Digital Rights Ireland* (n 76) [69].

[78] *Digital Rights Ireland* (n 76) [46]; *Tele2/Watson* (n 77) [95]–[107].

Apart from the necessity requirement, there are legal requirements for entering into a contract. It is dubious whether those requirements are met when somebody merely uses a website or an app. From a legal perspective, the main requirement to enter a contract is that both parties want to enter a contract.[79] To illustrate, the Vienna Sales Convention says that '[a] statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance'.[80] But somebody who visits a website or uses and app rarely intends the wish to enter a contract about tracking or RTB.[81]

Therefore, in most situations, internet users do not enter a contract with companies about trading personal data for ad targeting against the use of a service. Especially if a company collects or uses information about people without them being aware, it is hard to see how those people could have entered a contract with the company.[82] Indeed, the European Data Protection Board says that the legal basis necessity for contract performance is not an appropriate legal basis for data processing for behavioural advertising; consent is always required for such advertising.[83]

4.1.3 Necessity for the controller's legitimate interests

Another legal basis that a controller can invoke for personal data processing is the legitimate interests provision.[84] Roughly summarised, a controller can rely on this provision when personal data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, and those interests outweigh the data subject's interests or fundamental rights. In the words of the GDPR:

> Processing shall be lawful only if and to the extent that at least one of the following applies: (...) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[79] J Smits, 'The Law of Contract' in J Hage, A. Waltermann and B Akkermans (eds), *Introduction to Law* (Springer 2017), p. 59.

[80] Article 18(1) of the Vienna Convention on International Sale of Goods.

[81] See in more detail, Zuiderveen Borgesius (n 50) 163–76.

[82] See also Article 29 Working Party, Letter to Google (signed by 27 national Data Protection Authorities), 16 October 2012 <www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf> Appendix: <www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf>.

[83] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC' (WP 217) 9 April 2014, p. 17. The Working Party adds that 'consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research' (p. 47).

[84] Article 6(1)(f) of the GDPR.

The CJEU says that the legitimate interests provision implies three cumulative requirements: 'first, the pursuit of a legitimate interest by the data controller or by the third party (…); second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.'[85]

First, are RTB and targeted advertising 'legitimate interests'? Recital 47 gives 'direct marketing purposes' as an example of legitimate interests. The recital thus gives an argument in favour of accepting RTB and targeted advertising as legitimate interests. Moerover, RTB companies can invoke their 'freedom to conduct a business in accordance with Union law and national laws and practices', as protected by the Charter of Fundamental Rights of the European Union.[86] The Advocate General of the CJEU confirms that online marketing relates to the freedom to conduct a business.[87]

The European Data Protection Board emphasises, logically, that only lawful practices can form a legitimate interest.[88] If RTB brings serious risks for people's privacy and data protection rights, its lawfulness could be questioned. But for now, let us assume that the controller (a company doing RTB) has some legitimate interest.

The second question is: is the processing 'necessary' to pursue those interests? As noted in the previous section, the necessity hurdle is difficult to take. Whether RTB is 'necessary' is debatable. Suppose that the company's interest is making money with online advertising. In that case, there are many other ways of online advertising that do not entail much personal data collection. For example, contextual advertising does not require collecting data about people. Contextual advertising is the practice where ads are adapted to the context, or content, of a web page. For instance: ads for local hotels on a website about tourism in Madrid.

However, a company might also argue that it specialises in behavioural advertising or in RTB. A counter argument could be that behavioural advertising is possible without large-scale data collection. Several systems have been developed for, in short, confidential ad targeting.[89] Already 10 years ago, researchers developed Adnostic, a browser plug-in that does not involve sharing

[85] *Rīgas satiksme* (n 52) [28].

[86] Charter, art 16.

[87] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2013:424 (Opinion of AG Jääskinen) [95].. See also Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC' (WP 217) 9 April 2014, p. 25: marketing is a legitimate interest.

[88] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC' (9 April 2014) WP 217, p. 25.

[89] Whether these are privacy or data protection–friendly rather than just confidential (see in that respect Michael Veale and others, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105), or indeed exempt orchestrating organisations from classification as data controllers (as they may remain orchestrating forces following Case C-25/17 *Jehovan todistajat* ECLI:EU:C:2018:551), are questions for another time.

one's browsing behaviour with a company. Adnostic builds a profile based on the user's browsing behaviour, and uses that profile to target ads – all within the user's device. Minimal information leaves the user's device, as the behavioural targeting happens in the user's browser.[90] Such techniques are entering practice, such as Google's Federated Learning of Cohorts (FLoC) system for microtargeting within Chrome.[91]

Seeing that behavioural advertising is possible without sharing much data with companies, one could argue that large-scale data collection for behavioural advertising is disproportionate and thus not necessary. The requirements for necessity are indeed strict. However, Data Protection Authorities rarely, if ever, follow that line of reasoning, perhaps because it risks prescribing certain means of processing.[92] Furthermore, current proposals, such as FLoC, require large-scale infrastructural control and co-ordination, such as through shaping a browser and being able to orchestrate a protocol through it, which is not within the power of all data controllers to achieve.[93] Let us then assume, for argument's sake, that some companies engaged in RTB can, in some situations, pass this necessity test.

That would bring us to a third requirement: do the data subject's interests outweigh the company's interests? Few, if any, companies engaged in RTB could overcome this hurdle. The data subject's interests include the fundamental rights to privacy and data protection.[94] Case law of the European Court of Human Rights confirms that people have a reasonable expectation of privacy regarding their Internet use.[95] Moreover, surveys consistently show that people see online tracking and related practices as a privacy invasion.[96]

[90] Solon Barocas and others, 'Adnostic: Privacy Preserving Targeted Advertising' (2010) NDSS. See also: <http://crypto.stanford.edu/adnostic/>.

[91] See generally Bennett Cyphers, 'Don't Play in Google's Privacy Sandbox' (30 August 2019, *EFF*) <https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1>.

[92] Acquisti, an economist, makes an argument along those lines (A Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (Background Paper for the Conference: The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines) (2010) <www.oecd.org/Internet/ieconomy/46968784.pdf, p. 42-43. The EDPB indicate a willingness to move in this direction further in recent draft guidance: European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (2020) para 47.

[93] Note that FLoC is currently under investigation by several competition authorities, including the UK's Competition and Markets Authority and DG COMP.

[94] Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (ASNEF)* ECLI:EU:C:2011:777 [41]; Joined Cases C-465/00, C-138/01, C-139/01 *Österreichischer Rundfunk & Ors* ECLI:EU:C:2003:294 [68]; *Google Spain* (n 58) [74].

