Information Commissioner's Office

Update report into adtech and real time bidding

20 June 2019

ico.
Information Commissioner's Office

Contents

Commissioner's foreword

As the UK's regulator responsible for data protection, we want people to have confidence in how their data is being used, even in complex online systems.

That's why my office has made looking at the adtech sector a priority. Many people will not have given a moment's thought to the complex process that leads to advertisements appearing on the webpages and apps they use, but behind the scenes is a complex and large scale system.

When you visit a website, some of the ads you see have been specifically selected for you. As the site was loading, the website publisher auctioned a space on the page you are viewing, and an advertiser bought it because it specifically wants to reach people like you. The process can involve many companies, and happens in milliseconds. Billions of online ads are placed on webpages and apps in this way every day.

The process – known as real time bidding – relies on the potential advertiser seeing information about you. That information can be as basic as the device you're using to view the webpage, or where in the country you are. But it can have a more detailed picture, including the websites you've visited, what your perceived interests are, even what health condition you've been searching for information about.

That use of personal data is why the ICO has published this report.

Our work began by examining how people's personal data was used and shared. More specifically, we wanted to see if that process complied with the law – both General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR). For example, the GDPR has clear requirements for transparency. The law also requires organisations to have a lawful basis to process your personal data, and it requires information to be kept secure.

To help answer our questions, we spoke to the different parts of the industry, from publishers to advertisers, from civil society to start ups, from adtech firms to legal counsel. We brought together more than a hundred people for a full day fact-finding event in London. We considered concerns we'd received from consumers about how their data was being handled.

What we found was an industry that understood it needed to make improvements to comply with the law. Our report today sets out where we expect to see change, and sets out the timescales in which we expect to see action.

We set out our concerns about sensitive data – known as 'special category data' in the GDPR – being shared and used without people's consent.

We list our concerns - that the creation and sharing of personal data profiles about people, to the scale we've seen, feels disproportionate, intrusive and unfair, particularly when people are often unaware it is happening.

We outline that one visit to a website, prompting one auction among advertisers, can result in a person's personal data being seen by hundreds of organisations, in ways that suggest data protection rules have not been sufficiently considered.

Our report will be passed to the adtech sector for their response. We are clear about the areas where we have initial concerns, and we expect to see change. But we understand this is an extremely complex market involving many organisations and many technologies. We want to take a measured and iterative approach, before undertaking a further industry review in six months' time.

With that in mind, we'll continue engaging with the sector, further exploring the data protection implications of the real time bidding system. We'll continue collaborating with Data Protection Authorities in other European countries too, who are also looking at complaints in this area.

Innovation in technology has the potential to enhance all of our lives. The internet is central to that, and we understand that advertisements fund much of what we enjoy online. We understand the need for a system that allows revenue for publishers and audiences for advertisers. We understand a need for the process to happen in a heartbeat. Our aim is to prompt changes that reflect this reality, but also to ensure respect for internet users' legal rights.

The rules that protect people's personal data must be followed. Companies do not need to choose between innovation and privacy.

Elizabeth Denham

Information Commissioner

1. Executive summary

Real-Time Bidding (RTB) is a set of technologies and practices used in programmatic advertising. It has evolved and grown rapidly in recent years and is underpinned by advertising technology (adtech), allowing advertisers to compete for available digital advertising space in milliseconds, placing billions of online adverts on webpages and apps in the UK every day by automated means.

Whilst RTB is only part of the online advertising ecosystem, we decided we needed to investigate further due to its complexity and scale, the risks posed to the rights and freedoms of individuals and the concerns we've received.

This update report therefore clarifies the ICO's views on adtech, specifically the use of personal data in RTB, and our intended next steps. The findings have come from our:

- research undertaken as part of our Technology Strategy[1];
- stakeholder engagement with industry;
- consideration of concerns we have received[2]; and
- recent Fact Finding Forum (where participants from across the adtech industry met to discuss lawful basis, transparency and security challenges)[3].

While many RTB market participants place some controls on their processing and sharing of personal data, it's become apparent during our work that there are substantially different levels of engagement and understanding of how data protection law applies, and the issues that arise.

Our initial investigations raised a number of concerns with the data protection practices within RTB. For the purposes of this report we have prioritised the following areas:

- **Transparency and consent:** The protocols used in RTB include data fields that constitute special category data, which requires the explicit consent of the data subject. Furthermore, current practices remain problematic for the processing of personal data in general, even if the special category data were removed. For example:
    - identifying a lawful basis for the processing of personal data in RTB remains challenging, as the scenarios where legitimate interests could apply are limited, and methods of obtaining

[1] https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf
[2] Specifically, the concerns raised by Michael Veale, Jim Killock and Dr Johnny Ryan made in September 2018 (https://brave.com/adtech-data-breach-complaint) and by Privacy International in November 2018 (https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what).
[3] See https://ico.org.uk/about-the-ico/research-and-reports/adtech-fact-finding-forum/ and https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-fact-finding-forum-shows-consensus-on-need-for-change/

consent are often insufficient in respect of data protection law requirements;

- the privacy notices provided to individuals lack clarity and do not give them full visibility of what happens to their data;
- the scale of the creation and sharing of personal data profiles in RTB appears disproportionate, intrusive and unfair, particularly when in many cases data subjects are unaware that this processing is taking place; and
- it is unclear whether RTB participants have fully established what data needs to be processed in order to achieve the intended outcome of targeted advertising to individuals. The complex nature of the ecosystem means that in our view participants are engaging with it without fully understanding the privacy and ethical issues involved.

- **Data supply chain**: In many cases there is a reliance on contractual agreements to protect how bid request data is shared, secured and deleted. This does not seem appropriate given the type of personal data sharing and the number of intermediaries involved.

