

CompLex



Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Tervel Bobev

Track or Treat

Personal Data Protection and Behavioural Targeting in Web Advertising

1/2022



UiO : Det juridiske fakultet

Henvendelser om denne bok kan gjøres til:

Senter for rettsinformatikk

Postboks 6706 St. Olavs plass

0130 Oslo

<http://www.jus.uio.no/ifp/om/organisasjon/seri/>

ISSN 2703-8777 Complex (online)

Grafisk produksjon: 07 Media AS – 07.no

I. Preface

This report is a revised and slightly condensed version of a thesis originally submitted in partial fulfilment of the requirements for a Master of Laws degree at the University of Oslo. The thesis in question was researched as part of the ‘Security in Internet Governance Networks: Analysing the Law’ (SIGNAL) project of the Norwegian Research Center for Computers and Law (NRCCL), itself a branch of the University of Oslo’s Department of Private Law. The SIGNAL project was made possible by funding from the Norwegian Research Council and UNINETT Norid AS, with support from the University of Oslo.

My work owes a particular debt to my supervisor, Professor Lee Andrew Bygrave, whose guidance, patience, and insightful feedback elevated the final product. In addition, thanks go to Luca Tosoni, Peter Davis, Professor Tobias Mahler, and Christiane Hunsbedt for their support and input during the writing process. Finally, I extend my gratitude to Veselin Trakiyski for his technical insight into Adtech.

Any and all deficiencies in this text are attributable solely to myself. References to legal instruments are to their amended states as of 01 December 2021.

The original thesis was finalised in June 2021 and defended in October 2021. Technical developments continue at breakneck speed, with regulatory developments invariably following. Eventually, this text will become an artifact, though I hope that its message stays relevant: privacy matters.

Contents

I. Preface	3
II. Table of Abbreviations	6
III. Abstract	8
1 Introduction	9
2 An Overview of Adtech	11
2.1 Contextual Advertising	12
2.2 Programmatic Advertising and Real-time Bidding	13
2.2.1 Real-time Bidding: A Step-by-Step Explanation	14
2.2.2 Step 1	14
2.2.3 Step 2	15
2.2.4 Step 3	16
2.2.5 Step 4	16
2.2.6 Step 5	17
2.2.7 Step 6	17
2.2.8 Step 7	17
2.2.9 Step 8	17
2.2.10 Step 9	17
2.2.11 Summary	17
2.3 Online Tracking	19
2.3.1 Methods of Online Tracking	19
2.3.2 Stateful Tracking	19
2.3.3 Cookies and Storage Trackers	20
2.3.4 Cookie Successors – FLoC and FLEDGE	24
2.3.5 Etags and Cached Trackers	27
2.3.6 Stateless Tracking	27
2.3.7 Fingerprinting	28
2.3.8 Web Beacons	30
2.3.9 Unique First-Party Identifiers	31
2.3.10 Cross-Device Tracking and Summary	32
2.3.11 Results of Online Tracking	33
3 Adtech and the General Data Protection Regulation	36
3.1 Background to the GDPR	36

3.2	Applicability of the GDPR.....	37
3.2.1	Material Scope.....	37
3.2.2	Pseudonymization, Anonymization, and Digital Advertising	41
3.2.3	Territorial Scope.....	44
3.3	Assigning the Roles of RTB Actors.....	50
3.3.1	Users.....	54
3.3.2	Publishers.....	54
3.3.3	Actors in FLoC and FLEDGE.....	56
3.3.4	Advertisers.....	57
3.3.5	SSPs, DSPs, Networks, Exchanges, and Brokers.....	57
3.3.6	CMPs.....	58
3.3.7	The IAB.....	59
3.3.8	Summary of RTB Roles and the Morass of Joint Controllership	62
3.4	The Seven Principles of Personal Data Processing.....	63
3.5	Legal Basis for Behavioural Tracking: Why it Never Hurts to Ask..	64
3.5.1	Contractual Performance.....	64
3.5.2	Legitimate Interests.....	65
3.5.3	Consent.....	69
3.6	Requirements for Consent under the GDPR.....	70
3.6.1	Freely Given Consent.....	70
3.6.2	Freely Given Consent and Dark Patterns.....	74
3.6.3	Freely Given Consent and Cookie Walls.....	78
3.6.4	Specific Consent.....	80
3.6.5	Informed Consent.....	84
3.6.6	Unambiguous Consent.....	87
3.7	Special Categories of Personal Data.....	91
3.8	Security under the GDPR.....	94
3.8.1	Nature of Processing: Multimodal, Automatic, and Possibly Sensitive.....	95
3.8.2	Scope of Processing: Broad.....	95
3.8.3	Context of Processing: Broad and Unrestrictive.....	95
3.8.4	Purposes of Processing: Profiling of Individuals.....	95
3.8.5	Specific Risks.....	96
3.8.6	Conclusion on Appropriate Security Level.....	96
3.8.7	Achieving an Appropriate Level of Security.....	97
3.9	Transparency Issues.....	99
4	Conclusion.....	102
5	Bibliography.....	107

II. Table of Abbreviations

Abbreviation	Meaning
A29WP	Article 29 Working Party
AND	Ad Network
ADX	Ad Exchange
AEPD	Agencia Española de Protección de Datos (Spanish DPA)
AP	Autoriteit Persoonsgegevens (Dutch DPA)
APD/GBA	Autorité de protection des données/Gegevensbeschermingsautoriteit (Belgian DPA)
Adtech	Advertising Technology
CJEU	Court of Justice of the European Union
CMP	Consent Management Platform
CNAME record	Canonical Name record
CNIL	Commission Nationale Informatique & Libertés (French DPA)
DMP	Data Management Platform
DPA	Data Protection Agency
DPC	Data Protection Commission (Irish DPA)
DPD	Data Protection Directive
DSB	Datenschutzbehörde (Austrian DPA)
DSP	Demand-Side Platform
ECHR	European Convention on Human Rights
EctHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union

Abbreviation	Meaning
Etag	Entity Tag
FLEDGE	First 'Locally-Executed Decision over Groups' Experiment
FloC	Federated Learning of Cohorts
GDPR	General Data Protection Regulation
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
IAB	Interactive Advertising Bureau
ICO	Information Commissioner's Office
LSO	Local Storage Object
PARAKEET	Private and Anonymized Requests for Ads that Keep Efficacy and Enhance Transparency
PII	Personally Identifiable Information
RTB	Real-Time Bidding
SSP	Supply-Side Platform
TCF	Transparency and Consent Framework

III. Abstract

Behaviourally-targeted online advertising plays a major role in financing the modern internet economy. Yet, its core business model relies on user surveillance and data sharing between opaque partnerships of multitudinous industry partners. This report interrogates the compatibility between the technical and organizational underpinnings of behaviourally-targeted advertising and the legal requirements of European Union data protection law. The juxtaposition of real-time bidding and online tracking on one hand and the requirements of the General Data Protection Regulation (GDPR) on the other reveals fundamental issues in delineating and regulating controller-processor relationships, securing an appropriate standard of consent as a legal basis for data processing, and maintaining appropriate levels of security and transparency. This report concludes that these issues are largely inherent in the technological and organizational structure of the behaviourally-targeted advertising industry, and only further exacerbated by pervasive noncompliant conduct on the part of the industry. Currently proposed technical solutions for the data protection gap in behaviourally-targeted advertising fall short of achieving harmony with European Union law, indicating the need for a regulatory push toward personal data-free and privacy-friendly technologies.

1 Introduction

Targeted advertising permeates modern society, influencing far more than simple consumer behaviour during the procurement of goods or services. Alongside television screens and milk brands, the sophisticated online advertisements of today tout political platforms, societal views, and even dubious scientific claims.