[95] *Copland v the United Kingdom* ECLI:CE:ECHR:2007:0403JUD006261700, para 42.

[96] See: J Turow and others, 'Americans Reject Tailored Advertising and Three Activities that Enable it' (29 September 2009) <http://ssrn.com/abstract=1478214>. In Europe, seven out of ten people are concerned that companies might use data for new purposes such as targeted advertising without informing them (European Commission, 'Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>; S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, 'Online behavioral advertising: a literature review and research agenda' (2017) Journal of Advertising 363-376. See also Ben Weinshel and others, 'Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing' in (ACM 11 June 2019) Proceedings of the 2019 ACM SIGSAC Conference on Computer and

Indeed, the European Data Protection Board suggests that data controllers cannot rely on the legitimate interests provision for personal data processing for targeted advertising: 'consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research'.[97] Several authors agree.[98]

The UK DPA confirms in a 2019 report that 'the nature of the processing within RTB makes it impossible to meet the legitimate interests lawful basis requirements.'[99] The DPA adds that 'the only lawful basis for "business as usual" RTB processing of personal data is consent (ie processing relating to the placing and reading of the cookie and the onward transfer of the bid request).'[100]

Regardless of this array of explicit regulatory guidance on the inappropriateness of this lawful basis, empirical research finds that many RTB vendors in Europe still claim legitimate interest as a lawful ground.[101]

In conclusion, in almost all cases, the data subject's consent is the only available legal basis for personal data processing for RTB and behavioural advertising under data protection law. Even in the far-fetched case that a company can rely on another legal basis for RTB, separate EU law still requires the company to ask consent, namely for the cookies and similar technologies. That cookie consent requirement is the topic for the next section.

Communications Security 149 (where 71.3% of participants considered it 'creepy' for 'advertising companies to track which websites [they] visit in order to show [them] ads', and 52.9% to 30.6% said the practice was 'unfair').

[97] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203), 2 April 2013: 'consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research' (p. 46).

[98] See P Traung, 'EU Law on Spyware, Web Bugs, Cookies, etc. Revisited: Article 5 of the Directive on Privacy and Electronic Communications' (2010) 31 Business Law Review 216, p. 218; L Moerel, 'Big Data protection. How to make the draft EU Regulation on Data Protection future proof' (inaugural lecture) (14 February 2014) <www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf>. The Dutch government comes to the same conclusion. See for an English translation of the relevant remarks of the Dutch legislator: College bescherming persoonsgegevens (Dutch DPA), 'Investigation into the combining of personal data by Google, Report of Definitive Findings' (z2013-00194) (November 2013) https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf p. 81, footnote 294.

[99] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020, p. 18.

[100] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020, p. 18.

[101] Maximilian Hils and others, 'Measuring the Emergence of Consent Management on the Web' in (ACM 27 October 2020) Proceedings of the ACM Internet Measurement Conference 317; Célestin Matte and others, 'Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?' in *Privacy Technologies and Policy* (Cham, Luís Antunes and others eds, Springer 2020). Both these studies find evidence that the use of legitimate interest as a legal basis is decreasing over time.

4.1.4 e-Privacy Directive and consent for tracking

Apart from the GDPR, the e-Privacy Directive (amended in 2009) requires consent for the use of tracking cookies and similar technologies. The European e-Privacy Directive says, roughly summarised, that cookies may only be placed after a website visitor has given his or her informed consent, unless those cookies are necessary for communication or to provide a requested service.[102] A website must also ask the visitor consent if third parties (such as advertising networks or social media companies) place cookies on the visitor's computer via the website.[103]

There are two exceptions to this consent rule. First, a website does not need to ask consent if a cookie is placed for the sole purpose of sending communication. For example, if a cookie is needed for the login procedure of an online bank, no consent is required. Second, consent is not required if a cookie is necessary to provide a service requested by the visitor. No consent is therefore required for cookies that are used, for example, for a virtual shopping cart. And no consent is required for a cookie that is placed when a visitor sets his or her language preferences for a website.

For the sake of readability, we speak of cookies, but the e-Privacy Directive applies to many more technologies. The rule applies as soon as a party places information (such as a cookie) on a user's device, or reads information from a user's device. The rule therefore also clearly applies to, for example, flash cookies (local shared objects) and some forms of device fingerprinting.[104]

Consent in the e-Privacy Directive must be interpreted as consent in the GDPR.[105] Hence, consent for cookies must comply with the GDPR's strict requirements for consent, for instance regarding sufficient information.

The CJEU adds that the information provided by the company operating cookies 'must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed.'[106] Moreover, 'the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.'[107] It 'must enable the data subject to be able to determine

[102] 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) (Official Journal L 201, 31/07/2002 P. 0037 – 0047), as amended by Directive 2006/24/EC [the Data Retention Directive], and Directive 2009/136/EC [the Citizen's Rights Directive], art 5(3). All references are to the consolidated version of 2009, and we refer to it as the e-Privacy Directive.

[103] Case C-49/17 *Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629 [102].

[104] The rule also applies, for example, when an app reads the contact list on someone's phone. See Authoriteit Persoonsgegevens, 'WhatsApp Non-Users Better Protected' (*Authoriteit Persoonsgegevens (Dutch DPA)*, 3 November 2015) <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-whatsapp-non-users-better-protected> accessed 26 January 2021.

[105] Article 2(f) of the e-Privacy Directive, consolidated version 2009.

[106] *Planet49* (n 62) [74].

[107] ibid.

easily the consequences of any consent he or she might give and ensure that the consent given is well informed'.[108]

The CJEU confirms that opt-out systems do not lead to valid consent for cookies: 'consent (...) is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.'[109]

If somebody gives consent for the placing of a cookie (as required by the e-Privacy Directive), he or she does not automatically give consent for related personal data processing.[110] So even after a company obtained consent for dropping a cookie on someone's device, the company still needs a legal basis for personal data processing if the company wants to use personal data for RTB or targeted advertising. Hence, if a company wants to use a tracking cookie for personal data processing for RTB or targeted advertising, both the privacy's consent requirement and the GDPR's requirement for a legal basis apply. In practice, a company could ask for consent for a cookie and consent for personal data processing in one consent request.[111]

4.1.5 Lifting the ban on using sensitive data

In many cases, there is yet another reason why RTB requires the consent of the data subject. As the UK DPA notes, RTB often concerns the processing of special categories of data, also called sensitive data.[112] Special categories of data are data about, for instance, someone's political opinions, health, or sexual preferences. In principle, the processing of such data is prohibited. The GDPR defines special categories of data as follows:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership (…), data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[113]

RTB can lead to the processing of special category data in several situations. For instance, visits to certain websites (Muslim news, Kosher recipes) can suggest somebody's likely religion. Visits to certain online newspapers can suggest

[108] Case C-61/19 *Orange Romania* ECLI:EU:C:2020:901 [40].

