Technology and Regulation

Impossible Asks:

Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?

Michael Veale*, Midas Nouwens** and Cristiana Teixeira Santos***

adtech, real-time bidding, rtb, online advertising, online tracking, transparency and consent framework, GDPR

m.veale@ucl.ac.uk

midasnouwens@cc.au.dk

c.teixeirasantos@uu.nl

On 2 February 2022, the Belgian Data Protection Authority (DPA) issued a decision concerning IAB Europe and its Transparency and Consent Framework (TCF), a system designed to facilitate compliance of real-time bidding (RTB), a widespread online advertising approach, with the GDPR. In this article, we summarise the context of this decision and analyse the decision itself. We argue that by characterising IAB Europe as a joint controller with RTB actors, the Belgian decision gives DPAs an agreed-upon blueprint to deal with a structurally difficult enforcement challenge. Furthermore, under the DPA's simple-looking remedial orders are deep technical and organisational tensions. We analyse these "impossible asks", concluding that absent a fundamental change to RTB, IAB Europe will be unable to adapt the TCF to bring RTB into compliance with the decision.

1. Introduction

Real-time bidding (RTB) is a system where predetermined advertising space, such as a banner advert on a website or a splash screen in an app, is allocated in "real-time" (while the website or app is loading) through an auction process for each ad space, typically by profiling the user to whom the advert will be shown. The precise mechanics of this practice are quite complex, have been detailed elsewhere, and for this paper some knowledge will be assumed about the main practises and actors for reasons of space.[1] In effect, RTB involves a range of actors interacting around a bid request, structured data about a site or app and its visitor which informs auction participants, who in turn analyse and profile the request to inform their bidding choices, with the auction winner able to choose the ad shown on the page. Actors include the **advertisers** that pay for advertising space; the **publishers** who offer advertising slots on their websites or apps; **consent management platforms** (CMPs), which show sophisticated "cookie banners'' that publishers employ to interact with both users and technologies embedded on their websites and apps; and the **adtech vendors** who intermediate between publishers and advertisers, and offer services ranging from auction exchanges, profiling and data brokering, tracking technologies, ad fraud detection, or the technical delivery and display of adverts. Within this system, an important actor is the **Interactive Advertising Bureau** (IAB), a membership organisation that coordinates various efforts concerning RTB, with many related organisations in different jurisdictions, including IAB Europe in Belgium.

1.1 RTB's Enforcement Challenge

Proponents claim that RTB benefits marketers, businesses and websites, but as RTB has emerged and matured over the last 10–15 years, its functional effects and use of personal data has led to an accumulation of concerns around the privacy and data protection properties of the ecosystem that operates it.[2]

Regulators have struggled to get a handle on the data protection challenges of RTB. A first hurdle is the complexity of the technical data processing infrastructure, understanding of which is a valuable commodity that adtech intermediaries — the many actors, sometimes called "vendors", between advertisers and publishers — themselves sell.[3] This complexity is compounded by a difficulty in identifying which of the many actors in a system of RTB are responsible for what. We summarise the general stances of industry actors below.

- **Adtech vendors** hold that they are processing data legally, as they place their trust in assurances from other actors they believe are capable of creating a valid legal basis for their activities and send-

1 Readers new to RTB may find it useful to either read the first part of the ruling itself, or a more detailed description aimed at lawyers can be found in Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23 *German Law Journal*.

* Michael Veale is Associate Professor at the Faculty of Laws at University College London, London, United Kingdom.
** Midas Nouwens is Assistant Professor, Department of Digital Design and Information Studies, Aarhus University, Denmark.
*** Cristiana Teixeira Santos is Assistant Professor, School of Law, Utrecht University, Utrecht, the Netherlands.

Received 7 Feb 2022, Accepted 8 Feb 2022, Published: 9 Feb 2022.

2 See eg an early study by Lukasz Olejnik and others, 'Selling off Privacy at Auction' in Proceedings of the 2014 Network and Distributed System Security Symposium (Internet Society 2014); Róisín Áine Costello, 'The Impacts of AdTech on Privacy Rights and the Rule of Law' (2020) 2 *Technology and Regulation* 11.

3 On intermediation in RTB, see Competition and Markets Authority, 'Appendix M: Intermediation in Open Display Advertising' (1 July 2020) https://assets.publishing.service.gov.uk/media/5fe49531d3bf7f089e48dec9/Appendix_E_Ecosystems_v.2_WEB.pdf.

ing them reliable records to prove this.

- **Consent management platforms** hold they are just a configurable tool for publishers to deploy, and that illegality should lay on the door of publishers for misconfiguration.
- **Publishers** hold they are at the behest of an industry in which they are rule-takers more than rule-makers. Legal limits have been set on their responsibility for illegality downstream by adtech actors by the CJEU.[4]
- **Advertisers** hold that they simply purchase a service with little direct role, contracting with adtech vendors, although at times they may also be publishers (eg relating to tracking or ad attribution infrastructure on their own websites).

Amidst all this, the Interactive Advertising Bureau claims, through various legal entities using the IAB brand in several jurisdictions, to simply provide some best practice tools, and denies legal responsibility for data processing operations relating to aspects of real-time bidding.

The consequence of these stances is that each actor in RTB attempts to locate significant responsibility elsewhere. The structural allocation of responsibility appears deliberately nebulous, and has long left DPAs struggling. Data protection is arguably not well set-up for such ecosystems, with its current imaginaries of data controllership, "[enabling] the design of complex cobwebs of control the principal purpose of which is to complicate enforcement".[5] There is a huge number of actors in the RTB ecosystem; 790 legal entities in IAB Europe's "Global Vendor List" alone.[6] DPAs are capable of launching a joint operation across borders,[7] or requiring mutual assistance on national investigations,[8] but the scale seems daunting. Furthermore, data protection authorities can struggle to know who to enforce against first. As both the Decision discussed below and recent CJEU rulings indicate,[9] adtech entities tend to misclassify themselves within the regime, for example either as data processors or not processing data at all, further relieving themselves of responsibility. DPAs therefore have to engage in both a disagreement with entities about their factual status within data protection before coming to substantive conclusions about enforcement. In a cross-border process, enforcement entails a tricky two–step alignment between regulators, which only amplifies the procedural difficulties of co-operation. All of these factors impede co-ordination and risk inconsistency, and risk enforcement chaos and confusion — meaning that that industry has long gone systematically unassessed.

1.2 The Transparency and Consent Framework (TCF)

With the heightened penalties of the General Data Protection Regulation (GDPR) since May 2018, actors in this ecosystem sought to establish that their activities were aligned with the regulation.[10] The Interactive Advertising Bureau Europe (IAB Europe), "a federation representing the digital advertisement and marketing industry on the European level",[11] supported regulatory alignment on behalf of its members through the development of the Transparency & Consent Framework (TCF). The TCF aimed to provide the necessary legal basis for the data processing as part of RTB to continue.

In essence, the TCF is a set of policies, technical specifications, and terms and conditions that instruct participating organisations how to act, including how to generate, transmit, and treat the metadata that describes the lawful bases for data processing happening in the context of RTB, specifically OpenRTB. OpenRTB is one of the most widely used protocols for RTB, providing the technical standards for messages between ad space providers, publishers, and competing buyers of ad space. Google provide a proprietary alternative, "Authorized Buyers", which is not the subject of this paper, although it does interact and partially interoperate with both OpenRTB and the TCF.[12] IAB Europe developed the TCF with the express purpose to bring the processing of personal data already happening in OpenRTB into conformity with the GDPR and ePrivacy Directive[13], indirectly promoting it as an attractive solution. Incidentally, OpenRTB is developed by the (legally distinct) IAB Tech Lab, located in New York.