On the political level, the utilization of targeted marketing initiatives has helped elect major political figures,¹ while simultaneously undermining journalism, open discourse, and the so-called ‘marketplace of ideas’.² In their stead, researchers note the rise of radicalized closed communities, frequently coalescing around extreme positions and disinformation peddled by highly-targeted ad campaigns on social platforms.³ On a more individual level, targeted advertising has been demonstrated to subtly alter individuals’ self-perception, and therefore nudge their views and behaviour.⁴

Whereas many of its critics challenge aggressive targeted advertising on normative grounds, it is becoming increasingly apparent that the advertising technology (adtech) industry may also run afoul of the prescriptions of positive law. To this end, this report analyses the legal ramifications of behavioural targeting practices from the perspective of European Union (EU) data protection law. In particular, relevant legal sources include EU primary law (such as the Charter of Fundamental Rights⁵), EU secondary law (via Union regulations and directives), and EU supplementary law (particularly the case law of the Court of Justice of

1 Wong, J. (2018), “‘It might work too well’: the dark art of political advertising online”, *The Guardian*, [<https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy>]. All URLs referenced in this paper were last accessed 10 November 2021, unless indicated otherwise.

2 Anderson, J. and Rainie, L. (2020), ‘Concerns about democracy in the digital age’, *Pew Research Center*, [<https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/>].

3 Ibid. See too Nadler, A., Crain, M., and Donovan, J. (2018), ‘Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech’, *Data & Society Research Institute, Inc.*, [https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf]; Gary, J. and Soltani, A. (2019), ‘First Things First: Online Advertising Practices and Their Effects on Platform Speech’, *Knight First Amendment Institute* at Columbia University, [<https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech>].

4 Summers, C.A., Smith, R.W., and Reczek, R.W. (2016), ‘An Audience of One: Behaviorally Targeted Ads as Implied Social Labels’, *Journal of Consumer Research*, vol. 43, no. 1, p. 157.

5 Charter of Fundamental Rights of the European Union, 2016, O.J. C 202/389.

the European Union [CJEU]).⁶ Jurisprudence by national courts and decisions by Member States' Data Protection Agencies (DPAs), while not binding on a Union level, may serve as informative sources for legal interpretation of Union law. The non-binding opinion of advisory bodies such as the European Data Protection Board (EDPB) and its predecessor, the Article 29 Working Party (A29WP), are likewise consulted, since they shape Union law by means of authoritative guidance and norm-setting.

Following this introduction, Chapter 2 discusses precisely how behavioural targeting works from a technical point of view, with special attention being paid to the underlying technology of 'Real-Time Bidding' (RTB).

Chapter 3 then undertakes a *lex lata* consideration of the EU General Data Protection Regulation (GDPR).⁷ This chapter represents the main thrust of the report and discusses the most salient points of tension between behavioural targeting technologies and the GDPR: legal scope, concepts of data controllership, legal basis requirements, consent requirements, processing of special categories of personal data, security requirements, and finally transparency issues.

Finally, Chapter 4 summarizes the main points raised during the course of the report and looks towards the future. It recapitulates the current state of online behavioural tracking and advertising practices, describes the challenges posed to data protection, and evaluates the prospects of some upcoming legislative and technical developments in safeguarding personal data. The report's final remarks concern the possibility or desirability of returning to a de-personalized model of online advertising.

⁶ Publications Office of the European Union (2020), 'Sources of European Union law', [<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A114534>].

⁷ 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'), 2016, O.J. L 119/1; hereafter: GDPR.

2 An Overview of Adtech

Advertising, defined as ‘a paid form of non-personal presentation of ideas, goods, or services’⁸ is not a recent invention. While advertising itself has been conducted for millennia, online advertisements merely date back to 1978, when Gary Thuerk of DEC sent the world’s first mass spam email via ARPANET.⁹ It was a broad and brutish approach to marketing, with the entirety of ARPANET’s userbase on the US West Coast targeted based on their geographical location.

Since then, the digital ad industry has grown dramatically. As of 2020, online ads now account for more than half of the ad industry’s total expenses, inexorably pushing back traditional media.¹⁰ Not only are there many digital adverts, there are many *forms* of digital adverts. By nature, they may be visual (e.g., images or text), auditory (e.g., sound clips), or audio-visual (e.g., multimedia videos). By location, digital ads are most commonly encountered as webpage ads or in-app ads, although modern digital ads may be delivered through anything from smart billboards to robotic assistants.¹¹ For the sake of brevity, this report focuses chiefly on the case of digital adverts placed in webpages, although the legal ramifications of tracking and sharing user data should be comparable regardless of the advertising medium.

Digital advertising’s dominant position would not have been achieved without several underlying technological developments: contextual advertising, programmatic advertising and real-time bidding, and behavioural tracking and targeting technologies. Each of these are introduced and explained in the following sections, so as to enable a legal analysis of their ramifications.

8 Leader, W.G. and Kyritsis (1994), N., *Fundamentals of Marketing*, Nelson Thornes, p. 195.

9 Freitas, S. and Levene, M. (2005), ‘Spam’, in Ghaoui, C. (ed.), *Encyclopedia of Human Computer Interaction*, IGI Global, 2005.

10 Barker, A. (2020), ‘Digital ad market set to eclipse traditional media for first time’, *Financial Times*, [<https://www.ft.com/content/d8aaf886-d1f0-40fb-abff-2945629b68c0>].

11 Germain, T. (2019), ‘Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads.’, *Consumer Reports*, [<https://www.consumerreports.org/privacy/digital-billboards-are-tracking-you-and-they-want-you-to-see-their-ads/>]; Lombard, M. and Snyder-Duch, J. (2017), ‘Digital Advertising in a New Age: The Power of (Tele)Presence’, in Rodgers, S. and Thorson, E. (eds.), *Digital Advertising: Theory and Research*, Routledge, p. 179.

2.1 Contextual Advertising

Contextual advertising deals with the suitable matching of displayed ads with the digital space that houses said ads. Indeed, its distinguishing feature is that contextual advertising concerns itself solely with analysing a user's online environment rather than with analysing the individual user.¹²

This approach to digital marketing is a reflection of traditional print and television advertising that sought to pair, for example, sports equipment ads with news and coverage of sports events. Such a pairing might occur by specifically picking out the sports section of a general newspaper or TV broadcast, or by matching the ad with a sports magazine or TV channel that is wholly dedicated to that single topic. The natural expectation behind this is that an audience would be much more likely to buy items that correspond to its apparent interests.

Early online contextual advertising usually involved three actors: a website operator, a sales channel operator (which might either be an ad sales team within the website operator or a separately contracted advertising network), and an advertiser to whom adspace was marketed and sold.¹³ Mellet and Beauvisage note that this earlier model of contextual advertising is 'large-grained', meaning that it operates with large and broadly defined audience segments and is based around broadly defined topics rather than specific keywords.¹⁴

Modern advancements in contextual advertising have relied on machine learning and artificial intelligence¹⁵ to provide greater granularity. Algorithms are now capable of analysing the text, language, link structure, and page structure¹⁶ of each individual page in what is sometimes termed 'full-path URL content

12 Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 117.

13 Ibid., p. 117.

14 Ibid., p. 117.

15 Artificial intelligence refers to the ability of machines and programs to solve problems in a manner that humans would consider rational or creative. Machine learning, on the other hand, has been defined by Bygrave (2021) as 'AI [that] involves programming computers to optimise performance (based on defined models) using example/sample data, and where the basic task involves drawing inferences from the samples'. Bygrave identifies ML system deployments as being preceded by a training phase and a validation phase. References: Bell, L. (2016), 'Machine learning versus AI: what's the difference?', *Wired*, [<https://www.wired.co.uk/article/machine-learning-ai-explained>]; Bygrave, L.A. (2021), 'Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions', in Ienca, M. et al. (eds.), *Cambridge Handbook of Life Sciences, Information Technology and Human Rights*, (forthcoming).