[109] *Planet49* (n 62) [74].

[110] See for more details: Frederik J Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: which legal basis?', International Data Privacy Law 2015-5-3, p. 163-176. See also ibid [69]–[70].

[111] The Working Party said in 2013: "[t]hough both consent requirements are simultaneously applicable (…) the two types of consent can be merged in practice (…)." Article 29 Working Party, 'Opinion 02/2013 on apps on smart devices' (WP 202) 27 February 2013, p. 14.

[112] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020.

[113] GDPR, art 9(1).

someone's political opinion, and visits to certain sites can give an indication of someone's sexual preferences.

The ban on using special categories of data can only be lifted under certain specific exceptions. For instance, hospitals can process medical data.[114] For adtech and RTB, the only available exception is the data subject's 'explicit consent'.[115]

In conclusion, for several reasons, a company doing RTB can only legally do so after the data subject's consent. To avoid misunderstanding — we are not arguing that informed consent is a panacea, nor that consent requirements are the best way to regulate RTB and adtech. Under what conditions less consent-focussed privacy and data protection law might protect privacy remains an interesting question — albeit one that falls outside the scope of this paper.

4.2 Can RTB comply?

As we argue that the lawful basis for RTB can only be consent, it is relevant how companies might go about obtaining consent. An important feature of consent is that is has to be established in relation to categories of data processed for a particular purpose by a particular controllership arrangement. So far, we loosely used the word 'controller' to refer to organisations using personal data, but we must rectify that sloppiness.

The GDPR is more precise: the controller is the 'body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[116] If 'two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'.[117]

Lawful bases in general cannot be transmitted between controllers, but have to be established by the controller(s) who are undertaking the processing. For example, the CJEU has stated that even where controllers' processing activities are aligned, such as in cases of joint controllerships, each must establish, justify and pursue their own legitimate interest in order for processing to be lawful.[118] For consent, this is doubly true, as consent is only valid if it is informed. The required information must include 'at least of the identity of the controller and the purposes of the processing for which the personal data are intended'.[119] The nature of the consent required has led to a particular institutional innovation in RTB systems — the consent management platform.

[114] GDPR, arts 9(2)(c), 9(2)(i).
[115] GDPR, art 9(2)(a).
[116] Article 4(7) of the GDPR.
[117] Article 26(1) pf the GDPR.
[118] *Fashion ID* (n 103) [96].
[119] GDPR, recital 42.

4.2.1 Consent management platforms

This understanding is part of the driver behind a recent trend within web tracking: the emergence of 'consent management platforms' (CMPs). Using these code libraries, which are embedded within webpages and, less frequently, within apps, a large number of third parties (the industry prefers the term 'vendors') simultaneously seek consent from a data subject in one action. Consent management platforms facilitate this single transactional moment, usually through user interface resembling banner or a barrier. They emerged in early 2018 as the GDPR became enforceable, with the market characterised by a small handful of main players.[120]

The attempt to get simultaneous consent can, and does end up with consent sought for hundreds of vendors at once. A recent study used web scraping to look at the five largest consent management platforms in the field, and found a median number of 315 vendors from whom consent is requested at once.[121] At the time of the study in late 2019, the largest consent management platform by market share, QuantCast, was nearly always configured to request consent for 542 vendors with a single click.[122] The identity of these vendors changes and fluctuates over time.[123]

The CMP approach has several problems which result in questions around its legality, which we will discuss below.

4.2.2 Inability to withdraw consent as required by law

Consent management platforms seem to breach the GDPR's requirement that consent be 'as easy to withdraw as to give'.[124] Let us have a look at the common standard for consent management platforms across the industry, the *Transparency and Consent Framework* co-ordinated by the Interactive Advertising Bureau (IAB). The IAB is the industry body who co-ordinate the actors in much of the RTB ecosystem, enabling the processing to be carried out through the standardisation, monitoring and continued negotiation of the *OpenRTB* protocol. The IAB also seeks to assure data protection authorities that RTB is compliant with the law through contractually limiting and shaping the means and purposes of processing of actors within the ecosystem using its *Transparency and Consent Framework*. The latest version of the Framework is 2.0, and it is this version that is being analysed here.

The IAB Transparency and Consent Framework sets up a system whereby consent management platforms can be automatically queried by vendors embedded on a website to get the current data protection status of a visitor to that

[120] Hils and others (n 101) 324.

[121] Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020), 5.

[122] ibid.

[123] Hu and others (n 9); Hils and others (n 101).

[124] GDPR, art 7(3).

page, such as whether they have been disclosed the identity of that vendor, whether they have expressed their consent to that vendor and similar variables. The idea is that if such a query to the consent management platform indicates the vendor is permitted to access and place information on the user's terminal device and process their personal data, the vendor can proceed to do so.

There is a flaw with this system, however. Imagine a user who consents to the processing of personal data of TRACKERA and TRACKERB on WEBSITE1. TRACKERA and TRACKERB query the consent management platform embedded on the website, which informs them that consent has been established, and as a consequence, cookies are laid and read from their browser by TRACKERA and TRACKERB, and personal data that is collected linked to these identifiers is processed server-side. The user later revisits WEBSITE1, and altering their settings, refuses tracking by TRACKERA and TRACKERB. Again, both trackers query the consent management platform, which this time tells them they are not permitted to read data from the browser, nor permitted to process personal data on the basis of consent. Neither trackers therefore link the user who withdrew consent to the same, original time that user gave it.

Such a scenario does not pose problems in relation to the ePrivacy Directive, as, in accordance with the law, the trackers did not store or access data on the terminal device following the withdrawal of consent. It does, however, create a problem with the GDPR, as despite the consent being withdrawn, both trackers have not had this result actively communicated to them in relation to that user. They continue to — now illegally — process personal data despite the withdrawal of consent by the user.[125]

Another, related problem can be observed when the user moves between websites. Assume the user has consented to TRACKERA processing data on WEBSITE1, but on WEBSITE2, refuses consent to TRACKERA. Under the IAB Transparency and Consent Framework, WEBSITE2 can store this refusal 'locally', in its own cookie, rather than updating the 'global' consent string that is stored across websites on a cookie linked to the IAB-managed *consensu.org* server. As a result, the later refusal of consent elsewhere does not pass across websites. Even if it did, it still suffers from the problem described above where the consent refusal in practice only relates to the accessing and reading of data on the terminal device, rather than the server-side processing in the tracking ecosystem.