Our prioritisation of both RTB and the above issues in this report is not an indication that we think other areas in adtech and online advertising are 'issue-free' in terms of data protection. Additionally, we are aware of the wide range of non-data protection issues that are also associated with RTB and adtech more generally, including fraud (eg from the use of 'bots'), the market dominance of so-called 'big tech' firms, and the financial vulnerability of some publishers; these are also beyond the scope of this report. This report is issued as part of our role as the data protection regulator; however, these other issues, to the extent they impact on data protection,, have been considered as factors in determining our next steps.

Our work has highlighted the lack of maturity of some market participants, and the ongoing commercial incentives to associate personal data with bid requests. We do not think these issues will be addressed without intervention. We are therefore planning a measured and iterative approach, so that we act decisively and transparently, but also in ways in which we can observe the market's reaction and adapt our approach accordingly. This is because:

- this is an extremely complex market involving multiple technologies and actors – and we will doubtless learn more going forward;
- there are some industry initiatives to address these challenges that may gain further impetus and adoption following our initial interventions;
- there are additional considerations, in particular the economic vulnerability of many smaller UK publishers, which make it advisable for us to move carefully and observe the consequences of our actions; and

- adtech continues to grow and develop rapidly, and is spreading beyond the online environment – ensuring appropriate and responsible data protection practices is crucial.

As part of this approach, we intend to provide market participants with an appropriate period of time to adjust their practices. After this period, we expect data controllers and market participants to have addressed our concerns.

In the short term, we will:

- obtain further detailed submissions from a sample of data controllers on their management of bid request data, to enhance further our understanding of industry practices;
- further consult with IAB Europe and Google about the detailed schema they are utilising in their respective frameworks to identify whether specific data fields are excessive and intrusive, and possibly agree (or mandate) revised schema; and
- continue to share information with other data protection authorities across Europe and identify opportunities to work together where appropriate.

2. Introduction

2.1 What are adtech and RTB?

Adtech is a term used to describe tools that analyse and manage information (including personal data) for online advertising campaigns and automate the processing of advertising transactions. It covers the end-to-end lifecycle of the advertising delivery process, which often involves engaging third parties for one or more aspects of these services, although some advertising is still placed directly between advertisers and publishers.

Use of adtech may enable:

- advertisers to reach new audiences, increase the speed at which an advertisement reaches its audience, reduce the cost of campaigns and make the success of an advertising campaign more measurable;
- publishers to drive increased revenue by increasing the number of potential buyers for advertising space they want to sell, thereby increasing the value of individual advertising space sold, and selling advertising space that would otherwise not be sold; and
- intermediaries to make money through providing services to others in the ecosystem such as agencies and publishers, who use their services to purchase and deliver advertising.

RTB uses adtech to enable the buying and selling of advertising inventory in real time – ie in the time it takes a webpage to load in a user's browser – on an impression by impression basis, typically involving an auction pricing mechanism. It is a type of online advertising – specifically, a sub-type of 'programmatic' advertising[4] – that is most commonly used at present for selling visual inventory online, either on the website of a publisher or via a publisher's app. However, the same techniques can be applied to other channels, eg audio, video streaming, and facial detection and/or recognition technology on digital billboards. RTB involves open auctions. Although the technologies involved can also be used in private auctions, where advertising is placed directly between advertisers and publishers (ie access to the inventory is limited to certain parties). We do not address private auctions or 'programmatic direct' in this report.

For simplicity, this report uses desktop/website terminology. However, we address mobile and all other channels and media that utilise RTB given that the same features and challenges apply to these areas as well.

[4] 'Programmatic' advertising is defined by the Interactive Advertising Bureau (IAB) as 'the process of executing media buys in an automated fashion through digital platforms such as exchanges, trading desks and demand-side platforms'. See IAB (2014) *Programmatic 101 for Direct Sellers*. The IAB also defines four 'types' of programmatic transactions: 'Automated Guaranteed', 'Unreserved Fixed Rate', 'Invitation-Only Auction' and 'Open Auction'; see IAB (2013), *Programmatic and Automation – The Publisher's Perspective*, available at https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf. The IAB clarifies that 'Open Auction' is also referred to as RTB, 'open exchange' and 'open marketplace'.

2.2 What are the risks to information rights?

RTB carries a number of risks that originate in the nature of the ecosystem and how personal data is processed within it. These include:

- profiling[5] and automated decision-making;
- large-scale processing (including of special categories of data);
- use of innovative technologies;
- combining and matching data from multiple sources;
- tracking of geolocation and/or behaviour; and
- invisible processing.

Beyond these, the large number of organisations that are part of the ecosystem – as controllers, joint controllers or processors – has a significant impact on data protection implications. Additionally, many individuals have a limited understanding of how the ecosystem processes their personal data[6].

These make the processing operations involved in RTB of a nature likely to result in a high risk to the rights and freedoms of individuals. Many of the above factors constitute criteria that make data protection impact assessments (DPIAs) mandatory, for example:

- Article 35(3) of the GDPR states that DPIAs are required in circumstances where there is a systematic and extensive evaluation of personal aspects relating to natural persons, including profiling, and on which decisions are based that produce legal or similarly significant effects[7]; and where there is large-scale processing of special categories of data[8]; and
- the ICO's list of processing operations likely to result in a high risk, published under Article 35(4)[9], includes criteria such as invisible processing, tracking, combination and matching of data, and the use of innovative technologies.

---

[5] Article 4(4) of the GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

[6] The ICO commissioned Harris Interactive to undertake research into online advertising. 63% of the 2,300 participants indicated they found it acceptable that ads funded free content; however, when they were given an explanation of how RTB works, this fell to 36%. The survey is available here: https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf.