16 Google, 'About Contextual Targeting', [<https://support.google.com/google-ads/answer/2404186>].

categorization'.¹⁷ Novel computer vision technologies are also being leveraged, so as to use even the images and videos in a webpage to display the most relevant advertisement to the viewer.¹⁸

This greater granularity and specificity in modern online advertising would be impossible to exploit if firms still relied on the slow, traditional method of personally negotiating ad campaigns well in advance. Instead, adspace is now frequently allocated on-the-spot in what is known as programmatic advertisement, via a technology termed Real-Time Bidding.

2.2 Programmatic Advertising and Real-time Bidding

The Interactive Advertising Bureau (IAB) defines programmatic buying as 'media or ad buying that uses technology to automate and optimize, in real time, the ad buying process'.¹⁹ Programmatic advertising is thereby a technological approach that may be combined with other forms of advertising, such as the previously discussed contextual advertising or with behavioural targeting.

There are currently four major varieties of programmatic advertisement being utilized, differentiated based on the type of ads inventory being transacted and the price-setting mechanism. These varieties are:

- **Programmatic Direct** transactions, which are most closely aligned to the traditional, pre-arranged sale of ad impressions between an adspace seller and an adspace buyer. In other words, both the price and the advertiser have been established well in advance of the actual ad delivery. Programmatic direct transactions are programmatic only insofar as the adspace buyer uses automation to elicit bids from sellers and to consequently conduct the agreed-upon ad campaign. There is no negotiation process between buyer and seller.²⁰
- **Unreserved Fixed Rate** transactions, wherein adspace is reserved at a pre-arranged fixed price for an advertiser. In these so-called 'first look

17 Zvelo (2014), 'Full Path URL Content Classification', [<https://zvelo.com/content-classification-full-path-url-superiority/>].

18 Gungum, 'How we Process Images', [<http://view.ceros.com/gumgum/howweprocessimages/p/1>].

19 IAB, 'Glossary of Terminology', [<https://www.iab.com/insights/glossary-of-terminology/>].

20 IAB, 'Programmatic and Automation – The Publishers' Perspective', [https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf]; Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 84.

contracts', an advertiser pays an initial 'option price' to establish a desired price floor relating to an advertisement they wish to run in the future. They may then invoke and pay the fixed price, or refuse to do so, forfeit their initial 'option price' payment, and let the advertisement proceed to auction with other bidders.²¹

- **Invitation-Only Auctions**, wherein ad inventories are auctioned off between a closed list of invited advertisers.²²
- **Real-time Bidding**, wherein a complex ecosystem of advertisers, publishers, ad networks, ad exchanges, and individual end users are involved in the real-time sale and display of adverts on a per-impression basis following open auctions.²³

This report conducts its analysis chiefly on RTB, since its open nature and multiple stakeholders create the most friction with user privacy and standards of data protection.

2.2.1 Real-time Bidding: A Step-by-Step Explanation

The easiest way to understand the intricacies of the RTB process is through an illustrative example. This report's example is heavily based upon the RTB process' description in Wang et al.,²⁴ although it has been expanded therefrom to include additional information not found in the original description.

2.2.2 Step 1

A user, John Smith, uses his browser to visit a webpage that contains ad units (i.e., adspace for an impression). The webpage's operator is known as the **publisher**. While the webpage loads, its code collects data regarding the visitor and creates an ad request.²⁵

This code is usually structured in compliance with one of the two dominant **RTB protocols** that define the format and contents of all ad requests: the Interactive Advertising Bureau's OpenRTB (currently in version 3.0) or Google's proprietary 'Authorized Buyers' protocol.²⁶ Each protocol specifies a list of objects (e.g., device/user/publisher) and establishes a list of possible attributes for each

21 Wang et al., *ibid.*, p. 86.

22 IAB, 'Programmatic and Automation – The Publishers' Perspective', [https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf], p. 3.

23 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 10.

24 *Ibid.*, p. 13.

25 *Ibid.*, p. 13.

26 Google, 'Real-Time Bidding', [<https://developers.google.com/authorized-buyers/rtb/start>].

object (e.g., a user's gender or age, or a website's keywords or domain name).²⁷ In essence, the protocols define the information that advertisers and publishers can technically know about the user during the open auction.

Alongside the various first-, third-, and even 'fourth-party'²⁸ trackers on a webpage that immediately begin scraping the visiting user's information (via methods outlined in Section 2.3), many websites have begun to also employ **consent management platforms** (CMPs). These suites are deployed to ask or secure a user's consent to being tracked, so that tracking may lawfully proceed.

2.2.3 Step 2

The ad request usually travels through a **supply-side platform** (SSP) to reach an **ad network** (ADN) or an **ad exchange** (ADX).²⁹ Supply-side platforms are the tools that publishers employ to manage their own ad inventories and to send separate ad requests for each ad slot.³⁰ An SSP is an automated software suite that seeks to generate maximum revenue for the publisher by courting as many bids as possible, so as to settle on the highest one. To achieve this, it queries ad networks and ad exchanges, either consecutively (in the traditional method known as the 'waterfall sequence') or simultaneously (via a comparatively newer technique known as 'header bidding').³¹

Ad networks are intermediaries that match publishers' adspace inventories with the campaign criteria of partnered advertisers. Many ad networks are specialized in certain types of inventories or audiences. However, due to ad networks acting as intermediaries, ad publishers are unaware of who buys their ad space while advertisers are not fully aware of who serves their ads.³²

Ad exchanges are platforms that act as open marketplaces, agglomerating multiple ad networks and including every other actor in the RTB ecosystem with the goal of creating a centralized ad trading hub with a greater variety of offerings

27 Google, 'OpenRTB Integration', [<https://developers.google.com/authorized-buyers/rtb/open-rtb-guide/>].

28 T. Urban et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the World Wide Web Conference*, p. 1279.

29 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

30 Ibid., p. 121.

31 Ahamed, R. (2020), 'What is Header Bidding & How it Works', *automatad*, [<https://headerbidding.co/header-bidding/>].

32 Kostiuk, I. (2020), 'Ad Network vs. Ad Exchange – Programmatic Business Model', *Admixer*, [<https://blog.admixer.com/ad-network-vs-ad-exchange/>].

and a greater transparency than that afforded by any single ad network and publisher inventory.³³

2.2.4 Step 3

The ad exchange, having received the ad request, sends bid requests for John Smith's impression to advertisers' **demand-side platforms** (DSPs).³⁴ Demand-side platforms are the buyer-side (i.e., advertiser-side) counterpart to SSPs, seeking to manage advertisers' ad campaigns and secure them the most appropriate ad placements for the lowest possible price. These software suites receive first-party user data from the publisher's ad request and decide whether the adspace on offer matches any of the advertisers' ongoing campaigns. A DSP usually presents advertisers with a list of exchanges or SSPs that the advertiser is automatically opted into, leading to adspace purchases that advertisers may not even 'know or care about'.³⁵ However, an advertiser may be excluded from an otherwise open auction if a publisher has employed a blocklist and/or set minimum prices in relation to its adspace.³⁶

2.2.5 Step 4

The DSP queries **data management platforms** (DMPs) to obtain any additional third-party data regarding the user 'John Smith',³⁷ thereby enriching his user profile and making his ad impression more valuable to certain advertisers who can appeal to his needs or desires. The format of this data and the manner of tracking John Smith online is discussed in Section 2.3.

Data management platforms (also known as data exchanges or data brokers) are services that collect and sell user data, as well as analytics based upon said user data.³⁸ DMP-derived insights are most immediately relevant to advertisers wishing to maximize the value of their delivered ad impressions, making them natural interface points for advertisers' DSPs.

However, the data-driven RTB ecosystem is reliant on the free flow of user information, needing users like John Smith to be recognizable by advertisers regardless of which publisher currently auctions off John Smith's impression. There-

33 Ibid.

34 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

35 IAB, 'Programmatic and Automation – The Publishers' Perspective', [https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf], p. 3.