The European Data Protection Board notes that '[i]f the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR.'[126] Consequently, it seems questionable

[125] The European Data Protection Board note that 'As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.'. See Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP259 rev.01, 10 April 2018) 22.

[126] ibid.

whether the consent management platform consent mechanism has provided lawful consent since its introduction by the IAB in 2018 in the first Transparency and Consent Framework.

4.2.3 The impossibility of 'global' consent to RTB infrastructure

The IAB, as part of its coordination function, has put its weight behind a 'global' consent mechanism. Under these proposals, a cookie placed by a consent management platform via a subdomain of an IAB-controlled website (consensu.org) contains a 'global consent' signal that a consent management platform accepts as valid across all websites. There is also the recently introduced notion of an 'out-of-band' lawful basis, which supposes the possibility of a tracker to obtain a lawful basis outside of the IAB Transparency and Consent Framework's consent management platform system.

An analysis of the interaction of consent and joint controllership gives reason to question the legality of this arrangement.

The CJEU has held that in the context of embedded Web trackers, key technologies for RTB, a webpage will be a joint controller with the entity processing personal data using this tracker.[127] The predecessor of the European Data Protection Board, the Article 29 Working Party, has said since 2010 that a website publisher and a tracking company are generally joint controllers, if the company operates tracking cookies via that website.[128]

At the time of writing, compliance with the CJEU ruling seems questionable, as companies such as Google still insist they operate 'independent' controllership operations – and interpretation that seems hard to square with the CJEU judgment.[129] Given that the facts specifically concern the technologies and commercial situations of the tracking infrastructures discussed in this article, it seems difficult for companies to question the applicability of the CJEU judgment to online tracking and RTB.

A consequence of the CJEU judgment is that every webpage–tracker combination constitutes a distinct controllership arrangement, even where the tracker company operates across multiple websites in relation to the same data

[127] *Fashion ID* (n 103) [84]–[85].

[128] Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' (WP 171), 22 June 2010, p. 12: 'publishers will be joint controllers if they collect and transmit personal data regarding their visitors such as name, address, age, location, etc to the ad network provider.'

[129] See eg Google, 'Tools to Help Publishers Comply with the GDPR' (*Google Ad Manager Help*, no date) <https://support.google.com/admanager/answer/7666366?hl=en> accessed 3 January 2020. The authors cannot find any discussion of joint controllership in tracker documentation by Facebook, who were implicated directly in *Fashion ID* (n 103), however Facebook have added a 'joint controller addendum' to their Facebook 'Page' product in response to Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388, as have other companies such as LinkedIn (Microsoft) in relation to their similar products. See Facebook, 'Page Insights Controller Addendum' (*Facebook*, no date) <https://www.facebook.com/legal/terms/page_controller_addendum> accessed 3 January 2020; LinkedIn, 'LinkedIn Pages Joint Controller Addendum' (*LinkedIn*, no date) <https://legal.linkedin.com/pages-joint-controller-addendum> accessed 3 January 2020.

subject. Consent necessary to legitimise this personal data processing (and the interaction with devices under the ePrivacy Directive) relates at least in part to a joint controllership situation.

For example, two companies running a research project jointly on the basis of consent could not swap a joint controller out for another, which may not be trusted by the data subject, without re-establishing a lawful basis. If this were possible, it could even be envisaged in stages that a joint controllership arrangement would contain none of the original controllers that established consent in the first instance.

'Global' consent would hold that a publisher would, instead of collecting consent itself, look to an inherited cookie read by a third-party, the IAB domain *consensu.org*, and assume that consent as applicable to its own joint controllership operation. This, firstly, would directly contradict the finding of the CJEU in *Fashion ID*, which stated that

> it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data.[130]

Furthermore, it would be invalid to equate the consent of one joint controllership operation with another, as in the former, the data subject was informed about a different set of controllers. In this new, separate controllership operation, different controller(s) are in play, and consequently the previous consent is not 'informed' in relation to this operation.

Santos, Bielova and Matte argue on the basis of the judgments in *Deutsche Telekom*[131] and *Tele2 and Others*[132] that consent can be transferred between publishers.[133] They do not elaborate on this argument in detail, but the difference in circumstances and legal context between those judgments and the issue at hand make the argument unconvincing. Both cases relate to a specific aspect of the e-Privacy regime in a telecommunications context where consent is mandatory, relating to whether fresh consent is required to republish the information of a telephone subscriber in a public telephone directory owned by a new organisation. The Court leans heavily in *Deutsche Telekom* on the Advocate General's opinion. In teleological analysis, she notes that a purpose of the public directory elements of the e-Privacy Directive is to ensure the existence of a comprehensive public directory, and that the provisions on transfer of consent must be interpreted in this context such that this purpose is not 'severely compromised'.[134] There is no

[130] *Fashion ID* (n 103) [102].

[131] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* ECLI:EU:C:2011:279.

[132] Case C-536/15 *Tele2 (Netherlands) BV and Others v Autoriteit Consument en Markt (ACM)* ECLI:EU:C:2017:214.

[133] Cristiana Santos and others, 'Are Cookie Banners Indeed Compliant with the Law? ': [2020] Technology and Regulation 91, 109.

[134] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* ECLI:EU:C:2011:90 (Opinion of AG Trstenjak) [126].

equivalent EU legislation aiming at comprehensive online tracking — indeed, the GDPR specifically highlights online advertising as an example of an application where the "proliferation of actors and the technological complexity of practice" make it hard for data subjects to understand "by whom" data is processed.[135] Taking an opportunity to inform data subjects of this away would appear to go against the specific aims of the law, rather than act in concert with it.

Lastly, it would be unwise for publishers to accept this situation, as they would incur significant liability for invalid consent gathered elsewhere. Global consent IAB cookies can, and are, forged, as the empirical study by Matte, Bielova and Santos has demonstrated.[136] The publisher accepting global consent would have no proof that consent was ever obtained. The publisher would also be liable as part of a joint controllership operation for a legal action undertaken on the basis of accepting this unverified consent signal, even were it to be theoretically possible to accept as valid.

4.2.4 Too many parties for valid consent

Modern consent management platforms operate as to make even 'the identity of the controller and the purposes of the processing for which the personal data are intended' too much information to feasibly expect the data subject to be able to read. This is problematic, as consent must be 'informed' — a distinction that is clearer in the French text of the GDPR, which states that consent must be *éclairée* (enlightened or illuminated) rather than simply *informé*, which places the emphasis on the mental state of the data subject rather than the act of having provided information, regardless of its eventual use. Not including the time to operate the interface, or to click on nested privacy policies, a recent empirical study estimated that reading the basic data for all vendors would take on average 40 minutes per website.[137] This is clearly not conducive to placing the average data subject in an enlightened position. The Court has stated that information "must enable the data subject to be able to determine easily the consequences of any consent" and "ensure that the consent given is well informed".[138]

Moreover, the overarching fairness principle of the GDPR places a focus on creating an enabling environment for autonomous choice and the exercise of data rights, conscious of information asymmetries in the digital environment.[139] Clifford, Graef and Valcke argue that the fairness principle, and its corresponding manifestation in Article 7, 'appears to establish a burden of care on controllers regarding their responsibility to ensure data subjects have been informed and

[135] GDPR, recital 58.