TCF is not a "permissionless" technical document, a standard published by a national standardisation body typically would be. Anyone can make and host a website using standards such as HTTP, HTML and TCP/IP, without asking for permission from the bodies involved in making them, similarly to engineering standards throughout history.[14] In contrast, membership of the TCF requires an annual fee of 1,200 EUR to be paid to IAB Europe, and members must adhere to a range of specific and restrictive policies IAB Europe determine — for example, which adtech vendors they should include on their website or app, or how systems they use to obtain consent should store the consent signals in a cookie. Unlike typical engineering standards, parts of the TCF itself requires users to refer to a list of authorised users of the framework, called the Global Vendor List, published in a regularly updated JSON file by IAB Europe. As a whole framework, the TCF thus partly resembles an Internet standard (with technical specifications), partly a club (the system is technically designed not to work with non-members), and partly a contractual arrangement (through mandatory terms and conditions and policies created by IAB Europe). It is worth noting that many TCF participants are also members of IAB Europe.

1.3 Genesis of the Decision

Complaints around real-time bidding were publicly filed to data protection regulators in the UK and Ireland in September 2018,[15] and

4 René Mahieu and Joris Van Hoboken, 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (*European Law Blog*, 30 September 2019) https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection accessed 12 January 2021.

5 Michèle Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 *International Data Privacy Law* 333, 334.

6 At the time of writing in February 2022, see https://iabeurope.eu/vendor-list-tcf-v2-0/.

7 GDPR, art 62.

8 GDPR, art 61.

9 In particular Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* ECLI:EU:C:2018:388 (on Facebook fan-pages) and Case C-49/17 *Fashion ID* ECLI:EU:C:2019:629 (on Facebook website plugins).

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1 (hereafter "GDPR").

11 Decision, para. 36.

12 On proprietary and open RTB standards, see Costello (n 2) 13–14.

13 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 ("e-Privacy Directive").

14 See generally JoAnne Yates and Craig Murphy, *Engineering Rules: Global Standard Setting since 1880* (Johns Hopkins University Press 2019). This "permissionlessness" is distinct from the possibility of auditing driven by law or markets.

15 Douglas Busvine, 'Mozilla Co-Founder's Brave Files Adtech Complaint against Google', (*Reuters,* 12 September 2018); *James Killock and Michael*

in 12 other EU countries by the end of 2019.[16] Out of various actors mentioned in these complaints, IAB Europe is headquartered in Brussels, and therefore Belgium was considered the leading supervisory authority for those components. In February 2022, the Belgian Data Protection Authority (Belgian DPA) published a decision in relation to the role of IAB Europe within real-time bidding.[17] It concerns the conformity of the Transparency & Consent Framework with the GDPR and the responsibilities of various actors, specifically IAB Europe, over the processing of personal data happening based on the assumed legality of that framework. This complaint was based on a merger of nine complaints — four in Belgium, five made to other EU DPAs and passed through the one-stop-shop.[18] As a consequence, other EU DPAs examined and approved the contents of the decision by at least a two–thirds majority.[19]

1.4 Seeing The Whole Picture

Before moving to summarise this decision, it is worth providing some indication of why focusing on the detailed reasoning in this one regulatory decision may be important. Other decisions on RTB actors have previously been handed down by DPAs.[20] This one is markedly different. Previous decisions typically focused on organisations holding personal data, and occupying a distinct point within a much bigger system. It is not in dispute that the IAB Europe holds little relevant personal data in the RTB ecosystem. However, the system that this entity designs and manages, the TCF, is inextricably part of the processing undertaken by all actors in OpenRTB interested in legally operating in Europe. By using TCF as a starting point, and establishing, as the Belgian DPA does, that the activities performed under the TCF involve the processing of personal data, and that IAB Europe is a controller in relation to where this data is used within the OpenRTB system, the supervisory authority is able to do what other DPAs have failed to: analyse and comment on the whole ecosystem at once, even though it only lays some of the responsibility at IAB Europe's door.

An important side-effect of the decision here is that the Belgian DPA has started to sketch out the roles of the many different actors in the RTB ecosystem and envisage some clearer allocation of responsibilities which avoid the trap of nebulous responsibility described above. This allows both the Belgian DPA and those across Europe who signed off on the decision in the European Data Protection Board (EDPB) to build on this framework, and start to place actors in their own jurisdictions within it, without having to start from scratch. While DPAs have long been grabbing different bits of the metaphorical elephant, arguably now for the first time they have a formal decision that can serve as a blueprint for what the RTB elephant looks like as a whole.

In the rest of this paper, we first summarise the decision itself, and then step back and draw together an analysis across the whole ruling to understand its broader consequences, particularly those that are not visible from just a reading of the breaches, sanctions, or the Belgian DPA's press release.

2. Summary of the decision

What follows is an account of the main points of the nearly 130 page decision, showing the structure of the Belgian DPA's argument. For the reasons above, many of the key points and broader consequences in this ruling come out through a detailed reading of the reasoning and analysis of RTB more broadly, rather than looking simply at the breaches and sanctions, such as the changing of TCF policies, which are fully anchored in the IAB Europe's responsibilities alone.

2.1 The TC string is personal data

IAB Europe's entire TCF hinges on passing around a standardised text string (the "Transparency and Consent String", hereafter "TC string") between all the actors in the RTB ecosystem. This TC string supposedly represents a data subject's consent, objections, and preferences for the processing of their personal data, and is generated as a result of a user interacting with a consent management platform on a website or app. The Consent Management Platform (CMP) captures such preferences, encodes them and stores it in a TC string which will be shared with the organisations participating in the OpenRTB system as metadata. All processing of personal data that happens afterwards in the context of the TCF and OpenRTB is predicated on the values in this string.

The Belgian DPA states that the TC string is personal data under the GDPR. The TC string does not contain a unique identifier for a user, leading the regulator to agree with IAB Europe that the contents of the string do not directly identify a user.[21] In place of a unique identifier, the TC string is connected to a user by how it is i) stored on a user's device as a cookie, and retrievable by TCF members seeking to access it; and ii) used as metadata to a bid request made by a user's browser to indicate a user's recorded preferences.

The Belgian DPA states that the TC string can be considered personal data through two routes. Firstly, whenever the string is created and placed into or accessed from a user's cookies, personal data including a user's IP address will be visible to at least the consent management platform involved.[22] The result of this is that a TC string rarely, if ever, exists not associable with an identified or identifiable individual, and therefore it too is personal data. This reasoning holds a fortiori given the preponderance of personal data in the OpenRTB system in general beyond an IP address, such as unique cookie identifiers or

Veale v ICO, EW v ICO, Eveleen Coghlan (on behalf of C) v ICO [2021] UKUT 299 (AAC) [6–7] (United Kingdom).

16 Civil Liberties Union for Europe, 'Prevent the Online Ad Industry from Misusing Your Data - Join the #StopSpyingOnUs Campaign' (*Liberties.eu*, 4 June 2019) https://www.liberties.eu/en/stories/stop-spying-on-us-fix-ad-tech-campaign/275 accessed 5 February 2022; Tilman Herbrich and Elisabeth Niekrenz, 'Privacy Litigation Against Real-Time Bidding — Data-Driven Online Marketing: Enforcing the GDPR by Protecting the Rights of Individuals under Civil Law' (2021) 22 *Computer Law Review International* 129, 135.