36 Ibid., p. 3.

37 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

38 Ibid., p. 10.

fore, DMPs interface with *both* DSPs and SSPs, while DSPs and SSPs *also* interface with each other. In conducting such a *sync*,³⁹ both the user IDs and the actual user data is synchronized between platforms.

2.2.6 Step 5

Each advertiser's DSP processes all available information relevant to the bid request and determines whether to submit a bid for John Smith's impression.⁴⁰

2.2.7 Step 6

All bids are compared and the winning bid is selected. The bid's price is determined via 'second price auction', wherein the winning bid pays \$0.01 more than the second-highest bid, regardless of what the winning bidder actually pledged.⁴¹

2.2.8 Step 7

The advertiser is notified of their winning bid.⁴²

2.2.9 Step 8

The winning advertiser's ad is displayed on John Smith's webpage.⁴³ The time between Step 1 and Step 8 is usually less than 100 milliseconds.⁴⁴

2.2.10 Step 9

Additional data is collected regarding John Smith's reaction to seeing the ad, checking whether the impression achieved clickthrough or even conversion.⁴⁵

2.2.11 Summary

This 9-step process summarizes the basic modality of real-time bidding. While its broad outline is valid for all auctions, particular auctions may diverge in their specific mechanisms.

39 Ryan, J. (2018), 'Report from Dr Johnny Ryan – Behavioural advertising and personal data', *Brave*, [<https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf>], p. 5.

40 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

41 *Ibid.*, p. 21.

42 *Ibid.*, p. 13.

43 *Ibid.*, p. 13.

44 Olejnik, L. and Castelluccia, C. (2014), 'To bid or not to bid? Measuring the value of privacy in RTB', [<https://lukaszolejnik.com/rtb2.pdf>], p. 4.

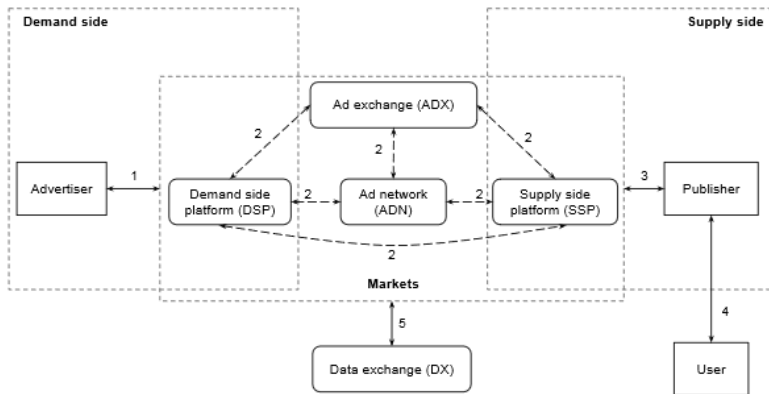
45 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

For example, an auction may use a protocol other than OpenRTB or Authorized Buyers, either as a complement or as a complete replacement.⁴⁶ If a bid request was sent to multiple ad exchanges simultaneously (such as via header bidding), then the winning bid is decided within the SSP rather than the ad exchange itself.⁴⁷

Furthermore, SSPs and DSPs may be operated by the same firm, leading to direct integration rather than interfacing.⁴⁸ Indeed, certain large companies such as Google offer products to both the demand side and the supply side of the RTB marketplace, complicating their role in the ecosystem.⁴⁹

Notably, the bidding for a certain impression may involve more than one consecutive successful auction. Since impressions may be resold after being won and since bidders in an auction may be ad exchanges themselves, it is possible to create a transactional chain that obfuscates the source of an advertisement that reaches a publisher.⁵⁰ This is noted as a potential source for fraud in the RTB ecosystem.⁵¹

This section concludes with an illustrative diagram of the RTB ecosystem from Wang et al.:⁵²



46 ICO (2019), *Update report into adtech and real time bidding*, [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-d1191220.pdf>], p. 14.

47 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 13.

48 Vivier, R. (2018), 'Curious to understand how the programmatic advertising ecosystem (DSP, SSP, DMP) works in detail?', *Digital Thought*, [<https://digitalthought.me/articles/digital-marketing/Programmatic-ad-bidding-cookie-sync.html>].

49 Bashir, M.A. (2019), *On the Privacy Implications of Real Time Bidding*, Ph.D. diss., Northeastern University, p. 15.

50 Ibid., p. 15.

51 Ibid., p. 15.

52 Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, p. 11.

2.3 Online Tracking

2.3.1 Methods of Online Tracking

As has been established, the digital advertising industry relies on extensive profiling data to match the most appropriate advertisement to each user. This practice is termed ‘behavioural targeting’ and is defined by the IAB as ‘using previous online user activity (e.g., pages visited, content viewed, searches, clicks and purchases) to generate a segment which is used to match advertising creative to users’.⁵³

In reality, there are myriad ways to accomplish this tracking. Even just examining the modalities that rely on in-browser trackers reveals more than 30 distinguished approaches, more than enough to warrant a dedicated monograph (or several).⁵⁴ This is compounded by many alternative tracking methods that occur entirely outside the user’s web browser, such as using mobile and IoT devices’ embedded sensors to log user data,⁵⁵ utilizing physical proximity trackers such as Bluetooth,⁵⁶ or even measuring user emotions via facial recognition.⁵⁷

This report’s scope is restricted to six of the most commonly used tools for in-browser tracking.

2.3.2 Stateful Tracking

Stateful tracking is so named because it involves saving an information ‘state’ containing identifiers of the tracker’s choosing directly on the end user’s machine.⁵⁸ Two major stateful tracking methods involve the use of Cookies and Entity Tags (Etags), which represent storage-based and cache-based tracking technologies, respectively.⁵⁹

53 IAB, ‘Glossary of Terminology’, [<https://www.iab.com/insights/glossary-of-terminology/>].

54 Bujlow, T. et al. (2017), ‘A Survey on Web Tracking: Mechanisms, Implications, and Defenses’, *Proceedings of the IEEE*, vol. 195, no. 8, p. 1480.

55 Bashir, M.A. (2019), *On the Privacy Implications of Real Time Bidding*, Ph.D. diss., Northeastern University, p. 20.

56 Korolova, A. and Sharma, V. (2018), ‘Cross-App Tracking via Nearby Bluetooth Devices’, *CODASPY’18*.

57 Davis, P. (2020), ‘Facial Detection and Smart Billboards: Analysing the “Identified” Criterion of Personal Data in the GDPR’, *European Data Protection Law Review*, vol. 6, no. 3, p. 365; George, D., Reutimann, K. and Tamò-Larrieux, A. (2019), ‘GDPR bypass by design? Transient processing of data under the GDPR’, *International Data Privacy Law*, vol. 9, no. 4, p. 286.

58 Karaj, A. et al. (2019), ‘WhoTracks.Me: Shedding light on the opaque world of online tracking’, [<https://arxiv.org/abs/1804.08959>], p. 3.