[136] Célestin Matte and others, 'Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework' [2019] arXiv:191109964 [cs].

[137] Nouwens and others (n 121) 6.

[138] *Orange Romania* (n 108) [40].

[139] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130, 139–40.

understand the provided information'.[140] This is reinforced by the way the legislator specified separately from Article 13 information requirements the minimal information needed for consent to be informed ('at least of the identity of the controller and the purposes of the processing for which the personal data are intended'[141]). This seems to be designed assuming that this information, at minimum, *must be feasible* for the data subject to assess before a consent choice.

As a consequence, with the number of vendors the real-time bidding system requires, consent management platforms cannot be used to obtain valid consent. This view has recently been echoed by the UK Competitions and Markets Authority:

> [I]t is challenging for intermediaries that do not offer user-facing services to obtain consent. At the extreme, this could mean that third-party intermediaries would need to radically reduce the number of other parties they shared a consumer's personal data with to a level the consumer could realistically understand so as to give valid consent to targeted personalised advertising.[142]

In conclusion, the GDPR and the ePrivacy Directive require consent for RTB. Current practices by companies engaged in RTB rarely, if ever, lead to valid consent. Indeed, it seems questionable whether it is possible at all to obtain valid consent for RTB.

5 Transparency

5.1 The GDPR's transparency requirements

The first of the six overarching principles of EU data protection law is the lawfulness, fairness and transparency principle. It says that '[p]ersonal data shall be (...) processed lawfully, fairly and in a transparent manner in relation to the data subject'. Case law of the CJEU and the European Court of Human Rights confirms the importance of transparency.[143] Since the 1970s, transparency has

[140] Damian Clifford and others, 'Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) 20 German Law Journal 679, 685.

[141] GDPR, recital 42.

[142] Competitions and Markets Authority (n 31) 213.

[143] *Tele2/Watson* (n 77) [100]. 'The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance'. Case C-201/14 *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others* ECLI:EU:C:2015:638 [33]: 'the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed'. *Bărbulescu v Romania* ECLI:CE:ECHR:2017:0905JUD006149608, para 133: 'The Court considers that to qualify as prior notice, the warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees' communications. International and European standards point in this direction, requiring the data subject to be informed before any monitoring activities are carried out (…)'.

been seen as a core principle for data protection law.[144] It has been suggested that mitigating the abuse of information asymmetry is data protection law's main goal.[145]

Article 13 and 14 of the GDPR list information that the data controller must give to the data subject to ensure transparency. The data controller can provide the information, for instance, in a privacy notice on a website.[146] The data controller must give this information regardless of the legal basis for processing. (Article 13 applies when a firm collects data from the data subject; article 14 applies where the data have not been obtained from the data subject. Both provisions require largely the same information. The main difference is the moment at which the information must be given.)

The information that is always required includes: the processing purpose,[147] 'the identity and the contact details of the controller',[148] and 'the recipients or categories of recipients of the personal data, if any'.[149]

Article 12 says that '[t]he controller shall take appropriate measures to provide [such] information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.

The preamble adds that information about personal data processing should be 'easily accessible and easy to understand'. And 'natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.'[150] Recital 58 adds that clear information is especially important in the context of online advertising, where the number of actors and the complicated technology may confuse the data subject:

[144] For instance, a Council of Europe resolution from 1973 said: 'As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information' (Committee of Ministers, Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973, para 6). A resolution from 1974 said: 'As a general rule the public should be kept regularly informed about the establishment, operation and development of electronic data banks in the public sector' (para 1). And: 'As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information' (para 6), Committee of Ministers, Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974. And the United States Department of Health, Education, and Welfare mentioned transparency as one of the classic Fair Information Principles in 1973: 'There must be no personal-data record-keeping systems whose very existence is secret' (United States Department of Health, Education, and Welfare 1973, 'Records, Computers, and the Rights of Citizens' (1973) US Government Printing Office, https://www.justice.gov/opcl/docs/rec-com-rights.pdf accessed 12 May 2020).

[145] Paul De Hert P and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes E, Duff A and Gutwirth S (eds), Privacy and the Criminal Law (Intersentia 2006). See also Frederik J Zuiderveen Borgesius, *Improving privacy protection in the area of behavioural targeting* (Information Law Series, Kluwer Law International 2015), section 4.3.

[146] GDPR, art 12(1) states that '[t]he information shall be provided in writing, or by other means, including, where appropriate, by electronic means.'

[147] GDPR, art 13(1)(c).

[148] GDPR, art 13(1)(a).

[149] GDPR, art 13(1)(e).

[150] The requirement to inform the data subject about risks is not included in arts 12–14 of the GDPR.

> The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. *This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.*[151]

The European Data Protection Supervisor has given guidance regarding the GDPR's transparency requirements.[152]

5.2 Can RTB comply?

Do current RTB practices comply with the GDPR's transparency requirements? And if not: would it be theoretically possible for RTB practices comply with the GDPR's transparency requirements?

We suggest that the answers are: No, currently, all RTB practices seem to be too opaque, and therefore in breach of the GDPR. The UK DPA notes that 'in RTB the privacy information provided often lacks clarity and does not give individuals an appropriate picture of what happens to their data.'[153] More worryingly, it seems almost impossible to make RTB comply with the GDPR's transparency requirements.

We start with the clearest transparency requirements of the GDPR. As noted, the controller must always provide 'the identity and the contact details of the controller'.[154] We recall that website publishers and cooperating RTB companies are joint controllers. Hence, if somebody visits a website, the publisher must tell that web user the identity of each joint controller – hence, of each company engaged in RTB concerning that website visit.

However, with RTB it is often impossible for the website publisher to predict who will win an auction. Therefore, the publisher does no know in advance which companies (such as advertising networks) will show ads on the site. Neither does the publisher know which companies will collect data via the site.