[7] The Article 29 Working Party's *Guidelines on automated decision making and profiling* (WP251rev.01), published 6 February 2018 and endorsed by the European Data Protection Board (EDPB) on 25 May 2018, observe that online advertising 'increasingly relies on automated tools and involves solely automated individual decision making'. The guidelines then say that 'in many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile', but go on to note that 'it is possible that it may do, depending on the particular characteristics of the case, including: the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted'. It is therefore clear that, depending on the circumstances, online advertising (including RTB) which involves automated decision making and profiling can have a significant effect on individuals.

[8] See Articles 35(3)(a) and (b) of the GDPR.

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Whilst we provide more information about DPIAs in section 3.6 below, our industry engagement to date has left us with a clear impression that many organisations within the RTB ecosystem have not undertaken any such assessments.

2.3 Why is the ICO publishing this report?

Processing of personal data in RTB, and adtech more generally, involves web and, cross-device tracking, depending on the circumstances. This is one of the ICO's regulatory priorities. We first highlighted the risks posed in the ICO's Technology Strategy 2018-2021, including aspects relating to hidden personalisation, big data, the Internet of Things, and invisible processing. The strategy summarises this priority area as follows

Priority area 3: Web and cross-device tracking

The use of HTTP cookies has not diminished although a range of alternative methods of performing tracking online have emerged and become more common; for example device fingerprinting, browser fingerprinting and canvas fingerprinting. This is likely to continue as more devices connect to the internet (IoT, vehicles, etc) and as individuals use more devices for their online activities. These new online tracking capabilities are becoming more common and pose much greater risks in terms of systematic monitoring and tracking of individuals, including online behavioural advertising. The intrusive nature of the technologies in combination drives the case for this to be a priority area.

This report is delivered partly as an update on progress in delivering the goals of the Technology Strategy.

2.4 How does RTB work?

Organisations wishing to generate revenue from digital advertising are likely to incorporate adtech into their online services. Generally an organisation (the 'publisher') operating an online service will use cookies and similar technologies[10] when a user visits that service to collect information about the user's device, the user themselves and the visit made to the website. This information is used for the purposes of displaying online advertising. The use of cookies and similar technologies is regulated under PECR, whilst the information collected by the publisher will include information that constitutes personal data under the GDPR.

Where the publisher is using RTB, the following takes place:

- the information collected will be incorporated in a 'bid request'[11]. This is transmitted into the RTB ecosystem so that advertisers can bid for

[10] The phrase 'cookies and similar technologies' is used in the ICO's Guide to PECR, and in the context of Regulation 6, refers to any method used to store information, or access information stored, in user devices. This includes cookies as well as tracking pixels, fingerprinting techniques, and any other method. See https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/.
[11] See section 2.6 below for the information typically contained within bid requests.

the opportunity to insert their advert into the respective ad space on the publisher's service, which will be presented to the individual that is viewing that service. Bid requests normally contain information that constitutes personal data under the GDPR;

- the collection of the user's information, the creation of the bid request, the auctioning, bidding and securing of the advertising space and subsequent presentation of the advert to the individual all take place in milliseconds[12,13]. This allows the successful advertiser to present adverts to individuals based on the information gathered about them via the RTB process;
- the types of information gathered within RTB are governed by particular industry specifications known as protocols, usually, OpenRTB or Google's Authorized Buyers Real Time Bidding Protocol[14];
- more detailed bid requests are deemed to be more attractive, either because they bring in higher revenue and/or because they are intended to enable more accurate targeting of adverts to individuals; and
- parties within the RTB ecosystem may also 'augment' the data collected with information from other sources, a process known as 'data matching' or 'enrichment'[15].

This open auction process involves multiple organisations processing personal data of website users[16]. Millions of bid requests are processed every second[17] utilising automation, which involves the leveraging of multiple data sources into user profiles shared throughout the ecosystem.

2.5 Who are the participants?

RTB involves multiple stakeholders including:

- **Advertisers**: organisations that bid in real time to serve ad impressions to webpage visitors. The highest bidder 'wins', and their advertisement will be presented on the webpage to the user;
- **Publishers**: websites that sell spaces for online adverts;
- **Advertising exchanges**: Platforms for comparing the price and quality of impressions, the 'location' where the bidding aspect occurs. They serve as mediators and connectors between advertisers and publishers and operate on both the demand and supply sides;
- **Data Management Platforms (DMPs):** These platforms analyse, categorise and collate incoming data from multiple sources (including

[12] Google, *Authorized Buyers overview*: 'This all happens within 100 milliseconds, or in real time.' Available at: https://support.google.com/authorizedbuyers/answer/6138000
[13] Lukasz Olejnik & Claude Castelluccia (2014), *To bid or not to bid: Measuring the value of privacy in RTB*, p4. Available at: https://lukaszolejnik.com/rtb2.pdf.
[14] See section 2.7 below for more information about OpenRTB and Authorized Buyers.
[15] Enrichment can also take place based on the use of aggregated data.
[16] As an example, there are over 450 organisations within the IAB's Transparency and Consent Framework vendor list, and not all actors within RTB are in the TCF.
[17] Google, *Infrastructure Options for RTB bidders*, which states that "RTB bidders are dealing with billions of requests per day" (available at https://cloud.google.com/solutions/infrastructure-options-for-rtb-bidders).

desktop, mobile web, mobile app, analytics, social media, and offline data), including bid requests, to support the personalised targeting of adverts;

- **Demand Side Platforms (DSPs)**: DSPs buy inventory (space on websites) based on behavioural, and often personal data. If the impression matches the advertiser's target audience then a bid is placed via the DSP;
- **Supply Side Platforms (SSPs)**: SSPs help publishers manage and sell their advertising inventories; and
- **Consent Management Platforms (CMPs)**: CMPs are intended to serve as a tool for publishers, for example to enable them to manage user consent, and to facilitate the operation of frameworks such as the IAB Europe's Transparency and Consent Framework.