59 T. Bujlow et al. (2015), ‘Web Tracking: Mechanisms, Implications, and Defenses’, p. 3.

2.3.3 Cookies and Storage Trackers

Cookies are split into two main types depending on who they were placed by: first-party cookies, stored by the domain that the user directly visits, and third-party cookies, stored by any domain other than the first-party domain, which the client browser has sent requests to.⁶⁰ The former constitute the originally intended usage scenario for cookies, while the latter, in the view of the cookie specification's authors, constitute 'a considerable threat to privacy' that they endeavoured to reign in.⁶¹ Presently, many online domains are linked to matryoshka doll-like cookie deployments, prompting certain researchers to distinguish 'fourth-party' cookies and beyond as separate categories.⁶² In this taxonomy, the visited website remains the first party, its directly embedded partners constitute the third party, the direct partners of the third parties are the fourth parties, and so forth into perpetuity. The deepest-set cookie discovered in a study by Urban et al. was an eighth-party cookie.⁶³

Cookies are also differentiated according to their parent technology, being either HTTP cookies (the most widespread form of cookies), Adobe Flash cookies (technically called 'Local Storage Objects' or LSOs), HTML5 cookies (mainly coming in the form of HTML5 Local Storage objects), and a number of other, less-prominent varieties.⁶⁴ These cookie varieties are distinguished based on parameters such as maximum size (HTTP = 4 KB, Flash = 100 KB, HTML5 Local = 5 MB), longevity/expiration time (HTTP = variable, Flash/HTML5 = indefinite until cleared), and potential for cross-session and cross-browser tracking (e.g. Flash cookies are able to track users across different browsers).⁶⁵

Presently, cookie use is incredibly prevalent among webpages – a 2020 study by Urban et al. found that out of a sample of 1.5 million websites, landing pages stored an average of 55 cookies each, while subsites stored an average of 78 cookies, with 99% of all observed cookies being used for tracking users or providing ads.⁶⁶

60 Krishnamurthy, B. and Wills, C.E. (2009), 'Privacy Diffusion on the Web: A Longitudinal Perspective', *Proceedings of the '09 World Wide Web Conference*, p. 542.

61 Kristol, D. (2001), 'HTTP Cookies: Standards, Privacy, and Politics', *ACM Transactions on Internet Technology*, vol. 1, no. 2, p. 159.

62 Urban, T. et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the '20 World Wide Web Conference*, p. 1279.

63 Ibid., p. 1283.

64 Buijlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, p. 1484.

65 Ibid., p. 1484.

66 Urban, T. et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the '20 World Wide Web Conference*, p. 1280.

Cookies, by definition, are expected to contain a simple name-value data pair in plaintext format, strictly limited in size and therefore in complexity.⁶⁷ Advertisers and data brokers circumvent this limitation through several means, so as to record greater amounts of sophisticated data and to avoid their tracking cookies being detected.

Firstly, many trackers use arbitrarily complex encoding schemas to write and read data-heavy cookie values.⁶⁸ What this means in practice is that instead of a cookie containing a value of '123ab', it may contain the following:⁶⁹

```
''253024271.1453122666.239.16.utmcscr=host.com/sea/|  
utmccn=(10.0.0.5)|utmcmd=org|utmctr=ail@host.com|''
```

Gonzalez et al. identify within the above value such elements as a Unix timestamp, an email address, and an IP address.⁷⁰

Secondly, additional data exceeding the cookie's size limit, such as a user's detailed interest categories, are stored server-side by the data tracker and linked to the cookie's unique identifier.⁷¹

Furthermore, many trackers specifically endeavour to shield their cookies from detection and tampering. They do so by secreting a user's unique identifier across multiple cookies⁷² or using complex formats such as JSON to encode multiple values in a single cookie.⁷³ Another noted practice is writing values directly into a cookie's name field, resulting in thousands of differently named cookies being issued by a single organization and making it exceedingly difficult to manage said cookies by their name alone.⁷⁴

To ensure cookie longevity and safeguard against possible deletion, many trackers employ what are known as 'evercookies' or 'zombie cookies'. This technique

67 Ibid., p. 1278.

68 Gonzalez, R. et al. (2017), 'The cookie recipe: Untangling the use of cookies in the wild', *Proceedings of the 1st Network Traffic Measurement and Analysis Conference*, p. 6.

69 Ibid., p. 6.

70 Ibid., p. 6.

71 Urban, T. et al. (2018), 'The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR', [<https://arxiv.org/abs/1811.08660>], p. 4.

72 Bujlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, p. 1482.

73 Gonzalez, R. et al. (2017), 'The cookie recipe: Untangling the use of cookies in the wild', *Proceedings of the 1st Network Traffic Measurement and Analysis Conference*, p. 5.

74 Ibid., p. 4.

involves copying a cookie's contents to multiple different storages and formats, e.g., transcribing an HTTP cookie into a Flash cookie, an HTML5 cookie, a web cache object, or even in the RGB values of specially-generated PNG images.⁷⁵ When the cookie is deleted from one instance where the user might expect to find it, it is immediately reconstructed and revived using any of its other copies. Zombie cookies might be bolstered by non-cookie technologies as well, such as when using Etags to respawn themselves.⁷⁶ Much like their namesake, zombie cookies are also virulent and can easily spread between a user's browsers due to the persistent nature of some of their storage formats, such as Flash.⁷⁷

Perhaps the most powerful tool cookie trackers have at their disposal, however, is the syncing first mentioned in Section 2.2. Browsers by default operate under a 'same-origin policy' that prevents one page from accessing a second page's data unless both pages share the same origin.⁷⁸ In practical terms, this means that a server may only access a cookie under the domain that set it, forbidding separate third parties from accessing each-other's cookies.⁷⁹ Cookie synchronization allows trackers to bypass this limitation by corresponding with each other via HTTP redirects and unifying their disparate profiles of a single individual into one large identity.⁸⁰ Researchers variously refer to this technique as 'bypassing' or outright 'violating' the same origin policy.⁸¹

In addition, several levy criticisms against cookie synchronization, since it tends to leak various categories of personal data (such as such location/gender/age/email) while it bypasses the same-origin policy.⁸² The same researchers have also demonstrated how cookie synchronization is capable of re-identifying a user

75 Bujlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, p. 1492.

76 Avenson, M.D. et al. (2011), 'Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning', [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390], p. 14; Etags are discussed in Section 2.3.5.

77 Kamkar, S. (2010), 'evercookie', [<https://samy.pl/evercookie/>].

78 'Origin' in this case denotes a combination between protocol, domain/subdomain, and port.

79 Urban, T. et al. (2018), 'The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR', [<https://arxiv.org/abs/1811.08660>], p. 4.

80 Ibid., p. 4.

81 Papadopoulos, P., Kourtellis, N., and Markatos, E. (2018), 'Exclusive: How the (synced) Cookie Monster breached my encrypted VPN session', *Proceedings of the 11th European Workshop on Systems Security*, p. 2; Papadopoulos, P., Kourtellis, N., and Markatos, E. (2019), 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask', *Proceedings of the '19 World Wide Web Conference*, p. 1438.

82 Papadopoulos, P., Kourtellis, N., and Markatos, E. (2019), 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask', *Proceedings of the '19 World Wide Web Conference*, p. 1439.

behind VPN or TOR protections⁸³ and how cookie synchronization might bolster technologies like zombie cookies. In the latter case, a user might delete their entire cookie storage, but if even a single tracker from a cookie-synchronized network manages to respawn their cookie, then the entire network may re-establish their previously deleted user profiles despite the profiles' prior erasure.⁸⁴ As to the spread of cookie synchronization, Papadopoulos et al. find that out of a dataset of 850 mobile users, 97% of those who submit more than 10 connection requests per day (i.e. regular internet users) were exposed to cookie synchronization.⁸⁵ Engelhardt and Narayanan demonstrate that 85 of the top 100 third parties are engaged in cookie synchronization.⁸⁶

Cookies, for all their versatility, are somewhat limited in usefulness in mobile devices compared to their desktop counterparts. Mobile web browsing is predominantly done in-app rather than via dedicated mobile browsing software,⁸⁷ yet mobile apps run their internet sessions in a sandbox 'Webview' that prevents cookies from being accessed by other apps.⁸⁸ As a consequence, mobile web tracking relies mostly on stateless tracking modalities that are discussed in Sections 2.3.6-2.3.8. Rarely, HTML5 local storage cookies may be used for tracking purposes, though this is disruptive to the user experience and generally avoided.⁸⁹

Companies that place third party cookies usually seek to deploy them in as many websites as possible, so as to ensure a broad and robust web of surveillance. The most successful of these companies are tech giants such as Google and Facebook, who are able to track users across the vast majority of popular websites.⁹⁰

83 Papadopoulos, P., Kourtellis, N., and Markatos, E. (2018), 'Exclusive: How the (synced) Cookie Monster breached my encrypted VPN session', *Proceedings of the 11th European Workshop on Systems Security*, p. 5.