Indeed, the IAB confirms that it is impossible to tell website visitors in advance which companies will collect his or her data in an RTB scenario. The IAB sent a lobbying document to the European Commission, outlining why the IAB thinks that proposals for a new ePrivacy Regulation (that is supposed to replace

[151] Emphasis added.
[152] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679', WP260 rev.01 (11 April 2018).
[153] Information Commissioner's Office (n 45) 19.
[154] GDPR, art 13(1)(a).

the ePrivacy Directive) would mean the end of RTB. The document became public after a freedom of information request.[155] The IAB writes:

> As it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario, programmatic trading, the area of fastest growth in digital advertising spend, would seem, at least prima facie, to be incompatible with consent under GDPR.[156]

Sometimes, website publishers were surprised themselves about which parties were present on their sites. The chairman of the US Association of Online Publishers said: 'As a publisher we feel we've been raided by the ad industry. We've done site audits and been flabbergasted by how many third party cookies have been dropped on our site by commercial partners – they were stealing our data.'[157]

In sum, currently, it appears that a website publisher who partners with RTB companies cannot inform visitors about who will collect data about them. Moreover, it appears that it is impossible to inform website visitors about the identity of RTB companies who will collect visitors' data. As noted previously, companies engaged in RTB through a website are generally joint controllers with the website publisher.[158] If the website publisher cannot tell the website visitor the identity of the joint controllers, the publisher cannot comply with the GDPR's requirement to provide 'the identity and the contact details of the controller'.[159]

'Given the complexity and opacity of the RTB ecosystem,' notes the UK DPA, 'organisations cannot always provide the information required, particularly as they sometimes do not know with whom the data will be shared.'[160] The UK DPA notes that 'RTB also involves the creation and sharing of user profiles within an ecosystem comprising thousands of organisations.'[161]

But suppose that one doubts whether all RTB partners must indeed be seen as a joint controller. Would such an interpretation make a difference? Probably not. The GDPR requires each controller to tell the data subject the 'the recipients

[155] https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/#evidence

[156] https://brave.com/wp-content/uploads/2019/02/1b-IAB-2017-paper.pdf

[157] Hall E, 'Marketers Could Be Hit by Tough New Data Laws for EU' (Adage) (2013) <http://adage.com/article/global-news/marketers-hit-tough-data-laws-eu/244674/> accessed 10 May 2020.

[158] See section 4.2.1.

[159] GDPR, art 13(1)(a).

[160] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020. A Dutch publisher of a website with hundreds of thousands of visitors each month said in an interview: 'I don't have any insight into what third parties are collecting on our site. I trust that those companies behave responsibly'. Martijn M, 'Big Business is watching you' (2013), <https://decorrespondent.nl/66/Big-Business-is-watching-you/3214002-df572412> accessed 10 May 2020 (our translation).

[161] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020, p. 20.

or categories of recipients of the personal data, if any'.[162] If an RTB company cooperates with a website publisher, but should not be seen as a joint controller, the company is a 'recipient'.[163] Following the same logic as above, the publisher cannot tell the data subject who the recipients are, as the publisher does not know I advance who will receive data about the web user. Could a publisher tell the data subject merely the 'categories of recipients'?[164] A publisher might argue that it could comply by saying something like:

> We may share your personal data with advertising networks, supply-side platforms, supply-side platforms, and advertising exchanges.

It is unlikely that such a statement would comply with the GDPR. As noted, controllers must provide information in a 'transparent, intelligible and easily accessible form, using clear and plain language'.[165] And the GDPR's preamble says that user-friendly information is particularly important 'in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.'[166] Presumably, most website visitors do not know what 'supply-side platforms' are, and do not understand what RTB entails. Indeed, a study on RTB commissioned by the UK's Information Commissioner's Office and Ofcom on how users' perceptions of the acceptability of RTB advertising online changed after it was briefly explained to them how it worked. Acceptability initially stood at 63% pre-explanation, yet fell to only 36% after an explanation was provided.[167]

In theory, a publisher could set up a system in which the publisher cooperates with only five companies for displaying ads. In theory, an RTB-like system could be developed, in which those five companies compete in an automated auction. In such a situation, the website publisher could tell the visitor which five companies could collect data about the visitor. Assuming that the publisher can explain for which purposes those companies process the personal data etc., such a system could perhaps comply with the GDPR's transparency requirements. But for the moment, we are not in this situation.

All in all, it appears that website publishers and companies engaged in RTB generally do not comply with the GDPR's transparency requirements. Moreover, complying with the GDPR's transparency requirements would only be possible if

[162] GDPR, art 13(1)(e).

[163] GDPR, art 4(9) states that "recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. (...)'

[164] GDPR, art 13(1)(e).

[165] GDPR, art 12(2).

[166] GDPR, recital 58.

[167] Michael Worledge and Mike Bamford, 'Adtech: Market Research Report' (ICO and Ofcom, March 2019) 19.

changes were made to RTB practices. Such changes would have to limit, dramatically, the number or parties involved in RTB.

6 Security

6.1 The GDPR's security requirements

The GDPR's integrity and confidentiality principle could also have been called the security principle. It obliges data controllers to ensure 'appropriate security' for personal data, 'including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'[168] Since the early 1970s, data protection laws emphasise the importance of security and confidentiality of data.[169] The CJEU has suggested that security is part of the essence of the fundamental right to the protection of personal data.[170]

The GDPR does not require absolute security; the level of security must be 'appropriate'. When assessing which level of security is appropriate, controllers and processors should consider 'the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons'.[171] When assessing what an appropriate level of security is, adds the GDPR, 'account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'[172] The GDPR says that costs can be considered when deciding what level of security is appropriate.[173]

[168] GDPR, art 5(1)(f). See also recitals 39, 78, and 83.

[169] See for instance the Data Protection Act of the German state of Hessen (G V Bl.II 300-10, published at Wiesbaden, 12 October 1970, in Gesetz-und Verordnungsblatt für das Land Hessen [Laws and Regulations Journal], Part I, No. 41). Article 2 reads 'The records, data and results covered by data protection shall be obtained, transmitted and stored in such a way that they cannot be consulted, altered, extracted or destroyed by an unauthorized person. This shall be ensured by appropriate staff and technical arrangements.' See also art 3. Security was also mentioned in Committee of Ministers, *Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, 26 September 1973, paras 8 and 9, and in Committee of Ministers, *Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, 20 September 1974, paras 6 and 7.

[170] *Digital Rights Ireland* (n 76) [40].

[171] GDPR, art 32(1).

[172] GDPR, art 32(2) and recital 83.

[173] GDPR, art 32. Regarding costs, the CJEU noted in *Digital Rights Ireland* that the Data Retention Directive allowed telecom companies to 'to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures.' The CJEU appeared to disapprove of the possibility to consider costs when assessing the appropriate level of security. *Digital Rights Ireland* (n 76) [67].