17 The original and official version is in Dutch. Gegevensbeschermingsautoriteit (Geschillenkamer), *Beslissing ten gronde 21/2022 van 2 februari 2022: Klacht inzake Transparency & Consent Framework* (DOS-2019-01377, 2 February 2022). The Belgian DPA has provided an unofficial translation, and where we quote from the text, we use this translation: Belgian Data Protection Authority (Litigation Chamber), *Decision on the merits 21/2022 of 2 February 2022: Complaint relating to Transparency & Consent Framework* (DOS-2019-1377, 2 February 2022) (hereafter "Decision").

18 GDPR, art 56. Complainants named in the decision are Johnny Ryan, Pierre Dewitte, Jef Ausloos, Katarzyna Szymielewicz (represented under GDPR, art 80(1) by the Panoptykon Foundation, a Polish NGO), the Dutch NGO Bits of Freedom and the Belgian NGO La Ligue des Droits.

19 Decision, para. 281. A simple majority vote is possible in the case of dispute, but only if at least a month has passed, see GDPR, art 65(2–3). The decision was published sooner than a month after a final version was submitted to the EDPB, and so at least two–thirds support can be assumed.

20 See eg decisions by the French DPA, the CNIL, against adtech firms Teemo and Vectaury. CNIL, *Décision n° MED 2018-022 du 25 juin 2018*; CNIL, *Décision MED-2018-042 du 30 octobre 2018*.

21 Decision, para. 300.

22 Decision, paras. 302–3; on IP addresses as personal data see GDPR, recital 30; Case C-70/10 *Scarlet Extended* ECLI:EU:C:2011:771 [51] (on static IP addresses); Case C-582/14 *Breyer* ECLI:EU:C:2016:779 [49] (an example of a dynamic IP address being personal data).

other mechanisms of singling out a user.[23]

Secondly, the regulator uses a teleological argument, stating that if the purpose of processing is to single individuals out (i.e. to transmit preferences unique to them), then it may be assumed that the controller or another party can identify these individuals.[24]

2.2 IAB Europe is a data controller in the context of the TC string

The Belgian DPA states that, contrary to the defendant's claims, IAB Europe is a data controller in relation to the TC string. The analytical reasoning of the regulator consists of the following.

2.2.1 Access to personal data

As a preliminary note, it is important to remember that IAB Europe does not need to have access to TC strings in use to be considered a controller. Settled European case-law states that data controllers need no access to personal data to be found as controllers, a definition depending instead on whether parties have decisive influence on the means and purposes of processing.[25]

2.2.2 Purpose of processing

IAB Europe determines the purpose of the TC string itself: to "encapsulate and encode all the information disclosed to a user and the expression of their preferences for their personal data processing under the GDPR", such that this information is captured by the CMP, which in turn encodes and shares the string with the vendors.[26] However, the Belgian DPA does not stop here. It notes that the TCF is offered "with the aim of indirectly promoting the use of OpenRTB", with IAB Europe acting as a "hinge" between OpenRTB and the TCF.[27] This, the Belgian DPA argues, stems primarily from an explicit determination of purposes: the exhaustive and specifically worded list of potential purposes, created by IAB Europe, that OpenRTB entities are allowed to pursue when using the TCF.[28] This link begins to blur the responsibility of IAB Europe and draw them into determining the purpose of TCF–affiliated entities' use of OpenRTB — i.e. OpenRTB use in the EU — even though the Belgian DPA does not claim that IAB, Europe, TechLab or otherwise, is a controller with regard to the vanilla OpenRTB standard.

2.2.3 Means of processing

The Belgian DPA also establishes that IAB Europe determines the means of processing. IAB Europe establishes this contractually, as participants to the TCF must follow the binding rules integrated in the Terms and Conditions for the IAB Europe Transparency & Consent Framework (which in turn refer to further documents).

Firstly, such terms require entities to register with IAB Europe before being permitted to generate a TC string, and to follow particular technical specifications relating to how many aspects of processing may occur. For example, IAB Europe states that "every consent manager MUST" provide an API with very specific function calls that allow the TC string to be queried in real-time by, for example, adtech vendors that are embedded on a page.[29] They also determine the storage location and method of the TC string, as well as the retention period.[30]

Secondly, IAB Europe determines the means of processing by determining the recipients to whom the TC string may be shared with, and who not, by means of the dynamically updated Global Vendor List, the list of TCF-authorised adtech vendors approved and published by IAB Europe.[31] Publishers are not allowed to both use the TCF standard and work with any vendor who has not registered with the IAB Europe.[32] This in particular appears to distinguish the TCF from a "permissionless" standard such as HTTP or TCP/IP.

This has lessons for the limits of controllership as well as its extent. IAB Europe does not merely set the rules of the road, but determines, dynamically and contractually, which specific road all actors are allowed to use, and which not. While influence over means will remain a case-by-case test, this specific role of the IAB in this regard will mitigate concerns that standard-setting bodies like the ISO, IETF or W3C might find themselves data controllers: these merely provide documents with voluntary guidelines, whereas TCF is a members-only, centrally managed, and non-discretionary set of rules with an annual price tag of 1,200 EUR.

2.3 IAB Europe is not a controller of OpenRTB, but...

While the Belgian DPA notes that the scope of this decision applies solely to the TCF and its TC string, it notes that both the string and the Framework are interwoven with OpenRTB. Compliance of the OpenRTB with the GDPR is assessed as part of a holistic analysis of the TCF and its interaction with OpenRTB.[33] After all, the TCF was designed "precisely to bring the processing of personal data based on the OpenRTB protocol, among others, into conformity with the applicable regulations", and was "never intended to be a stand-alone, independent ecosystem".[34]

IAB Europe was found in the decision to play a pivotal role in OpenRTB, but this does not mean it is a data controller in respect of that particular protocol of standard. This role stems from the way the current version of the TCF is the tool on which OpenRTB actors rely on to justify compliance with the GDPR, and how the defendant facilitates membership and use of the OpenRTB to a significant number of participating organisations. Indeed, none of the Belgian DPA's logics rely on identifying IAB Europe or any other actor as the data controller of the OpenRTB protocol.[35]

Instead, IAB Europe's data controllership of the TCF and TC string, and the data controllership of a broader array of data controllers acting within the OpenRTB must, according to the Belgian DPA, be considered as part of a pattern of converging decisions.[36] This terminology is used by the EDPB to indicate where joint controllership will be found: where decisions both complement each other and are inextricably linked, and processing would not be possible without all relevant parties' participation in the process.[37]

Given the role of the TCF in (attempting to) legalise the actors' processing within OpenRTB, the Belgian DPA notes that the TCF

23 Decision, para. 305.
24 Decision, para. 310.
25 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* ECLI:EU:C:2018:388 [38]; Case C-25/17 *Jehovan todistajat* ECLI:EU:C:2018:551 [69]; Case C-49/17 *Fashion ID* ECLI:EU:C:2019:629 [69].
26 Decision, para. 335.
27 Decision, para. 336.
28 Decision, paras. 336–8.
29 Decision, para. 355.
30 Decision, paras. 347–53, 358–9.
31 Decision, para. 356.
32 Decision, para. 357.
33 Decision, para. 544
34 Decision, para. 368.
35 Decision, para. 495.
36 Decision, paras. 368, 370.
37 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (7 July 2020) 19.

cannot be regarded as an activity undertaken for IAB Europe's "own purposes or self-preservation", but instead "to facilitate further processing by third parties" — i.e. other adtech actors.[38] This allows the regulator to come to a much larger conclusion than IAB Europe's role in controlling the processing of just the TC string: "IAB Europe and the respective participating organisations should be considered as joint controllers for the collection and subsequent dissemination of users' consent, objections and preferences [the TC string], as well as for the related processing of their personal data" [emphasis added].[39] This embroils IAB Europe — which held that it was neither a controller or processor, and that the TC string was not personal data — into joint controllership of not just the TC string, but of related processing occurring with actors throughout the OpenRTB system, at least where processing relies on the TCF.