Organisations may operate across the ecosystem – ie they could have a DMP, a DSP, and an ad exchange. Whilst this report does not mean to make assessments about operating models, it is nevertheless the case that, from a data protection perspective, this further complicates the ecosystem. For example, this makes it difficult even for market participants to be clear which organisations operate in which area.

2.6 What information is included in a bid request?

The information in a bid request can vary[18] but most include the following:

- a unique identifier for the bid request;
- the user's IP address (possibly with the final set of numbers removed, eg in Google's Authorized Buyers framework);
- cookie IDs;
- user IDs;
- a user-agent string identifying the user's browser and device type;
- the user's location;
- the user's time zone;
- the detected language of the user's system;
- the device type (desktop/mobile, brand, model, operating system);
- other information relating to the user (this can vary); and
- information relating to the audience segmentation[19] of the user.

[18] For a full list of information in Authorized Buyers, see Google, *Authorized Buyers Real Time Bidding Proto*, available at https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide; Google also maintains a similar list for the OpenRTB protocol at https://developers.google.com/authorized-buyers/rtb/openrtb-guide.

[19] Audience segments are described by the IAB as "subsets of user data signifying specific facts, interests and other attributes". See IAB (2016), *Data Segments & Techniques Lexicon*, page 4. Available at: https://www.iab.com/wp-content/uploads/2016/01/IAB-Data-Lexicon-Update-2016.pdf.

The above information is personal data where it enables a natural person to be identified, directly or indirectly, from the information itself (alone or in combination) as well as additional information that controllers may possess[20].

Other information about the user can include:

- referring sites (where the user came from);
- user journey on the site (including mouse cursor movement);
- events (scrolling, clicking, highlights, media views);
- location;
- search queries;
- session time;
- site behaviour (contextual and thematic preferences to certain topics and pages, interactions such as downloads, transitions to other pages through clicking on advertisements and links); and
- demographic data.

Some of the fields in the protocol specifications also indicate the processing of special category data either directly or where these are subsequently used to make inferences about the user.

Examples

The IAB's 'content taxonomy' (v2.0, November 2017) contains hundreds of fields, which include 'Heart and Cardiovascular Diseases', 'Mental Health', 'Sexual Health' and 'Infectious Diseases'[21] whilst Google's 'publisher verticals' include 'Reproductive Health', 'Substance Abuse', 'Health Conditions', 'Politics' and 'Ethnic & Identity Groups'[22].

We have heard assertions that, in some cases, such fields are not used for profiling individuals, but instead for alerting advertisers to the nature of the website being visited by the user, thereby enabling advertisers to prevent their adverts being placed on unsuitable websites. However, for both protocols, some of the published documentation states that these fields are used for both targeting and exclusion[23]. Also, regardless of how the

[20] The GDPR also includes 'online identifiers' within the definition of personal data. For more information, see Article 4(1) and Recital 30 of the GDPR as well as our guidance on determining what is personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. For guidance on identifiers and related factors, see also: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/.

[21] See IAB (2017), *Content Taxonomy v2.0*, available at: https://www.iab.com/wp-content/uploads/2017/11/IAB_Tech_Lab_Content_Taxonomy_V2_Final_2017-11.xlsx

[22] See Google's list of publisher verticals, available at: https://storage.googleapis.com/adx-rtb-dictionaries/publisher-verticals.txt

[23] See, for example: IAB TechLab (2016), *Taxonomy: The Most Important Industry Initiative You've Probably Never Heard Of*, published 21 July 2016, which states 'The long term objective of the project is to not only describe site content, but also look towards ad product and audience descriptors'; IAB TechLab (2017), *IAB Tech Lab announces final Content Taxonomy 2.0 ready for adoption*, published 30 November 2017 (available at https://iabtechlab.com/blog/iab-tech-lab-announces-final-content-taxonomy-v2-ready-for-adoption/) which states 'use cases spanned from contextual targeting, to inventory procurement, brand safety measurement, and audience segmentation' and that the revisions to version 2.0 of the taxonomy were 'to better serve the use cases of audience analysis and segmentation, by normalizing data formats and naming conventions'. The

advertisers intend to use this data, their collection alongside the identifiers and other personal data in a bid request indicates the processing of special categories of data either directly or by inference.

Finally, data within the ecosystem is not solely based on that processed at the 'front-end' when a user visits a webpage. Data matching and combination from other sources (eg data management platforms) can also be incorporated into the information collected via the bid requests during further processing within the ecosystem.

2.7 How is the processing undertaken?

RTB is facilitated by protocols governing how data is collected and shared, and how adverts are served. For the purposes of this report, the two main protocols considered are:

- the IAB's 'OpenRTB' protocol[24] and associated 'Adcom 1.0'[25] and IAB Europe's 'Transparency and Consent Framework'[26] (TCF); and
- Google's 'Authorized Buyers' framework[27], which includes the Authorized Buyers Real Time Bidding protocol.

These are technical specifications that delineate exactly what data is shared between parties in a transaction and how the data sharing takes place. They constitute attempts to standardise protocols across different market participants. Other protocols are also available, some of which are compatible with, link into or provide different functionality to those like OpenRTB; however this report does not focus on these.

This report considers OpenRTB and Authorized Buyers together, although we have heard representations that there are differing levels of governance and control associated with the two systems. Given the nature of our work to date, we have not yet tested these representations.

---

same article also announced the intent to develop an additional 'audience taxonomy' in the future. Google's publisher verticals (see above) are stated to 'specif[y] the verticals (similar to keywords) of the page on which the ad will be shown', and that 'Google generates this field by crawling the page and determining which verticals are used'. See https://developers.google.com/authorized-buyers/rtb/data.