84 Papadopoulos, P., Kourtellis, N., and Markatos, E. (2019), 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask', *Proceedings of the '19 World Wide Web Conference*, p. 1434.

85 Ibid., p. 1437.

86 Engelhardt, S. and Narayanan, A. (2016), 'Online Tracking: A 1-million-site Measurement and Analysis', Princeton University, [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf], p. 11.

87 Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 123.

88 IAB (2013), 'Cookies on Mobile 101', [<https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>], p. 6.

89 Ibid., p. 6.

90 Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 121.

Due to their universal exploitation and myriad privacy concerns, cookies have long been the subject of public policy debate. Presently, the largest browsers either forbid third-party cookies (e.g., Firefox and Safari) or are preparing to phase them out (e.g., Chrome).⁹¹

2.3.4 Cookie Successors – FLoC and FLEDGE

In this section, it is pertinent to introduce two proposed substitutes for traditional cookies – Google’s Federated Learning of Cohorts (FLoC) and First ‘Locally-Executed Decision over Groups’ Experiment (FLEDGE) initiatives.⁹²

FLoC technology relies on machine learning to assign shared IDs to large groups of users based on their similar browsing histories. More specifically, a machine learning algorithm creates an abstract, multidimensional mathematical space that represents all possible web browsing histories. A SimHash function is used by each browser to appraise a user’s recent browsing history and assign it an ID that corresponds to an area within the mathematical model. While individual browsing histories are unique, the assigned IDs are not – the IDs are, instead, shared between thousands of users based on the close similarity of their browsing history, as revealed by the SimHash function. It is this shared ID that unites individual users into the Cohorts of FLoC.⁹³

In FLoC, the processing of a user’s browser history is carried out client-side by their own browser. The information directly transmitted to advertisers by a FLoC-enabled browser is merely the resultant Cohort ID, where the intent is to provide individuals with anonymity via aggregation of their data.

Separately, advertisers and publishers continue to collect behavioural data such as entered search terms and other on-site activity, but Google’s intent is for trackers to only be able to link that data to a group of browsers’ shared Cohort ID rather than to individual users. Therefore, an RTB auction under the FLoC model has as its inputs the Cohort ID of a browser and the collected behavioural data regarding that particular cohort, which together lead to the selection of an appropriate ad to display.⁹⁴

91 IAB (2020), ‘A Guide to the Post Third-Party Cookie Era’, [https://designrr.s3.amazonaws.com/mardare_at_iabeurope.eu_80924/_5449.pdf], p. 3.

92 Web Incubator CG, ‘floc’, *GitHub repository*, [<https://github.com/WICG/floc>]; Web Incubator CG, ‘turtledove’, *GitHub repository*, [<https://github.com/WICG/turtledove/blob/main/FLEDGE.md>].

93 Dutton, S. (2021), ‘What is FLoC?’, Google, [<https://web.dev/floc/>].

94 Ibid.

Google's current FLoC design anticipates minimum cohort sizes in the thousands of users and intends to merge smaller cohorts until a sufficient size for each cohort is achieved. The cohorts themselves are to be recalculated roughly every seven days.⁹⁵

FLoC technology is still under development but, as of March 2021, has been undergoing trials by Google via its Chrome browser.⁹⁶ These trials have so far not been held in countries where the GDPR and the ePrivacy Directive are in effect due to a variety of concerns regarding their compatibility with EU data protection law.⁹⁷

FLoC technology still has certain purely technical failings that need to be addressed over the course of its development, such as leaking whether users are in incognito mode or generating cohorts based on as little as 3 visited websites, thereby making it possible for a malicious actor to accurately predict the browsing behaviour of anyone in such a cohort.⁹⁸

Alongside FLoC, Google is poised to trial a complementary project called FLEDGE later in 2021.⁹⁹ Whereas FLoC's cohorts are generated outside of the control of actors such as DSPs, advertisers, and publishers, FLEDGE is intended to allow these actors to create their own 'interest groups' of users and carry out retargeting and other behavioural advertising based on on-site actions. The privacy-enhancing caveat is that interest group membership would be stored locally, not leaving a user's browser. Auctions for impressions would likewise be held entirely in-browser.

95 Olejnik, L. (2021), 'Initial privacy analysis of Google's Privacy Sandbox - Federated Learning of Cohorts leaking information about browsing in incognito mode', *Security, Privacy, and Tech Inquiries* [web blog], [<https://blog.lukaszolejnik.com/privacy-analysis-of-googles-privacy-sandbox-federated-learning-of-cohorts-leaking-information-about-browsing-in-incognito-mode/>].

96 Temkin, D. (2021), 'Charting a course towards a more privacy-first web', *Google Ads & Commerce Blog*, [<https://www.blog.google/products/ads-commerce/a-more-privacy-first-web/>].

97 Schiff, A. (2021), 'Google Will Not Run FLoC Origin Tests In Europe Due To GDPR Concerns (At Least For Now)', *AdExchanger*, [<https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/>].

98 Olejnik, L. (2021), 'Initial privacy analysis of Google's Privacy Sandbox - Federated Learning of Cohorts leaking information about browsing in incognito mode', *Security, Privacy, and Tech Inquiries* [web blog], [<https://blog.lukaszolejnik.com/privacy-analysis-of-googles-privacy-sandbox-federated-learning-of-cohorts-leaking-information-about-browsing-in-incognito-mode/>];

Olejnik, L. (2021), 'Privacy of Google's Privacy Sandbox 2 - Federated Learning of Cohorts leaking user's visited websites?', *Security, Privacy, and Tech Inquiries* [web blog], [<https://blog.lukaszolejnik.com/privacy-of-google-privacy-sandbox-floc-leaking-visited-website-history/>].

99 Web Incubator CG, 'turtledove', *GitHub repository*, [<https://github.com/WICG/turtledove/blob/main/FLEDGE.md>].

FLEDGE begins with the creation of an interest group by an owner – a publisher, advertiser, or DSP. These interest groups may be as general or brand-specific as their creators desire. Furthermore, an interest group’s owner may delegate certain membership operations (such as adding new users to the interest group) to a third party, such as an SSP.¹⁰⁰

When a user visits a site, their on-site behaviour may lead to them being added to one or more interest groups by the owners or operators of these interest groups. The actual act of being added to an interest group entails the transmission of an interest group’s information to a browser, which the browser records locally. Alongside its membership in interest groups, the browser is also tasked with storing the business logic that will be used to conduct ad auctions.¹⁰¹

At a later date, when the same browser visits a web page with ad space, an auction is carried out within the device itself to select the most appropriate ad. The winning ad is displayed in a ‘Fenced Frame HTML Component’ that isolates the ad impression from the rest of the publisher’s page. This prevents the publisher from learning about the user’s interest groups and viewed ads, while also preventing the ad sellers and buyers from retrieving user information from the publisher’s site.¹⁰²

Since running a bid auction entirely within the browser may prove resource-intensive and impact performance for the user, FLEDGE compromises on its principle to conduct auctions entirely in a local manner by offloading part of the processing duties to ‘trusted key-value-type servers’.¹⁰³ Such a server would be characterized, at minimum by a lack of event-level logging, so that sensitive information sent by a browser (such as the set of all interest groups it has joined) does not leak out. However, the precise criteria that make a server ‘trusted’ is yet to be defined by Google, which anticipates ‘robust discussions’ on the topic in 2021.¹⁰⁴

Indeed, FLEDGE is currently further away from implementation than FLoC and many of its technical underpinnings are yet to be revealed to the public. Nevertheless, a baseline understanding of the technology’s intent is helpful

100 Ibid.

101 Underwood, C. and Watson, C. (2021), ‘Birdwatching for Marketers: What Google’s FLoC & FLEDGE Mean for You’, *Search Discovery*, [<https://www.searchdiscovery.com/blog/floc-and-fledge-clarity-for-marketing/>].