2.3.1 Relation with CJEU Fashion ID decision

At first glance, the DPA's approach to controllership might seem to contradict the CJEU in Fashion ID, where a website and an advertising plugin were joint controllers but only for the stage of obtaining the consent; such joint controllership by the website did not extend to the downstream processing of personal data by the organisation that owned the plugin (Facebook).[40] However, there are key differences in this case. In particular, IAB Europe are not the website responsible for securing consent; they are the organisation setting, inter alia, the list of purposes for which that consent can legally be obtained by all downstream actors, even when the data is passed from one adtech vendor to another, and the means by which it can be obtained, recorded and queried later on, and binding each of those actors technically and through policies.

The TCF's influence and its structural necessity to even the putative legality of the entire system spans actors down the chain of processing, unlike the website in Fashion ID, which, in the eyes of the CJEU, could only ever influence the first "phase" of processing — collection. Consequently, the view of the regulator does not seem out of line with the view of the CJEU in Fashion ID.

2.4 Who is IAB Europe a joint controller with?

If IAB Europe is not a joint controller with the abstract notion of the OpenRTB as a protocol, then who are these actors IAB Europe is joint controller with, and to what extent?

2.4.1 Consent Management Platforms (CMPs)

The Belgian DPA, in its factual analysis of the controllership situation of RTB, disagrees with the claim of IAB Europe that CMPs are "in principle" processors, concluding instead that TCF-registered CMPs play a significant role and therefore bear some (joint) responsibility.

CMPs' main task is to provide interfaces through which users indicate their preferences, and the TCF gives them some discretion over how to design these.[41] Because these interfaces can have a direct impact on users' choices,[42] CMPs bear joint responsibility over the processing of users' personal data within the TCF and OpenRTB ecosystem.

IAB Europe is a joint controller with CMPs since they determine the potential recipients through the Global Vendors List. This list of recipients is included by default in TCF CMPs' interfaces. Should CMPs choose to exclude some vendors from this list on their own volition or by request of the publisher, the Belgian DPA then considers that the CMP or the publisher are acting as data controller in that respect. However, this does not entirely remove the responsibility of IAB Europe, since without them this list of adtech vendors from which the CMPs and publishers pick and choose would not even exist.

2.4.2 Publishers

The Belgian DPA concluded that publishers act as data controllers for the processing of user's preferences in a TC string as well as their personal data processed in a bid request.[43] The TCF envisages publishers as controllers, deciding which (TCF-approved) CMP to contract, which adtech vendors are allowed to operate within their website or application, exercising control over the legal basis for a specific purpose, and excluding certain processing purposes.[44]

The Belgian DPA, however, notes that IAB Europe binds publishers through its TCF Policies to only use the processing purposes specifically laid out by IAB Europe, and to refrain from instructing CMPs to use any different processing purposes either. Consequently, unless publishers choose to ignore IAB Europe's policy (at which point, the TCF Policies forbid them from participating in the TCF), then IAB Europe is to be considered a joint controller with the publishers. Because publishers utilise CMPs, they act as a joint controller in all cases with regard to the TC string for the reasons similar to CMPs.[45]

It is worth noting that the Belgian DPA did not elaborate on the balance of responsibility between publisher–CMP, as this was not required in this decision, and in any case may differ on specific factual grounds.

2.4.3 Adtech vendors

Like publishers, many adtech vendors too are typically accepted uncontroversially as controllers. In further similarities to publishers, adtech vendors registered with the TCF are restrained in the processing purposes they can choose based on the list provided by IAB Europe. Consequently, IAB Europe is a joint controller with adtech vendors of these processing activities — except insofar as adtech vendors do further processing outside of this framework, such as by attempting to establish a legal basis independent of the TCF with regard to a data subject, or with adtech vendors not registered with the TCF and therefore not on the Global Vendor List.[46]

2.4.4 Summary

These findings together lead the Belgian DPA to conclude that "[IAB Europe] as well as the CMPs, publishers and participating adtech vendors should be regarded as joint data controllers for the collection and dissemination of users' preferences, objections and consent and for the subsequent processing of their personal data".[47]

2.5 Illegal processing and failed obligations

The regulator finds an array of breaches of the GDPR. They also analyse other provisions and find there were no breaches. For space, we consider only breaches here.

2.5.1 Illegal processing of the TC string

Because IAB Europe did not consider the TC string as personal data, it did not establish a legal basis for processing it: consent was not

38 Decision, para. 370.
39 Decision, para. 371.
40 Case C-49/17 *Fashion ID* ECLI:EU:C:2019:629.
41 Decision, para. 381.
42 Decision, para. 379.
43 Decision, para. 391, 394.
44 Decision, para. 387.
45 Decision, para. 396.
46 Decision, para. 399.
47 Decision, para. 402.

requested; contract necessity was inapplicable, and so legality hinged on an analysis of legitimate interest. Although the Belgian DPA found that generating and processing the TC string happened for a legitimate purpose (signalling user's preferences) and only included the necessary information to do so (necessity of processing test), they found that the third condition for legitimate interest—whether the processing that happened could be reasonably expected by the data subject—was missing. Because hundreds of advertising actors would be sent the TC string, with no information about this provided to the user, and no way to object to it[48], the Belgian DPA concluded this could not reasonably be expected, and thus there was no legal basis for the processing of the TC string.

It is worth noting that none of this reasoning is based on the e-Privacy Directive, which would require a finding that the TC string cookie was strictly necessary for a service requested by an end-user to avoid it requiring separate consent to store or access from a user's browser.

2.5.2 Illegal processing of personal data facilitated by the TC string

The purpose of the TCF String was to provide a legal basis for the processing of other personal data throughout the RTB ecosystem, but the Belgian DPA found that "none of the legal grounds proposed and implemented by the TCF can be lawfully invoked by TCF participants"[49], whether consent, legitimate interest, or contract.

Consent. Consent, as typically the most challenging legal basis to establish because of its strict requirements that it needs to be free, specific, informed and unambiguous, has a number of hurdles to its validity.[50] Firstly, the processing purposes that IAB Europe imposes on TCF participants are too vague and even misleading to render consent specific ("measure content performance"; "apply market research to generate audience insights").[51] Secondly, there are too many actors involved that it would require a disproportionate amount of time for data subjects to understand who they are consenting to and be meaningfully informed.[52] Thirdly, users cannot consent to downstream processes of enrichment of their bid requests by data brokers because they "cannot possibly be properly informed", as the TCF does not allow brokers to indicate what data they already hold on a particular user and what they do with it. Fourthly, CMPs considered by the Belgian DPA both provide insufficient overviews about categories of data collected,[53] and insufficient granularity about the different processing operations undertaken by each vendor.[54] Lastly, users cannot effectively withdraw consent, because after withdrawing consent the adtech vendor is in principle no longer able to process personal data of a data subject, and is thus unable to identify who that withdrawal signal belongs to.[55]