[24] See IAB Tech Lab, *OpenRTB 3.0 Final*, available at https://github.com/InteractiveAdvertisingBureau/openrtb.

[25] See IAB Tech Lab, *AdCOM 1.0*, available at https://github.com/InteractiveAdvertisingBureau/AdCOM.

[26] See IAB Europe, *Transparency and Consent Framework*, available at https://advertisingconsent.eu/.

[27] Formerly known as DoubleClick Ad Exchange; see Google, *Introducing Authorized Buyers*, available at https://support.google.com/authorizedbuyers/answer/9070822, and the developer pages beginning with https://developers.google.com/authorized-buyers/rtb/start.

3 What are the key issues?

We have prioritised the following key issues identified on the nature of RTB and how it creates risks to individuals. They do not represent the full nature of our concerns with RTB or adtech more generally.

Additionally, a number of themes are interlinked such as consent, transparency, lawful basis, and profiling.

3.1 Lawful basis and PECR

Many RTB participants define themselves as data controllers. However, we identified a lack of clarity from a significant number of controllers regarding the appropriate lawful basis for processing, as well as the particular requirements of each basis. For some market participants, these were at best not fully understood or at worst ignored.

The next section of this report explores this issue in the context firstly of special category data and then non-special category data. However, it is important to note that we also found a common lack of understanding about the role of PECR and how this impacts lawful basis. For example, some participants rely on legitimate interests both for processing of personal data **and** the use of cookies.

However, the rules on the use of cookies and similar technologies are specified in Regulation 6 of PECR; they take precedence over the GDPR in respect of cookies due to PECR, particularising data protection law in this area. PECR requires organisations to provide clear and comprehensive information about the purposes of any cookie or similar technology that stores information (or accesses information stored) on user devices, and obtain prior consent (which must be to the GDPR standard). The exemptions from this requirement do not apply in the context of RTB specifically or online advertising more generally[28]. In essence, for the purposes of compliance with Regulation 6 of PECR, it is irrelevant whether the information being stored or accessed is personal data; Similarly, if it is personal data, it is also irrelevant whether it is special category data or not.

Market participants' lack of clarity has implications for PECR compliance because the processing of information, including personal data, in the

[28] In practice, the only applicable exemption is at Regulation 6(4)(b) of PECR, where the storage of information, or access to information stored, is 'strictly necessary for the provision of an information society service requested by the subscriber or user.' However, cookies used for advertising purposes are not 'strictly necessary'. Guidance issued by the Article 29 Working Party in *Opinion 04/2012 on cookie consent exemption* clarifies that when applying this exemption 'it is important to examine what is strictly necessary from the point of view of the user, not the service provider'. It then states that 'third party advertising cookies cannot be exempted from consent' and further clarifies that 'consent would also be needed for operational purposes related to third party advertising such as frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging.' The Working Party's later *Opinion 09/2014 on device fingerprinting* also states that 'device fingerprinting for the purpose of targeted advertising requires the consent of the user'. As these Opinions apply to the ePrivacy Directive, the EU law on which PECR is based, they remain applicable post-GDPR.

ecosystem is initially effected by the use of cookies and similar technologies on publisher websites.

We have also found that most industry initiatives are focused either solely or primarily on GDPR compliance rather than PECR.

3.2 Special category data

A proportion of bid requests involve the processing (either directly or by inference) of special category data, either at the point of collection or subsequently. Special category data is more sensitive than 'ordinary' or non-special category personal data, and needs more protection, as our guidance makes clear[29]. It also constitutes the area of greatest potential harm to individuals.

The schema used within both OpenRTB and the TCF, and Authorized Buyers, include fields relating to politics, religion, ethnic groups, mental health and physical health, among others. The bid requests include these fields as well as other information about the user such as device IDs, cookie IDs, location data etc. The available documentation for these schema indicate that these 'taxonomies' are used for different purposes, including functioning essentially as keywords to describe the content of an online service (eg to mitigate the risk of serving ads to the 'wrong' site), but also for audience targeting and exclusion – ie placing users into various 'audience segments' for targeted advertising[30].

However, data protection law is clear that processing of this data (regardless of which of these two purposes it is for) is prohibited, unless a condition within Article 9 of the GDPR[31] applies. The only applicable condition is explicit consent. No other condition can be relied upon and none of the public interest conditions within the DPA 2018 can apply to RTB specifically or online advertising more generally. Organisations can still consider legitimate interests as an Article 6 lawful basis for processing special category data, but they also need an Article 9 condition.

This means that the current consent requests provided under both the TCF and AB frameworks are non-compliant. Consent mechanisms must be appropriate for the processing of special category data. Market participants must therefore modify existing consent mechanisms to collect explicit consent, or they should not process this data at all.

[29] For example, 'Special category data is personal data which the GDPR says is more sensitive, and so needs more protection' and 'this type of data could create more significant risks to a person's fundamental rights and freedoms' See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.
[30] https://iabtechlab.com/taxonomy-the-most-important-industry-initiative-youve-probably-never-heard-of/
[31] The Schedule 1 conditions in the DPA 2018 enable reliance on exceptions within Article 9, specifically 9(2)(b), (g), (h), (i) and (j) for Part 1 of Schedule 1 and 9(2)(g) (public interest) for part 2 of Schedule 1. None of these include 9(2)(a) (explicit consent), nor do the cited Article 9 provisions apply in the context of online advertising.