102 Ibid.

103 Web Incubator CG, ‘turtledove’, *GitHub repository*, [<https://github.com/WICG/turtledove/blob/main/FLEDGE.md>].

104 Ibid.

when gauging the future course of adtech and anticipating how that course may interface with data protection law.

2.3.5 Etags and Cached Trackers

Whereas tracking cookies are data files kept in explicitly-designated storage spaces, Etags are HTTP headers that reside in a browser's web cache.¹⁰⁵ When a user visits a webpage, the publisher or their partners may assign objects within the webpage a unique Etag identifier. These objects may then be cached by the user's browser. When the user revisits the publisher or their partners, the objects in the web cache are retrieved and their Etag identifiers are used to identify the returning user.¹⁰⁶ An advantage of Etag tracking is that, since the web cache is stored separately from any cookies, Etag identifiers are able to function despite cookie deletion or cookie blocking. Such identifiers are only removed when the browser's cache is purged.

While Etags are the most readily used form of cache-based user tracking, it is worth noting that there exist many similar approaches. Last-modified HTTP headers are a closely-related alternative to Etag tracking.¹⁰⁷ It is also possible to look past the web cache entirely and instead track users through DNS and operational caches.¹⁰⁸

It has also been observed how the HTTP Strict Transport Security (HSTS) specification may be abused to create resilient, cached 'supercookies' by having a server transfer a collection of benign files to users. Some of these files will be marked by the server as requiring an HSTS reply, while others will be marked with regular HTTP requests. When a user reconnects to the server, he may be identified and tracked according to the unique pattern of HSTS and HTTP requests sent by his files.¹⁰⁹

2.3.6 Stateless Tracking

Unlike stateful tracking, which relies on saving state data to a user's system, stateless tracking relies on server-side tracking of browser APIs and network

105 Bujlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, p. 1485.

106 Ibid., p. 1485.

107 Ibid., p. 1485.

108 Ibid., p. 1485.

109 Stockley, M. (2015), 'Anatomy of a browser dilemma – how HSTS 'supercookies' make you choose between privacy or security', *Sophos*, [<https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/>].

information.¹¹⁰ User identifiers are created and stored entirely on the host system, making it impossible for users to personally clear them.

2.3.7 Fingerprinting

Fingerprinting denotes a category of tracking techniques that seek to create unique user identifiers by aggregating a large number of browser and system attributes. While elements such as time zone, system language, installed fonts, and operating system are non-specific by themselves, when dozens of them are combined they can create a footprint unique to all but the most purposefully generic, newly-setup machines.¹¹¹

Fingerprinting relies on executing code, usually JavaScript, that monitors system attributes on the client machine and reports the results back to the server.¹¹² As such, individual users are hard-pressed to prevent fingerprinting in any meaningful way. Doing so would require either disabling JavaScript (which would be deleterious for the functioning of many modern websites, including non-tracking ones), using slower but anonymity-heavy browsers such as Tor, or installing browser extensions to block some of the known fingerprinting domains.¹¹³

Besides collecting basic system attributes such as a user's installed fonts and operating system, fingerprinting may rely on much more advanced methods, such as drawing invisible graphics on an HTML Canvas to detect minute and highly specific differences in the way a system renders pixels.¹¹⁴ Analogously, an audio fingerprint may be generated by delivering an audio signal and detecting minute differences in the way the client machine processes it.¹¹⁵ Certain trackers fingerprint a user by interfacing with their battery status API.¹¹⁶ This list of techniques is illustrative rather than exhaustive and, much like in the real world, a person may be described and uniquely identified via any number of observational parameters.

110 Karaj, A. et al. (2019), 'WhoTracks.Me: Shedding light on the opaque world of online tracking', [<https://arxiv.org/abs/1804.08959>], p. 3.

111 Bujlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, p. 1486.

112 Karaj, A. et al. (2019), 'WhoTracks.Me: Shedding light on the opaque world of online tracking', [<https://arxiv.org/abs/1804.08959>], p. 3.

113 EFF, 'Cover Your Tracks', *Electronic Frontier Foundation*, [<https://coveryourtracks EFF.org/about>].

114 Engelhardt, S. and Narayanan, A. (2016), 'Online Tracking: A 1-million-site Measurement and Analysis', Princeton University, [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf], p. 11.

115 Ibid., p. 13.

116 Ibid., p. 13.

Fingerprinting on mobile devices was harder in the past due to more homogeneous device configurations, however modern mobile devices are highly personalized and make it possible to reliably profile and ID users based on their configurations.¹¹⁷ Thus, a mobile device may be fingerprinted according to variables such as installed apps, user music tastes, device model, screen and memory metadata, and more.¹¹⁸

Due to the growing sophistication and reliability of fingerprinting techniques, this approach to tracking is increasingly commonplace across the internet. Al-Fannah et al. report that 68% of the top 10,000 most visited websites appear to engage in fingerprinting, which is a significant increase from 2013, when only 0.4% of the top 10,000 websites employed such techniques.¹¹⁹

117 Kurtz, A. et al. (2016), 'Fingerprinting Mobile Devices Using Personalized Configurations', *Proceedings on Privacy Enhancing Technologies*, vol. 4, no. 19, p. 14; Zimmeck, S. et al. (2017), 'A Privacy Analysis of Cross-device Tracking', *Proceedings of the 26th USENIX Security Symposium*, p. 1397.

118 Forbrukerrådet (2020), *Out of Control: How consumers are exploited by the online advertising industry*, [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 31; Kurtz, A. et al. (2016), 'Fingerprinting Mobile Devices Using Personalized Configurations', *Proceedings on Privacy Enhancing Technologies*, vol. 4, no. 19, p. 17.

119 Al-Fannah, N.M., Li, W., and Mitchell, C.J. (2019), 'Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking', *Proceedings of the 21st International Conference on Information Security*, p. 491.

Below is an example device fingerprint generated by Laperdrix et al..¹²⁰

Attribute	Source	Example
User agent	HTTP header	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36
Accept	HTTP header	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Content encoding	HTTP header	gzip, deflate, br
Content language	HTTP header	en-US,en;q=0.9
List of plugins	JavaScript	Plugin 1: Chrome PDF Plugin. Plugin 2: Chrome PDF Viewer. Plugin 3: Native Client. Plugin 4: Shockwave Flash...
Cookies enabled	JavaScript	yes
Use of local/session storage	JavaScript	yes
Timezone	JavaScript	-60 (UTC+1)
Screen resolution and color depth	JavaScript	1920x1200x24
List of fonts	Flash or JS	Abyssinica SIL,Aharoni CLM,AR PL UMing CN,AR PL UMing HK,AR PL UMing TW...
List of HTTP headers	HTTP headers	Referer X-Forwarded-For Connection Accept Cookie Accept-Language Accept-Encoding User-Agent Host
Platform	JavaScript	Linux x86_64
Do Not Track	JavaScript	yes
Canvas	JavaScript	Cwm fjordbank glyphs text quiz, ☺ Cwm fjordbank glyphs vext quiz, 😊
WebGL Vendor	JavaScript	NVIDIA Corporation
WebGL Renderer	JavaScript	GeForce GTX 650 Ti/PCIe/SSE2
Use of an ad blocker	JavaScript	yes

2.3.8 Web Beacons

Web beacons are invisible resources, usually tiny, transparent images, HTTP elements, or scripts, that are placed within a web page, email, or other online resource that supports HTML formatting.¹²¹ When the web beacon is retrieved by a user's system, the server logs the user's IP address, the User Agent (i.e. the user's web browser ID or equivalent software), referring URLs, a timestamp of the user's activity, and possibly a user's cookie ID if any can be found.¹²² Usually, web beacons are deployed alongside cookies to broaden the scope of the data they collect.¹²³ Web beacons, unlike cookies, function by logging data on a serv-

120 Laperdrix, P. et al. (2020), 'Browser Fingerprinting: A Survey', *ACM Transactions on the Web*, vol. 14, no. 2, Article Number 8, p. 5.