Legitimate interest. Given that consent cannot structurally be obtained, it is unsurprising that the Belgian DPA rejects legitimate interest as a ground within TCF participants' use of RTB. They do so in several ways. Firstly, they state that the TCF policies structurally prevent vendors in explaining their specific legitimate interests, instead abiding to generic IAB Europe–provided text, meaning that they will be unable to establish them.[56] Secondly, they note that necessity requires data minimisation, which is impossible to establish due to the lack of safeguards surrounding downstream data use.[57] Thirdly, similarly to concerns around consent, the Belgian DPA notes that there are too many participants, this time not relating to an individual's capacity to inform herself, but in relation to an individual's reasonable expectations of processing (failing the balancing test the legitimate interest so requires).[58] Lastly, they point to statements by the EDPB and the UK ICO as supporting their view that legitimate interest cannot be used in behavioural advertising and/or RTB.[59] While the Belgian DPA initially homes in its analysis on only legitimate interest purposes that "entail targeted advertising or profiling of the users", part of the reasoning they use, particularly around the lack of transmission safeguards and number of vendors, appears to relate to all legitimate interests communicated through RTB.[60]

Contract. Following EDPB guidelines, the Belgian DPA does not consider processing personal data for behavioural advertising a (pre) contractual necessity.[61]

Thus, the Belgian DPA concludes that processing of personal data in OpenRTB on the basis of the TCF is incompatible with the GDPR due to a lack of lawfulness and fairness.

2.5.3 Breach of Transparency

Similarly to the reasoning concerning the inapplicability of consent, the Belgian DPA finds that the processing purposes provided are too vague, not sufficiently clearly described, and in some cases are even misleading[62], showcasing that purpose 8 ("Measure content performance") and 9 ("Apply market research to generate audience insights") provide little or no insight into the scope of the processing. The decision notes the user interface is not transparent regarding the categories of the personal data processed or for how long the personal data processed will be retained if the user does not withdraw her consent. The identity of data controllers and adtech vendors for whom consent is obtained is absent too.

The decision further notes that while IAB Europe reserves the right to obtain records of consent from CMPs under the Terms & Conditions, they do not inform users of this processing.[63]

2.5.4 Breach of security

The Belgian DPA found that IAB Europe did not do enough to ensure that values in the TC strings actually reflected data subjects' preferences and were not falsified by participating organisations in the TCF, and that downstream actors actually abided by the preferences in the TC string when processing data instead of just ignoring them. the Belgian DPA highlighted that IAB Europe clearly foresaw the possibility

48 Decision, paras. 420–3.
49 Decision, para. 428.
50 GDPR, arts. 4(11), 7.
51 Decision, para. 433.
52 Decision, para. 435.
53 Decision, para. 434.
54 Decision, para. 436.
55 Decision, paras. 433–438.
56 Decision, para. 451.
57 Decision, para. 455.
58 Decision, para. 459.
59 Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203, 2 April 2013) https://perma.cc/A8S2-3Y94 46; Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (*Information Commissioner's Office*, 20 June 2019) https://perma.cc/X7PX-EL3L 17.
60 This may explain why the sanctions, described further below, refer to the prohibition of all legitimate interests in their current form via the TCF, rather than exempting "non-marketing-related" purposes. This is a point being challenged by the IAB. See IAB Europe, 'APD Decision on IAB Europe and TCF' (*IAB Europe*, 3 February 2022) https://perma.cc/SS32-P6D9.
61 Decision, para. 462.
62 Decision, para. 433.
63 Decision, para. 468.

of this happening, since it explicitly mentions that this is not allowed in its TCF Policies[64], but had taken no organisational or technical measures to verify or enforce this.

2.5.5 Illegal international transfers

The Belgian DPA finds that there is an infringement of the GDPR in relation to international transfers with no legal bases (Articles 44 to 49 of the GDPR), but lacks evidence of a systematic international transfer to act on an infringement due to this topic not being covered in an earlier assessment report, and so does not sanction IAB Europe on this ground.[65] They note that IAB Europe claim the TCF is not designed for international transfers, but that given that the TCF is the method through which OpenRTB is supposedly brought into compliance with the GDPR, IAB Europe cannot pick and choose which parts to facilitate or not in the absence of other means to facilitate them within a joint controllership arrangement.[66]

2.5.6 Accountability

Breaches of accountability are split between organisational aspects of IAB Europe, and the possibility or impossibility of broader accountability in the TCF and OpenRTB systems. In fact, the authority denotes that IAB Europe does not sufficiently monitor compliance with the rules it has developed with regard to participating organisations.[67] IAB Europe was found to have not appointed a DPO, undertaken a DPIA, or maintained records of processing, all of which effectively stem from its denial that it was either a controller or that the TC string was personal data.[68]

The systemic issue is of greater interest. The Belgian DPA brings IAB Europe into broader accountability requirements by considering its role in the controllership operations. Consider, for example, that the TCF's terms and conditions already account for the possibility of falsification or modification[69] of the TC string by its vendors and CMPs, and attempts to prevent it. The Belgian DPA seems to take this to indicate that while IAB Europe seeks to manage consent and objection, it does not have the ability to ensure conformity to those rules, the integrity of the signals being sent, and the validity of the legal bases it facilitates the dissemination of.[70] Consequently, the joint controllership operation fails in terms of the accountability principle.

2.6 Summary of corrective measures

In view of the infringements, the Belgian DPA ordered a series of corrective measures aimed at bringing the current version of the TCF into compliance with the GDPR. The measures place requirements on the IAB Europe directly, and through changes to design and governance requirements, also impact upon other TCF participants. In effect, because the TCF binds its participants through a mixture of code, club and contract, the Belgian DPA has identified it as an effective conduit through which obligations to attempt to bring the entire system closer to legality can be passed.

2.6.1 Measures relating to IAB Europe

While IAB Europe is not liable for all RTB, insofar as it attempts to orchestrate a system of compliance, it becomes partially responsible for ensuring that compliance is real. The Belgian DPA consequently ordered the following.

Legal basis. IAB Europe is required to limit issues around the legal bases used by TCF participants. They must prohibit the use of legitimate interest by updating their terms of use. This prohibition entails the review of all current purposes reliant upon legitimate interests. It also prohibits the use of "default consent" in CMPs. In this line, it further ordered the deletion of personal data collected based on a, already deprecated, "globally scoped" TC string. They particularly note the role of data protection by design as mandating these obligations.

Transparency obligations in relation to TCF-registered-CMPs. Reasoning based on transparency rights both overlap with and go beyond the obligations around legal bases mandated under data protection by design. Here, the Belgian DPA requires IAB to force TCF-registered-CMPs to: i) prevent automatic authorisation of participating vendors relying on legitimate interest for their processing activities; ii) prevent consent from being ticked by default in the CMP interfaces; iii) adopt a uniform and GDPR compliant approach to ensure their information is both thorough but also "precise, concise and understandable", to avoid users being "surprised". This deceptively simple demand may in fact require rethinking of the entire RTB system, and will be discussed further below.

Security obligation. As part of its security and integrity obligations, IAB Europe must "take the necessary steps to ensure the validity, integrity and compliance of users' preferences and consent" transmitted by CMPs to adtech vendors,[71] given that a signal may be tampered with and not adhered to.[72] It also orders for a strict audit and vetting of organisations that join the TCF.

Data subject rights. Data subject rights against any other actor in the joint controllership operation may be exercised against IAB Europe, and this must be facilitated.[73] However, the Belgian DPA was not in a position to establish a violation of the Articles 15-22 GDPR.[74] The Belgian DPA only based this requirement on data protection by design, as they did not look into the details of data subject rights as part of their investigation. The initial lack of consideration of this was highlighted by the Dutch DPA in the EDPB, who required the Belgian DPA to include a response to the complaints by NGO Bits of Freedom on this topic.[75]

Accountability obligations. IAB Europe is ordered to put into place records of processing of personal data in the TCF by IAB Europe, a DPO, and undertake a DPIA with regard to the processing activities under the TCF and their impact on the processing activities carried out under the OpenRTB system.