3.3 Non-special category data

Our understanding is that at the point of collection of personal data from the user (eg when the user visits a website and cookies and similar technologies are used), the TCF currently suggests both consent and legitimate interests as a lawful basis for processing[32]. Our discussions with IAB and IAB Europe in August 2018 indicated that a number of TCF participants were indeed relying on legitimate interests to set cookies. (Google Authorized Buyers mandates consent as the only lawful basis for processing.[33])

Bid requests that comprise non-special category data do not require explicit consent under Article 9. However, due to the use of cookies to process this information, consent (to the GDPR standard) is still required under PECR at the initial point of processing. (Previous guidance from the Article 29 Working Party indicates that the consent can apply to subsequent processing of the data within the ecosystem, as long as it remains valid.)

Our guidance also states that if organisations are required to obtain consent for marketing in accordance with PECR, then in practice consent is the appropriate lawful basis under the GDPR[34]. Furthermore, trying to apply legitimate interests when an organisation has GDPR-compliant consent would be an entirely unnecessary exercise and would cause confusion for individuals[35]. For example, organisations would need to ensure that they had both valid consent and had also fulfilled all of the legitimate interest requirements. There may also be an element of unfairness as well. For example in cases where individuals understand their personal data is processed on the basis of consent, yet once they withdraw that consent, the organisation then continues to process via legitimate interests.

In any case, reliance on legitimate interests as a lawful basis for processing means that organisations take on extra responsibility for ensuring that the interests, rights and freedoms of individuals are fully considered and protected. As our guidance on legitimate interests makes clear, there are three elements involved. Organisations need to:

- identify a legitimate interest – the 'purpose test';
- show that the processing is necessary to achieve it – the 'necessity test'; and

---

[32] IAB Europe, *Transparency and Consent String with Global Vendor List Format* (draft v2.0), published 25 April 2019, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2%20(draft%20for%20public%20comment).md#translations.

[33] Google, *Authorized Buyers Program Guidelines*, published 22 August 2018, available at: https://www.google.com/doubleclick/adxbuyer/guidelines.html.

[34] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

[35] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. Organisations may also find it useful to consult our lawful basis tool, available at https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/, and our legitimate interests assessment template, available at https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx.

- balance it against the individual's interests, rights and freedoms – the 'balancing test'.

Reliance on legitimate interests for marketing activities is possible only if organisations don't need consent under PECR and are also able to show that their use of personal data is proportionate, has a minimal privacy impact, and individuals would not be surprised or likely to object.

We believe that the nature of the processing within RTB makes it impossible to meet the legitimate interests lawful basis requirements. This means that legitimate interests cannot be used for the main bid request processing. This is the case even if it were possible for legitimate interests to be applicable elsewhere in the RTB ecosystem – for example if a DMP is asked to supplement a bid request with additional information. There seems to be a perception by some participants that consent is 'challenging' and legitimate interests is the 'easy option'. Overall, we do not believe there is a full understanding of what legitimate interests requires.

In our view, 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). Firstly, this is because PECR requires consent at the initial point for the use of any non-essential cookies. Cookies used for the purposes of online advertising (not just RTB, but all types of online advertising) require prior consent to the GDPR standard and cannot rely on an exemption in Regulation 6, as stated above. Secondly, whilst associated processing of personal data may be able to rely on an alternative lawful basis[36], consent is also the most appropriate lawful basis for processing of personal data beyond the setting of cookies. This due to the nature of the processing in RTB, particularly when viewed alongside previous guidance from data protection authorities about processing in the context of online advertising[37,38].

[36] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/.

[37] Examples include the recent EDPB *Opinion 05/2019 on the interplay between the GDPR and the ePrivacy Directive*, and the Article 29 Working Party's previous *Opinion 06/2014 on the notion of legitimate interests*, *Opinion 03/2013 on purpose limitation* and *Opinion 02/2010 on online behavioural advertising.*

[38] For example, the Article 29 Working Party's *Opinion 06/2014 on the notion of legitimate interests* states (*inter alia*) that 'whilst controllers may have a legitimate interest in getting to know their customer's preferences to as to enable them to personalise their offers and, ultimately, offer products and services that better meet the needs and desire of the customers' this does not mean they could rely on legitimate interests 'to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes and create – and for example, with the intermediary of data brokers, also trade in – complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject' (pp24-25). The Working Party's *Opinion 03/2013 on purpose limitation* also states that, when an organisation 'specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform "measures or decisions" that are taken with regard to those customers' that 'free, specific, informed and unambiguous "opt-in" consent would almost always be required, otherwise further use [of the personal data] cannot be considered compatible. Importantly, such 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.' (p46)

Our work has established that, at present, some parts of the adtech industry are unaware of this advice.

3.4 Lack of transparency

Whilst transparency and consent are closely linked in the context of RTB, in data protection terms they are separate concepts. For example, an organisation may meet the consent requirements (freely given, specific, informed, and unambiguous etc) but this does not necessarily mean it is compliant with the information requirements in Articles 13 and/or 14 of the GDPR. However, in RTB the privacy information provided often lacks clarity and does not give individuals an appropriate picture of what happens to their data. Whilst we recognise that provision of this information in the online environment can be challenging, this does not mean that participants can ignore the requirements of PECR ('clear and comprehensive information') and the GDPR.

Given the complexity and opacity of the RTB ecosystem, organisations cannot always provide the information required, particularly as they sometimes do not know with whom the data will be shared. For example, the vendor list that forms part of IAB Europe's TCF has over 450 organisations, each with separate privacy policies to the online service the user is actually visiting[39]. It is therefore unclear whether this vendor list is of practical use to individuals when they are presented with the TCF 'mechanism'. Furthermore, the list does not include all RTB actors. Those services that implement the TCF are still able to use third parties that are not on the list as there is no industry, sectoral or legal requirement or control preventing this. For example, some implementations of front-end consent mechanisms on the part of web publishers include organisations who are not part of any established vendor list. This means that the mechanisms do not provide any controls to individuals about the use of cookies or similar technologies by those organisations. In these cases, individuals may have to take additional actions, for example, visiting other opt-out services, or the websites of those other organisations themselves.