CJEU case law also gives some guidance on the factors that should be considered when deciding how much security must be ensured.[174] The CJEU mentions a number of factors to consider when assessing which level of security is appropriate: (i) the quantity of personal data, (ii) the data's sensitivity, and (iii) the risks. The CJEU adds (iv) that a higher level of security is needed 'where personal data is subjected to automatic processing and (v) where there is a significant risk of unlawful access to that data.'[175]

6.2 Can RTB comply?

Can RTB companies comply with the GDPR's security requirements? For several reasons, the security requirements for RTB are high. We apply the CJEU's elements to assess what level of security is needed.

First, RTB concerns personal data of millions of people. As the UK DPA notes, 'Thousands of organisations are processing billions of bid requests in the UK each week with (at best) inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest.'[176]

Second, the data can be sensitive. For instance, the data can show which websites people visit and when. Case law of the European Court of Human Rights confirms that people have a reasonable expectation of privacy regarding their internet use,[177] and that 'information derived from the monitoring of a person's internet use' is covered by the right to private life in article 8 of the European Convention on Human Rights.[178]

As noted, someone's website visits may even suggest special categories of data (sometime called sensitive data).[179] Website visits may suggest one's medical condition (websites about obesity or wheelchair), one's political opinion (certain newspapers) or one's religion (sites with Kosher recipes).

Moreover, RTB usually involves storing or accessing cookies (or similar files) on the user's device, such as a computer or smart phone. The Court of Justice of the European Union says that the right to privacy protects the contents of people's devices: 'any information stored in the terminal equipment of users of electronic communications networks [is] part of the private sphere of the users requiring

[174] ibid [66] ('[The Data Retention] Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.') The CJEU repeated the three factors in a later judgments, *Tele2/Watson* (n 77) [122]; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791 [132]; Case C-623/17 *Privacy International* ECLI:EU:C:2020:790 [68].

[175] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [91].

[176] Information Commissioner's Office. 'Update report into adtech and real time bidding' (20 June 2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed on 14 May 2020, p. 23.

[177] *Copland v the United Kingdom* (n 95) para 42.

[178] *Bărbulescu v Romania* (n 143) para 72.

[179] GDPR, art 9.

protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.'[180]

Third, the risks are high. One risk is data leakage. Another risk is that bad actors publish ads, distributed through RTB, to spread malware. Indeed, there are several examples of ads spreading malware, ads that were placed on well-known websites. In sum, the legal security requirements are high in the context of RTB.

Fourth, RTB concerns automated processing, which, according to the CJEU, is a factor that calls for higher security.[181] Fifth, there is a risk of unlawful access to the data. The adtech industry, let alone the data subject, has hardly any control about what happens to people's data during RTB. As the UK DPA notes in a report on RTB:

> The nature of the processing is what leads to the risk of 'data leakage', which is where data is either unintentionally shared or used in unintended ways. Multiple parties receive information about a user, but only one will 'win' the auction to serve that user an advert. There are no guarantees or technical controls about the processing of personal data by other parties, eg retention, security etc. In essence, once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls.[182]

Many RTB companies could argue, however, that they implement at least one security measure. The GDPR says that controllers (and processors) must implement security measures, and gives four examples of possible measures. One of the examples is 'pseudonymisation'. If a company processes data about individuals but does not know their names, the company can reasonably argue that it only processes pseudonymous data.[183] However, merely pseudonymising data is not sufficient to comply with the GDPR's security requirements. As the UK DPA concludes about RTB, '[i]ndividuals have no guarantees about the security of their personal data within the ecosystem.'[184] In sum, currently, most RTB practices are breaching three core GDPR requirements, namely the requirements for a legal basis, transparency, and security.

[180] *Planet49* (n 62) [70].
[181] *Schrems I* (n 175) [91].
[182] Information Commissioner's Office (n 45) 20–21.
[183] See article 4(5) of the GDPR: '"pseudonymization" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.
[184] Information Commissioner's Office (n 45) 23.

7 Discussion

So far, this paper focused on positive law: asking what the law says. We showed that RTB breaches several aspects of the European data protection law. Now we take a step back and explore whether the law makes sense.

In theory, two scenarios are possible, (a) and (b). In scenario (a), many companies engaged in RTB breach the GDPR. RTB practices are wrong, and the law is right.

In theory, scenario (b) would also be possible. In scenario (b), RTB illustrates drafting mistakes in the GDPR. In other words, the law is wrong and RTB practices are right. In this scenario, the EU forgot to pay sufficient attention to the adtech industry while drafting the GDPR, and adopted rules (requirements for a legal basis, transparency, and security) that are outdated or otherwise wrong.

In our opinion, we find ourselves in scenario (a). Each of the three rules discussed in this paper (requirements for a legal basis, transparency, and security) make sense. For instance, the requirement of a legal basis for processing has been part of EU data protection law for twenty-five years. Apart from the that, the requirement is included in the Charter of Fundamental Rights of the European Union, so there is no serious chance that the requirement is abolished.

RTB companies might try to argue that they should be able to rely on the legitimate interests provision (rather than on consent). As explained in section 4, however, we think that argument will not work. In an earlier paper, one of us showed that under the 1995 Data Protection Directive, behavioural advertising can only be based on the legal basis consent.[185] If our claim back then was correct, surely RTB can only be based on consent. RTB is generally riskier and more privacy-invasive than behavioural advertising. Therefore, a claim that RTB can be based on the legitimate interests provision is even more implausible than a claim that behavioural advertising can be grounded on that legal basis.

Is the GDPR's transparency requirement unreasonable? Again, we think not. With good reason, the requirement of transparency regarding personal data usage has been a staple of data protection law since the 1970s. Data protection law aims, among other things, to impede abuse of information asymmetry. Some RTB companies might claim that while transparency in general is a laudable goal, the requirements as specified in the GDPR are too burdensome. We saw that the GDPR requires data controllers to tell their identity to data subjects.[186] In many RTB scenarios, website publishers cannot tell which RTB companies will collect or use data about the website visitors. However, it seems unwise to abolish the requirement that data controllers must disclose their identity. Apart from that, it seems implausible that the EU would abolish that rule in a revision of the GDPR.

[185] Zuiderveen Borgesius (n 50) 163–76.
[186] See section 5.

Lastly: are the GDPR's security requirements unreasonable? Again, we think not. Data security has been a core tenet of data protection law since the 1970s, and rightly so. It would be ill-advised to abolish or lower the GDPR's security requirements. Apart from that, it is unlikely that the EU would so do. In sum, in our opinion, the non-compliance of RTB with the GDPR is not the fault of the GDPR.