IAB Europe must submit an action plan to the Belgian DPA within two months, and complete the obligations within six months, and will receive a daily penalty of 5,000 EUR for non-compliance. They may appeal in Belgium to the Marktenhof (Market Court), including requesting a stay of the timeframes the Belgian DPA sets, and potentially from there to the Hof van Cassatie (Court of Cassation). Given the wide complexity of this case and the way it touches on many aspects of data protection law, it seems probable that any of these proceedings may be stayed for a preliminary reference to the CJEU. Furthermore, if they dispute procedural issues (such as regarding a

64 Decision, para. 485.
65 Decision, para 490.
66 Decision, para. 491.
67 Decision, para. 57.
68 Decision, paras. 507–524.
69 IAB Europe, 'Transparency & Consent Framework Policies' (IAB Europe, 22 June 2021) https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/#13_Working_with_CMPs, ch. III(13), para. 6.
70 Decision, paras. 493, 500.
71 Decision, para. 494.
72 Decision, para. 535.
73 Decision, para. 535.
74 Decision, para. 506.
75 Decision, para. 277.

right to be heard) with the EDPB's treatment of this case in the one-stop-shop, IAB Europe might attempt an action for annulment at the General Court of the CJEU.

2.6.2 Measures relating to other TCF participants

As this operation constitutes a joint controllership relation, the sanctions imposed on IAB Europe do not reflect the last word in enforcement that may flow from this ruling. There is a limit to what IAB Europe can do to rectify data that has already been collected.

Adtech vendors. While the processing of the TC string is found illegal, and derives from the inappropriate choices made by IAB Europe as data controller, IAB Europe is no longer in a position to delete the TC strings that are in existence — only other adtech firms holding the data have that ability.[76] While IAB Europe is told to delete some data that they may have themselves held from their so-called "global consent" mechanism, a short-lived and controversial attempt to re-use consent to vendors across sites and apps, it is interesting the Belgian DPA did not go so far as to attempt to order them to organise the deletion of data held within their many identified joint controllership arrangements. This choice in itself indicates how difficult cross-border joint controllership operations can be to practically regulate where data is held to different degrees by different controllers.

CMPs' and publishers' accountability obligations. The Belgian DPA warns forebodingly that "it is the responsibility of the CMPs and the publishers who implement the TCF, to take the appropriate measures, in line with Articles 24 and 25 GDPR, ensuring that personal data that has been collected in breach of Articles 5 and 6 GDPR is no longer processed and removed accordingly."[77]

As this decision has been given the blessing of the EDPB via the one-stop-shop, this is one of many parts of this ruling that effectively put actors in the RTB ecosystem "on notice" that regulators may take a different view of their status and the nature of their processing operations going forward.

3. The DPA's Impossible Asks

Though the IAB Europe claims to offer the TCF to make OpenRTB compliant with the GDPR, the Belgian DPA tellingly "notes, for the record, that it is uncertain whether, in view of its current architecture and support of the OpenRTB protocol, the TCF can be reconciled with the GDPR."[78] In this light, the above remedial measures placed on IAB Europe look very different. Are these requirements actually irreconcilable with the fundamental functioning of RTB, as legitimised by the TCF or any other envisageable measure? We believe there are several reasons to think they are, and list some of them below.

3.1 Informed consent as irreconcilable with RTB's scale and unforeseeability

The Belgian DPA asks IAB Europe to inform data subjects about the processing of their personal data following the transparency principle. The information should, inter alia, be comprehensible, concise, and prevent unpleasant surprises for data subjects down the line. While transparency failures in the context of normal data processing are often easy to remedy, the structure of RTB makes meeting the GDPR criteria here a difficult, if not impossible, task. We focus here on establishing consent, as the Belgian DPA already makes it clear legitimate interests are prohibited — and this is a fortiori the case upon considering the requirements of the e-Privacy Directive.

3.1.1 Specific processing and categories unknowable in advance

The purpose of RTB is to let a large number of vendors bid on impression space, and transfer data to an even larger array of downstream actors such as data brokers for "enrichment". At the point of consent, it is structurally unclear what types of data will be combined, collected or retained in order to inform the bids, as downstream actors do so opportunistically and driven by the economic incentives of a competitive bidding market. As a result, the only information as to the categories of personal data processed that can be provided before consent would seem to be unacceptably wide and open-ended — and to remedy this without changing the very structure of RTB, not just the TCF, would require a crystal ball to see what downstream data management platforms will do with specific users' bid requests.

3.1.2 Too many actors for transparency; no obvious way to reduce them

IAB Europe's approach to RTB in Europe promises its participants an open market, where an open-ended number of actors can participate in bidding or enrichment, as long as they are members of the TCF. Necessarily, this entails that any visitor to a website faces a need to consent to hundreds of vendors simultaneously, because it is unclear beforehand which vendors will wish to be implicated in processing.[79] The Belgian DPA makes a repeated point throughout the decision that establishing legal bases in the face of so many actors at once is not feasible.[80] Even when configured in the best possible ways, CMPs squeeze so much information into multi-tabbed boxes that it would take over half an hour of constant reading on average for an adult of average literacy to read all the descriptions, let alone any linked policies.[81] The Belgian DPA's finding that the required reading is already disproportionate would be only adversely affected by its further stipulation that information about each vendor is unacceptably uniformly standardised by IAB Europe and needs to in more detail reflect the specificities of each actor's processing,[82] making compliance structurally less possible regardless of tweaks.

Consequently, unless RTB was structurally changed to only allow a much smaller and more immediately identifiable and comprehensible subset of bidders to process data from a specific site or app visitor (eg on a random or rotating basis), it is hard to see how it could ever provide the transparency required by the Belgian DPA to establish informed consent. Even consent to only subsets of actors would suffer from further practical and legal hurdles that would make it infeasible, such as an inability to easily withdraw consent from previous recipients or to remember a consent setting from visit to visit, let alone its impacts on the deeper functioning of RTB.

3.2 Data subject rights lack obvious communication channel

The Belgian DPA requires IAB Europe to facilitate within the TCF processes such that users can exercise their data rights. However,

76 Decision, para. 535.
77 Decision, para. 535.
78 Decision, para. 492.
79 Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020)* (ACM 2020) 5 (noting a median of 315 vendors [lower quartile 58, upper quartile 542] establishing a legal basis among the top 5 CMPs on UK websites).
80 Decision, paras. 435, 459, 472.
81 Nouwens and others (n 79) 6.
82 Decision, para. 436.

the entire RTB ecosystem was designed as a one-way data flow from individuals to adtech actors, through cookie IDs, fingerprinting technologies, and other systems. IAB Europe would become responsible for forwarding or facilitating any access or erasure request it receives to, at the very least, the hundreds of vendors in the TCF.