Additionally, the information requirements under Articles 13 and 14 require privacy notices to specify 'recipients or categories of recipients'. However, in cases where the processing of personal data by third parties is intended to rely on a consent obtained by a first party, those third parties would need to be named as recipients of the data, and the nature of RTB means that the first party has no means of determining which third parties the data will be shared with. This leads to extensive lists of organisations who the data 'might' be shared with, depending on the specifics of the auction process.

Transparency issues also exist for the ecosystem itself, given the opaque nature of the data supply chain. Whilst there is extensive documentation on both the underlying protocols and the TCF and Authorized Buyers, much of this is very long, detailed and technical in nature. It is unclear whether organisations that participate in the RTB frameworks fully understand how

[39] See IAB Europe's vendor list at https://advertisingconsent.eu/vendor-list/.

they function in general or how the processing of personal data works. Whilst industry initiatives (such as in the TCF) attempt to address this by creating a technical means by which participants don't necessarily have to know all of this content, in its current form this does not comply with the accountability principle of the GDPR[40]. Organisations must understand, document and be able to demonstrate:

- how their processing operations work;
- what they do;
- who they share any data with; and
- how they can enable individuals to exercise their rights.

Finally, RTB also involves the creation and sharing of user profiles within an ecosystem comprising thousands of organisations. These profiles can also be 'enriched' by information gathered by other sources, eg concerning individuals' use of multiple devices and online services, as well as other 'data matching' services. The creation of these very detailed profiles, which are repeatedly augmented with information about actions that individuals take on the web, is disproportionate, intrusive and unfair in the context of the processing of personal data for the purposes of delivering targeted advertising. In particular when in many cases individuals are unaware that the processing takes place and the privacy information provided does not clearly inform them what is happening[41].

3.5 The data supply chain

A single RTB request can result in personal data being processed by hundreds of organisations. The implications and risks for transparency and fair processing are summarised above. In this section, we summarise security and data sharing issues caused by this data supply chain.

As described in the previous section, the IAB Europe global vendor list comprises over 450 organisations, each with their own privacy policy. Some of these will be in non-EU jurisdictions, meaning that international transfers of personal data are taking place. As bid requests are often not sent to single entities or defined groups of entities, the potential is for these requests to be processed by any organisation using the available protocols, whether or not they are on any vendor list and whether or not they are processing personal data in accordance with the requirements of data protection law.

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,

[40] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

[41] See the previous reference to earlier Article 29 Working Party opinions on legitimate interests and purpose limitation.

essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls.

Industry has looked to use contractual controls to provide a level of guarantees about data protection-compliant processing of personal data. In fact some parties have asserted that they go 'beyond' contractual controls, a claim that has yet to be validated. However, this contract-only approach does not satisfy the requirements of data protection legislation. Organisations cannot rely on standard terms and conditions by themselves, without undertaking appropriate monitoring and ensuring technical and organisational controls back up those terms. For example, ICO guidance on controller/processor[42] and contracts and liabilities[43] states that controllers must:

- assess the processor is competent to process personal data in line with the GDPR;
- put in place a contract or other legal act meeting the requirements in Article 28(3); and
- ensure a processor's compliance on an ongoing basis, in order for the controller to comply with the accountability principle and demonstrate due diligence (such as audits and inspections).

Whilst the methods used to monitor compliance will depend on the circumstances of the processing, it is clear that the GDPR has increased requirements for controller/processor arrangements compared to previous legislation. Beyond this, the general principle of accountability also means that organisations need to be able to demonstrate how they comply with the requirements of the GDPR. For example, they should document what they are doing or have done with the data received, and ensure processes are in place to either protect that data or delete it.

3.6 Data protection impact assessments (DPIAs)

DPIAs are tools that organisations can use to identify and minimise the data protection risks of any processing operation. Article 35 of the GDPR specifies several circumstances that require DPIAs, including where there is large-scale processing of special category data. Guidance produced by European data protection authorities provides a list of criteria that organisations can use to determine whether their processing is likely to result in a high risk to the rights and freedoms of individuals, and therefore whether a DPIA is required[44]. Furthermore, under Article 35(4) of the GDPR, the ICO has published a list of processing operations likely to result in such a high risk,

[42] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/
[43] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/
[44] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment*, published 13 October 2017 and endorsed by the European Data Protection Board on 25 May 2018. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

for which DPIAs are mandatory[45]. RTB matches a number of examples on this list, such as where the processing involves:

- the use of new technologies, combined with any criterion from the EDPB guidelines on DPIAs;
- any profiling of individuals on a large scale;
- personal data that has not been obtained from individuals, where organisations consider compliance with Article 14 would involve disproportionate effort – this is known as 'invisible processing'[46];
- tracking an individual's geolocation or behaviour, combined with any criterion from the EDPB guidelines; and/or
- the use of personal data of children or other vulnerable individuals for marketing purposes, profiling or automated decision making.

Very few people outside the industry have a clear understanding that RTB exists, how it works or that their personal data is processed within the ecosystem. A survey undertaken by Harris Interactive, carried out prior to the Fact Finding Forum, supports this observation. Given this, and the other aspects of processing within RTB, organisations are therefore legally required to perform DPIAs. We have seen no evidence to date that the DPIA requirements are fully recognised by all participants in RTB (for processing involving special category data or otherwise)[47].