As an aside, RTB companies should not have been surprised that their practices run afoul of the GDPR. The requirements for a legal basis, transparency, and security were included in the 1995 Data Protection Directive too. So, also under the old regime, any data protection lawyer could have told RTB companies that they were on thin ice from a compliance perspective.

7.1 Enforcement

How is it possible that such a large breach of the GDPR exists? We briefly highlight a few possible explanations. The compliance deficit in the RTB sector can be largely explained by an enforcement deficit. DPAs have hardly enforced the law in this sector. True, there are exceptions. For instance, the French DPA has given a fine of 50 million Euro to Google for not properly explaining what it does with people's personal data.[187] Nevertheless, enforcement against RTB companies is rare. Why is there a lack of enforcement? We suggest a few possibilities.

First, DPAs are understaffed and overwhelmed. The GDPR applies to uncountable situations in which personal data are used, and DPAs are supposed to oversee compliance in many sectors.

Second, when the 1995 Data Protection Directive still applied (until May 2018), there was more ambiguity about several data protection rules. For instance, RTB companies could – back then – try to argue that the nameless, pseudonymous, data they used fell outside the scope of data protection law. And RTB companies could have tried to argue that opt-out systems could be used for consent. Such arguments would not have been convincing, but the old rules were vaguer than the GDPR's. Perhaps some DPAs were hesitant to impose sanctions in cases that were likely to lead to long and costly litigation. Several players in the RTB sector have deep pockets and can afford lengthy litigation.

Third, until the GDPR was applicable, many DPAs did not have the power to impose serious fines. Therefore, some companies may have decided that it's rational to make profits in breach of data protection law – after all, the chance of enforcement was low, as was the maximum fine. And DPAs may have thought that investigating this complicated sector was not worth the effort.

Fourth, some RTB companies may be established outside Europe, which makes enforcement harder. The GDPR does often apply to companies established

[187] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

outside the EU, but nevertheless, enforcement may be harder than enforcement against a company established in the EU.

Fifth, some companies engaged in RTB are formally established in Ireland. The DPA in Ireland, however, is understaffed. And the Irish DPA is sometimes accused of preferring a light touch approach over hard enforcement. Some commentators speak of the 'Ireland loophole' in EU data protection law.[188] Sixth, the GDPR is applicable since May 2018, so perhaps it should not be too much of a surprise if certain sectors are not fully compliant yet.

Sixth, the RTB ecosystem has been left to illegality for so long, it has formed a large, interwoven system that is difficult to regulate using the toolbox of data protection. Data protection legislation draws its heritage from the regulation of databanks, where the controller was clear. In the RTB environment, it is unclear that removing or applying sanctions to any one actor would drive the system into a different state, given the reinforcing effects of the current structure on data collection and sharing practices. Any DPA must act at scale, potentially in relation to many actors at once, which brings daunting issues of capacity, both inside the regulator and in relation to a slow justice system, given the likelihood of appeals in such existential cases for the industry.

While such factors might help to explain the lack of enforcement, the situation is not acceptable. We call upon DPAs to enforce the law in the adtech sector.

DPAs do not have to enforce the law against all companies engaged in RTB. A couple of serious fines against a couple of companies may already help compliance. If one company gets fined, others see that non-compliance can be costly. In many sectors, compliance improved dramatically with data protection law, because the GDPR (unlike the previous law) enabled serious fines. But of DPAs continue non-enforcement, many companies, also in other sectors, might think that they can break the law with impunity. Some companies may choose to break the law if the expected profit from breaking the law is higher than the chance of being fined, multiplied with the expected fine. Therefore, the possibility of high fines is not enough. There must be a credible chance of enforcement.

In the long term, alternative business models are needed online to fund journalism, websites, and other services.

ePrivacy Regulation

The EU has debated additional rules for privacy on the internet, including rules for the adtech sector. In 2017, the European Commission presented a proposal for an ePrivacy Regulation, which should replace the ePrivacy Directive. Especially after amendments by the European Parliament, the proposed ePrivacy Regulation included promising ideas to regulate adtech. For instance, the Parliament suggested to make compliance with Do Not Track and similar signals

[188] Jan-Philipp Albrecht, '#EUdataP State of the Union,' (speech at the Chaos Communication Congress, 2013) <http://www.janalbrecht. eu/fileadmin/material/Dokumente/30C3-JPA-EUdataP.pdf>.

obligatory for all parties. In such a scenario, people could choose a 'Do not track me' setting once, in their computer (browser), on their phone, or on another device.[189] Like that, people would not have to give or withhold consent to many different consent requests. But at the moment, it is unclear whether, when, and in what form an ePrivacy Regulation will be adopted.

8 Conclusion

In conclusion, we assessed whether ad tech and real-time bidding (RTB) complies with three rules from the GDPR, the requirement for a legal basis, transparency, and security. We showed that for each of the requirements, most RTB practices do not comply. Indeed, it seems close to impossible to make RTB comply.

First, the EU Charter of Fundamental Rights and the GDPR require data controllers, organisations that use personal data, to have a legal basis, such as consent, for that data use. We showed that in virtually all situations, the only available legal basis for RTB is the data subject's prior consent. Moreover, the ePrivacy Directive requires consent for cookies and similar tracking techniques. In practice, RTB companies rarely obtain valid consent. We also showed that it is hard for companies to obtain valid informed consent for RTB. One of the problems is that it is difficult for companies to explain to internet users what will happen to their data in an RTB scenario.

Second, the GDPR requires that data controllers are transparent about what will happen to the data subject's data, regardless of they want to obtain the data subject's consent. Controllers must provide clear, plain, and intelligible information. Here, data controllers run into similar problems as under the requirements for informed consent. The data controller must disclose, among other things, its identity to the data subject. If a website publisher cooperates with RTB companies, CJEU case law shows that those companies must be seen as joint controllers. Hence, the website publisher must also disclose the identity of all the RTB partners. However, with RTB, a website publisher often does not know in advance who will collect data on its site. The publisher thus cannot disclose the identities of the joint controllers to website visitors. More generally, it seems doubtful whether publishers can ever explain RTB to visitors.

Third, the GDPR requires appropriate security for personal data processing, including protection against unauthorised or unlawful processing. Appropriate security is extra important, as RTB concerns intimate data about millions of people. It seems doubtful whether RTB companies could meet de GDPR's security requirements.

[189] See Frederik J Zuiderveen Borgesius, Joris van Hoboken, Ronan Fahy, Kristina Irion, Max Rozendaal, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, European Parliament, May 2017).

In sum, RTB is difficult to reconcile with core tenets of the GDPR. We call upon DPAs to enforce the GDPR in the adtech sector.

* * *