This may not be technically impossible: individuals would need to firstly establish all of the relevant identifiers that they are associated with in the adtech ecosystem, for example, through a dedicated website or app using all the plugins, SDKs and methods across TCF vendors which are used routinely to identify users, but instead purposed to identifying users for access rights. The industry is no stranger to a website testing whether users are identifiable to ad companies for the purposes of offering them supposedly control — this is the functionality of an opt-out (from seeing customised adverts, but not data collection) service such as YourOnlineChoices.eu, an implementation of the now defunct IAB Europe OBA [Online Behavioural Advertising] Framework.[83] However, the problem becomes more difficult considering that access rights also need to be exercised vis-a-vis data management platforms and demand-side platforms which may not have the tracking systems that can directly identify users, but hold large amounts of data relating to identifiable individuals.[84] This appears to require significant engineering effort. Furthermore, it is unclear how each of these vendors would send the data to the individuals requesting it, given their usual means of communication is through advertising space in a user's browser, rather than through name, email or similar, even if some will hold the latter information.[85] As a result, IAB Europe will have to reconcile an industry-wide tension, where for reasons of system design, individuals are perfectly identifiable for the purposes of data processing, but imperfectly identifiable for purposes of permitting them.[86] This certainly seems a significant hurdle for IAB Europe to accomplish within 6 months, given that seemingly no effort so far has been made in integrating such subject rights within the TCF.

3.3 Withdrawal or even refusal of consent is structurally impossible without constant invasive data processing

The Belgian DPA clearly sees the issue with manifestly illegally configured CMPs, noting as they are responsible for guiding the user to submit their preferences and generating the consent string, they "[constitute] the cornerstone of the TCF".[87] It instructs IAB Europe to bind CMPs themselves to be unable to be illegally configured.[88] However, some issues with CMPs seem trickier to solve, and indeed go beyond any possible configuration publishers could implement today.

Firstly, users have no easy record of which publishers they have visited, and which trackers were implicated, other than meticulously maintaining and trawling through the browsing histories across their devices.

Secondly, even if all publishers are found, the CMP interfaces that are often inescapable when first interacting with a website or app, are unfindable in equal measure if a user wants to change their previous preferences.

Thirdly, even if the interface can be recalled, there is no guarantee that CMPs are positioned to support a user withdrawing their previous consent. The dynamic nature of the Global Vendor List, or the choices that publishers or CMPs make in relation to it, means that upon a future visit the user may well find the vendors previously given consent to have disappeared from the interface and are unavailable to communicate a withdrawal to. As far as the authors can tell from publicly available sources, the Global Vendor List has had 129 changes since August 2019.[89] The limited enforcement structure of the TCF (see below) furthermore foresees that if an organisation is found to be processing data incorrectly, they should be removed from the list, making withdrawal the hardest against the shadiest actors. Furthermore, even if such vendors were available, a withdrawal of consent currently is designed to stop a bid request reaching downstream vendors via other adtech actors. Individuals are typically identified by demand side platforms and data management platforms through cookie matching and other combinations. As a result, for a withdrawal of consent to be as effective throughout the ecosystem as a positive consent signal would paradoxically require exactly the type of invasive and surprising device matching, data combination and user identification that a user wishes to cease or never occur. This would have to occur every time a user expressed no consent — significant amounts of a user's identifiable information, including on the website they were visiting, would have to be transmitted entirely throughout the ecosystem simply to prevent processing that a user may never have consented to. So, too, might users making sporadic use of tracking blocking technologies paradoxically find themselves in a situation where their efforts to prevent tracking hamper their ability to withdraw consent from controllers they clearly do not wish to process their personal data.

If IAB Europe has to contract with CMPs to ensure that withdrawal of consent is as easy as giving it, and this is as structurally impossible as described above, it seems difficult to imagine what kind of requirements IAB Europe could place on CMPs that would still be compatible with the functioning of RTB.

3.4 Insecurity in RTB is structurally invisible to IAB Europe

The Belgian DPA noted the lack of systematic monitoring of compliance by IAB Europe with the TCF rules by the participating organisa-

83 IAB Europe, 'Announcement of Formal Withdrawal of The "IAB Europe OBA Framework" of 2011' (IAB Europe, 31 March 2021) https://iabeurope.eu/all-news/announcement-of-formal-withdrawal-of-the-iab-europe-oba-framework-of-2011/ ("Technically, the OBA Framework requires vendors to stop the delivery of OBA ads, though not the collection of OBA data").

84 Muhammad Ahmad Bashir, 'On the Privacy Implications of Real Time Bidding' (PhD, Northeastern University 2019) 3.

85 See reporting on a recent decision of the Polish DPA against a publisher highlighting difficulties in this regard, Panoptkyon Foundation, 'Hide and Seek: Polish DPA Agrees that People Should Be Able to Access Their Advertising Profiles, but There's No Way to Do So' (Panoptkyon Foundation, 24 January 2022) https://en.panoptykon.org/polish-dpa-agrees-people-should-be-able-access-their-advertising-profiles accessed 6 February 2022.

86 Michael Veale and others, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105; Chris Norval and others, 'RECLAIMING Data: Overcoming App Identification Barriers for Exercising Data Protection Rights' in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (UbiComp '18, ACM 2018).

87 Decision, para. 544.

88 cf. Nouwens and others (n 79), where ~88% of studied CMPs were not configured in compliance with minimal legal requirements, themselves below levels specified in parts of this decision.

89 As indicated from the latest version of the file https://vendor-list.consensu.org/v2/vendor-list.json. Between 2018–20, a different vendor list hosted at https://vendorlist.consensu.org/vendorlist.json was used that supported up to 4095 changes, however it is no longer archived by IAB Europe and no publicly available changelist is available from their servers to assess previous changes.

tions.[90] At first glance, it may appear that this obligation is disproportionate. Complying with the law surely does not mean binding others around you such that they cannot disobey the law.[91] However, considering the structure of responsibilities that the Belgian DPA has established, it becomes more reasonable. According to this decision, an adtech vendor is in a joint controllership operation with IAB Europe, whose purpose is to facilitate compliance. However, the design of the TCF splits this up such that the organisation that aims to facilitate compliance, and effectively complete the allocation of GDPR responsibilities in the joint controllership arrangement, is unable to actually see that it is doing so. It is because these organisations are tied in a joint controllership operation, where they must determine "respective responsibilities for compliance with the obligations'' that together make a coherent compliance approach,[92] that the Belgian DPA can find that this division is technically and factually structured to not follow data protection principles, and thus oblige the part of the operation within jurisdiction and partly responsible to fix it. However, whether it is fixable can be questioned on a number of grounds.

3.4.1 IAB Europe does not intermediate server-to-server transfers

IAB Europe's announced Vendor Compliance Programme,[93] after the hearing in this decision had concluded, which the regulator notes is manifestly insufficient in relation to the scope of this decision. Focussing on "live" deployments of TCF vendors on websites provides no insight into the "invisible" side of RTB happening between servers, representing a majority of RTB functions and which cannot be seen from an "automated audit" approach.[94] Scholars studying these transfers have to model them, as it appears to be complex to study them directly from the Web.[95] However, IAB Europe does not intermediate between these firms, so short of setting up a programme where server-to-server transfers cannot happen without being scrutinised by a third party, the extent to which IAB Europe can actually comply to remedy the structural failures that the TCF enables seems limited indeed.

3.4.2 Consent-string fraud compounds quickly

IAB Europe will still need to address the constant possibility of consent-string fraud and conflict of interests among its participants, which act upon their own incentives to allow target advertising.[96] The TCF will need to deal with the distributed risk among its players, since falsified consent strings are able to quickly spread, triggering and multiplying liability risks for other adtech vendors that may consume such strings.[97] Publishers and vendors could be deemed liable in the chain of consent.

This may further have interesting consequences for managed initiatives for automated consent signals from browsers, as it indicates there are conditions that the organisations managing them could be in part responsible for their integrity and interpretation.