3.7 Industry initiatives to address issues

During our work we have been briefed on various ongoing initiatives to change the way the RTB ecosystem operates. In due course, these may address some or all of the issues that concern us. Examples include further revisions to IAB Europe's TCF; the proposal from Dr Johnny Ryan (of Brave software) to reduce or truncate the number of data fields utilised by the protocols[48]; and the development of new technology to run parts of the RTB 'process' on a data subject's own device (thereby limiting the amount of personal data that needs to be shared elsewhere). However, we have not seen compelling evidence that any of these initiatives are fully mature, would sufficiently address our concerns in their current state, or that the current market would adopt such measures voluntarily.

---

[45] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

[46] 'Invisible processing' is an activity that carries inherent risk to rights and freedoms as it takes place with no or minimal user awareness. The ICO's Article 35(4) list provides the following definition: 'Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14(5)(b).' Our list clarifies that processing operations of this sort, combined with any of the criteria from the EDPB guidelines, require a DPIA. Similar examples appear on a number of the Article 35(4) lists prepared by other European data protection authorities.

[47] The requirement to undertake a DPIA does not equate to a requirement to undertake prior consultation with the ICO. The circumstances where prior consultation is required are detailed in Article 36 of the GDPR. For more information, see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/.

[48] Brave.com, *Update on GDPR complaint (RTB ad auctions)*, published 20 February 2018, available at https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/.

4 Summary and conclusions

Overall, in the ICO's view the adtech industry appears immature in its understanding of data protection requirements. Whilst the automated delivery of ad impressions is here to stay, we have general, systemic concerns around the level of compliance of RTB:

1. Processing of non-special category data is taking place unlawfully at the point of collection due to the perception that legitimate interests can be used for placing and/or reading a cookie or other technology (rather than obtaining the consent PECR requires).

2. Any processing of special category data is taking place unlawfully as explicit consent is not being collected (and no other condition applies). In general, processing such data requires more protection as it brings an increased potential for harm to individuals.

3. Even if an argument could be made for reliance on legitimate interests, participants within the ecosystem are unable to demonstrate that they have properly carried out the legitimate interests tests and implemented appropriate safeguards.

4. There appears to be a lack of understanding of, and potentially compliance with, the DPIA requirements of data protection law more broadly (and specifically as regards the ICO's Article 35(4) list). We therefore have little confidence that the risks associated with RTB have been fully assessed and mitigated.

5. Privacy information provided to individuals lacks clarity whilst also being overly complex. The TCF and Authorized Buyers frameworks are insufficient to ensure transparency and fair processing of the personal data in question and therefore also insufficient to provide for free and informed consent, with attendant implications for PECR compliance.

6. The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge.

7. 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, and with little or no consideration as to the requirements of data protection law about international transfers of personal data.

8. There are similar inconsistencies about the application of data minimisation and retention controls.

9. Individuals have no guarantees about the security of their personal data within the ecosystem.

5. Next steps

Our two prioritised areas of concern – the processing of special category data without explicit consent and the complexity of the data supply chain – require further analysis and exploration.

We intend to enhance our understanding by:

5.1 Targeted information-gathering activities

Based on the need to further explore the data protection implications of RTB, we will undertake targeted information-gathering activities related to the data supply chain and profiling aspects, the controls in place, and the DPIAs undertaken. We will start this work in July 2019.

5.2 Engagement activities with key stakeholders

We will also continue targeted engagement with key stakeholders. This autumn, we envisage holding an event, similar to the Fact-Finding Forum to continue dialogue and update stakeholders on developments. We will also continue bilateral engagement with IAB Europe and Google.

5.3 Cooperation with other Data Protection Authorities

To date, complaints have been raised in at least seven European jurisdictions. We will continue to liaise and share information with our European colleagues.

5.4 Industry sweep

Following continued engagement to obtain more information, we may undertake a further industry review in six months' time. The scope and nature of such an exercise will depend on our findings over the forthcoming months.

In the meantime, we expect data controllers in the adtech industry to re-evaluate their approach to privacy notices, use of personal data, and the lawful bases they apply within the RTB ecosystem.

Following these initial activities, we will continue to focus on both RTB and adtech in general, and may issue a further update report in 2020.

6. FAQs

What is the status of this update report?

This report summarises our findings into RTB to date. We've published it to provide a progress update on one of our regulatory priorities. It isn't guidance, and it isn't a formal outcome representing a legally-binding decision. The report represents our views and findings at this point in time, and may contribute to future guidance - if this happens we'll amend the report itself to say so.

Will the ICO write guidance about adtech?

Our existing guidance provides comprehensive information for organisations about how to comply with the law. These apply to adtech and RTB just as much as they do to other types of processing, particularly data protection by design and DPIAs. Organisations should look at this guidance first, but in the future we may write further guidance in this area or contribute to work at European level.

Why are you just focusing on RTB?

We're focusing on RTB due to the complexity of this type of online advertising, the general nature of the risks posed and the level of data protection compliance that we've found. We're clear that RTB isn't the only aspect of adtech that we're looking into – programmatic advertising has other forms, like private auctions, and online advertising as a whole is a larger concept. However, we think that due to how RTB works, if we address this first, there is potential to transform practices more widely.

RTB can generate significant revenue for organisations. Is the ICO saying they can't use it anymore?

RTB is an innovative means of ad delivery, but one that lacks data protection maturity in its current implementation. Whilst it is more the practices than the underlying technology that concern us, it's also the case that, if an online service is looking to generate revenue from digital advertising, there are a number of different ways available to do this. RTB is just one of these. Whatever form organisations choose, if it involves either accessing or storing information on user devices, and/or the processing of personal data, there are laws that they have to comply with.

How do individuals find out if their personal data has been processed in the RTB ecosystem?

Data protection law places obligations on organisations to, among other things, process personal data fairly, lawfully and transparently. It also gives individuals a number of rights over that data, including the right to access that data for free. We've provided more information about this in our Your Data Matters campaign on our website.