3.4.3 Independence of auditing

It can further be questioned whether an audit system can be effective in the current structure of IAB Europe. It has only a yearly turnover of just 2.5m EUR.[98] Furthermore, the potential impartiality of such an audit scheme is highly questionable, given that IAB Europe is itself a membership organisation composed of the bodies to be audited, which in turn would rely on a positive audit in order to operate in Europe.

4. Clarity, Consequences and Conclusions

All things considered, IAB Europe and the RTB ecosystem it facilitates seem caught between a rock and hard place. They are unable to address the fundamental tensions between the technical functioning of RTB and the requirements of lawful bases for processing and support for data subject rights that their role as a (joint) controller requires. At the same time, they are also unable to divest themselves from the tent of illegality they have spread over the advertising industry to escape the inevitable sanctions that non-compliance will exact. This conclusion seems to run in the face of their aspirations, even following this decision, to turn the TCF into a national or international GDPR code of conduct under data protection law. The conduct it would codify has deep and fundamental tensions which appear to render data protection compliance based on it structurally impossible.[99]

Where next for IAB Europe, the TCF, RTB and its European participants? We offer some concluding thoughts below.

4.1 Enforcement and TCF participants

Actors in the TCF seem to have delegated thinking about their structural data protection positions and roles to IAB Europe, accepting assumptions that both the Belgian DPA and EDPB clearly disagree with. This decision means that all TCF players will be forced to rethink their own positions, taking into account their factual processing activities.

This does not stem from any direct effect that this decision has upon actors other than IAB Europe. Given that this case has already passed through the GDPR's EDPB consistency mechanism,[100] it seems highly likely that EU DPAs will use this decision as a foundational template for consistent application of the Regulation in its understanding of the roles and responsibilities within RTB.

Consequently, IAB Europe's messaging to its members in response to the ruling that "the APD decision does not make it much easier for local Data Protection Authorities to attack specific vendors, pub-

90 Decision, paras. 487–9.
91 On the consequences for legitimacy of such "cybernetic regulation" or "regulative code", see Mireille Hildebrandt, 'Legal and Technological Normativity: More (and Less) than Twin Sisters' (2008) 12 *Techné: Research in Philosophy and Technology* 169, 178; and generally, Laurence Diver, 'Digisprudence: The Design of Legitimate Code' (2021) 13 *Law, Innovation and Technology* 325.
92 GDPR, art 26(1).
93 IAB Europe, 'IAB Europe Launches New TCF Vendor Compliance Programme' (IAB Europe, 26 August 2021) https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/ accessed 6 February 2022.
94 Robbert-Jan Willem van Eijk, *Web Privacy Measurement in Real-Time Bidding Systems: A Graph-Based Approach to RTB System Classification* (PhD, Leiden University 2019) 201.
95 Muhammad Ahmad Bashir and Christo Wilson, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) *2018 Proceedings on Privacy Enhancing Technologies* 85.
96 Kayleigh McCrea, 'Adtech Vendor Caught Tampering with Consent Signals' (Confiant, 22 January 2022) https://www.confiant.com/privacy-hub/consent-tampering accessed 6 February 2022.
97 We do not wish to speculate here on the details of the possibility of using cryptographic techniques to address at least the fraudulent production (rather than adherence to) consent strings, suffice it to say that we see a range of daunting challenges to doing this securely and verifiably within the current structure of RTB, and any proposal would need careful vetting by the academic community.
98 Decision, para. 565.
99 IAB Europe (n 60).
100 GDPR, art 65.

lishers or CMPs" seems somewhat premature.[101] IAB Europe further argues that, as they may appeal this decision nationally in Belgium, this prevents other DPAs in any EU Member State from bringing national proceedings against any of the hundreds of other actors in RTB, which seems an unlikely conclusion or legal outcome.[102]

A range of other consequences may follow. This ruling opens up the way for individuals and civil society organisations to take different forms of action, such as making data rights requests across joint controllership arrangements identified or putting pressure on publishers or CMPs based across the EU. Many EU DPAs will already likely be investigating adtech actors, and so this decision may also enter their thinking in the middle of an investigation, rather than at the start. The CJEU may end up considering aspects of any appeal, although that would delay regulatory action into the distant future again. Days after this decision, the Dutch DPA announced that actors in the Netherlands should stop profiling users with real-time bidding and associated tracking architectures, although did not yet reveal an enforcement schedule.[103]

4.2 Future of RTB

Without the TCF providing a lawful basis for processing in the context of OpenRTB, the Belgian DPA's logic turns the protocol into a poisoned well for actors looking for a way to start or continue the practice of bidding-based advertisement. Even if other RTB systems, such as Google's Authorised Buyers, suffer similar structural deficiencies, the fact that they do not have a direct ruling on their name might make it more attractive for inexperienced publishers in particular in the short-term, further concentrating a market already suffering from a lack of meaningful competition. Google's data protection fate in this regard largely sits with the Irish DPA, and the firm was named in many of the same complaints that were forwarded through the one-stop-shop to Belgium; it will be interesting to see whether there are parallels between any decision from Ireland compared to this one.

Furthermore, this ruling might also give impetus for alternative advertising logics that have been pushed to the margins because of the hegemony of real-time bidding to re-emerge, such as contextual advertising, user elicitation of advertising, or subscription models. The push away from RTB might further converge with recent international efforts to ban surveillance-based advertising at large.[104] Because data protection and privacy seeks to prevent open and low-friction dissemination of user data, it can be argued that regulating it empowers platforms, particularly those with large first-party datasets, and those with control of significant infrastructures for on-device targeting such as Google (Chrome) and Apple (iOS). To this end, work between different regulators concerned with the digital economy is necessary to ensure both competition law and data protection can be enforced together. The European Data Protection Supervisor's Digital Clearinghouse, a vision of the late Giovanni Buttarelli, is notable in this regard.

5. Conclusion

In this paper, we have argued that this decision is a milestone with important, broad and deep potential impacts. Firstly, the scope of the controllership and processing operations identified has, to an extent we have never seen before in either case-law or published regulatory decisions, considered and analysed a significant extent of the entire RTB ecosystem at once. This will likely have wider impacts for pan-European enforcement, and provide a blueprint going forwards in line with the GDPR's consistency mechanism. Secondly, while the decision appears to give a chance to IAB Europe to fix the TCF, the chalice the Belgian DPA hands the defendant is actually somewhat poisoned. Upon a detailed reading, in the context of how RTB does and could work technically, it becomes apparent that much of what the Belgian DPA asks ranges from structurally challenging to impossible without rethinking how RTB itself works. These "impossible asks" leave IAB Europe and its participants faced with a cliff edge. While this is far from the end of the saga of online advertising, tracking and data protection law, it may in retrospect be a very important moment indeed.

Acknowledgements

The first author was party to a complaint concerning RTB and IAB Europe filed in the United Kingdom in 2018; this complaint was not passed to the Belgian DPA and does not form part of the decision discussed. All authors would like to express their sincere gratitude for the extremely valuable and extraordinarily fast reviewer comments to and editorial support and handling of this article.

101 IAB Europe (n 60).
102 IAB Europe (n 60).
103 Jasper Houtman, 'Toezichthouder: advertentiebranche moet direct stoppen met online volgen bezoeker', (*FD*, 7 February 2022) https://fd.nl/tech-en-innovatie/1429434/toezichthouder-advertentiebranche-moet-direct-stoppen-met-online-volgen-bezoeker accessed 8 February 2022.
104 See eg Finn Myrstad and Ingvar Tjøstheim, 'Time to ban surveillance-based advertising. The case against commercial surveillance online' (Forbrukerrådet, June 2021). See also the Tracking Free Ads coalition, co-founded by Paul Tang MEP.