121 Naik, B. (2013), 'Tracking User Activities Using Web Bugs', *Infosec Institute*, [<https://resources.infosecinstitute.com/topic/tracking-user-activities-using-web-bugs/>].

122 Jokinen, J. (2018), *Personal Internet Privacy and Surveillance: Implementation and evasion of user tracking*, MSc diss., JAMK University of Applied Sciences, p. 26.

123 Ibid., p. 26.

er-side backend rather than in the users' machines, which means that they are not easily blocked by users.¹²⁴

Perhaps the most publicly recognizable web beacon is one that does not bother to hide its presence: Facebook's Like button. This and other similar social plugins function in the same way as a web beacon, fetching resources such as scripts from Facebook's servers while exposing the visiting user's information and attempting to correlate it with any cookies at Facebook's disposal.¹²⁵

2.3.9 Unique First-Party Identifiers

Many device manufacturers and other firms issue unique IDs on a per-device basis so that advertisers can track user activity from app to app and synchronize collected user information without breaking mobile apps' sandbox environments.¹²⁶ Examples of these IDs are Android's Advertising ID and Apple's Identifier for Advertisers.¹²⁷ While Android Advertising ID users are able to reset their IDs (which does not ultimately deter advertisers, who frequently re-identify users' new IDs via other bundled data),¹²⁸ the broadcasting of this identifier is opt-out rather than opt-in, requiring no consent from the user.¹²⁹

Perhaps to address this deficiency in securing user consent, in June 2020 Apple announced that it would turn its Identifier for Advertisers into an opt-in program that requires explicit consent.¹³⁰ In June 2021, Google took tentative steps in a similar direction when it announced an opt-out option for its Android Advertising ID.¹³¹ However, even with an opt-out mechanism, Android's Advertising ID would leave users vulnerable to tracking. Whereas an opted-out Apple ID replaces the ID value with zeroes to prevent identification, an opt-out from

124 Sipior, J.C., Ward, B.T., and Mendoza, R.A. (2011), 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons', *Journal of Internet Commerce*, vol. 10, no. 1, p. 4.

125 Acar, G. et al. (2015), 'Facebook Tracking Through Social Plug-ins', [<https://www.esat.kuleuven.be/cosic/publications/article-2555.pdf>], p. 2.

126 Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 124.

127 IAB (2013), 'Cookies on Mobile 101', [<https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>], p. 6.

128 Forbrukerrådet (2020), 'Out of Control: How consumers are exploited by the online advertising industry', [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 29.

129 Ibid., p. 28.

130 Koetsier, J. (2020), 'Apple Just Crippled IDFA, Sending an \$80 Billion Industry Into Upheaval', *Forbes*, [<https://www.forbes.com/sites/johnkoetsier/2020/06/24/apple-just-made-idfa-opt-in-sending-an-80-billion-industry-into-upheaval/>].

131 Grant, N. (2021), 'Google to Let Android Users Opt Out of Tracking, Following Apple', *Bloomberg*, [<https://www.bloomberg.com/news/articles/2021-06-03/google-to-let-android-users-opt-out-of-tracking-following-apple>].

Android's Advertising ID does not obfuscate or remove the identifier in any way, instead merely asking developers to respect user choices and not use it for ad personalization.¹³²

Furthermore, many larger platforms or services rely on tracking users via their own unique login solutions. Facebook, Google, Microsoft, and Twitter allow their users to log in to other services and partnered websites using their Facebook, Google, Microsoft, or Twitter credentials, thereby easily tracking user activity across the internet.¹³³ Additionally, such tech giants build up 'walled-garden environments' around their platforms, tracking permanently logged-in users across devices and reaping great stores of proprietary first-party user data.¹³⁴

2.3.10 Cross-Device Tracking and Summary

As this report has underlined several times, trackers rarely limit themselves to just one tracking modality. Cookies, fingerprinting, beacons, first-party tracking via logins, and more are all employed in conjunction to reap the greatest possible array of data. The many data sources and variables at trackers' fingertips also afford them the ability to track not just across sessions, browsers, locations, or websites, but also across devices. It is common practice for trackers to attempt to pool user data and match a desktop user with their mobile device.

In bridging the device gap, trackers may rely on data like a user's taste in music and other interest segments,¹³⁵ IP addresses and Wi-Fi SSIDs,¹³⁶ visited domains and installed apps,¹³⁷ nearby broadcasted Bluetooth Low Energy packets,¹³⁸ first-

132 Forbrukerrådet (2020), 'Out of Control: How consumers are exploited by the online advertising industry', [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 33.

133 IAB (2013), 'Cookies on Mobile 101', [<https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>], p. 7.

134 Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 124.

135 Kurtz, A. et al. (2016), 'Fingerprinting Mobile Devices Using Personalized Configurations', *Proceedings on Privacy Enhancing Technologies*, vol. 4, no. 19, p. 17.

136 Forbrukerrådet (2020), 'Out of Control: How consumers are exploited by the online advertising industry', [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 31.

137 Zimmeck, S. et al. (2017), 'A Privacy Analysis of Cross-device Tracking', *Proceedings of the 26th USENIX Security Symposium*, p. 1399.

138 Korolova, A. and Sharma, V. (2018), 'Cross-App Tracking via Nearby Bluetooth Devices', *CODASPY'18*.

party login information,¹³⁹ or even a user's typing behaviour.¹⁴⁰ All of these cross-device insights may be enhanced through cookie- and ID-synchronization between partnered trackers, leading to a pervasive surveillance apparatus.

Alongside the rise of the Internet of Things, cross-device tracking is also becoming more and more prevalent. A 2017 study by Zimeck et al. demonstrates the broad, cross-device reach many trackers have and underlines the impressive accuracy that the largest trackers (such as Google and Facebook) achieve in establishing user identities across devices.¹⁴¹

It bears emphasis that the average user is unable to prevent many of the more sophisticated tracking methodologies. While third-party cookies may be blocked via browser preferences or choices on consent management platforms, technologies such as fingerprinting are impossible to avoid without the use of privacy-centric software and domain blocklists. Web beacons, in both email and webpages, are difficult to prevent from leaking information such as IP addresses to third parties.

2.3.11 Results of Online Tracking

With the main online tracking methods having been described above, it is also pertinent to discuss what data types are being collected through these methods. The simplest answer is: everything. As Bruce Schneier points out, companies are able to employ microtargeting in digital advertising thanks to Big Data.¹⁴² The guiding principle of Big Data, as Schneier formulates it, is 'save everything you can, and someday you'll be able to figure out some use for it all.'¹⁴³

Under the umbrella of Big Data, massed computation delivers valuable insights by way of inferences. Some of the data being collected may appear benign or arbitrary at first glance, such as search patterns, scrolling behaviour, browsing history, or location data. Yet, based upon such data, algorithms are able to estimate a person's interests, personality, political ideology, race, gender, social circle, and more with ever-improving accuracy.¹⁴⁴ Schneier clearly illustrates this tension: 'data we're willing to share can imply conclusions that we don't want to

139 IAB (2013), 'Cookies on Mobile 101', [<https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>], p. 7.

140 Yuan, H. et al. (2018), 'Cross-device tracking through identification of user typing behaviours', *Electronic Letters*, vol. 54, no. 15, pp. 957-959.

141 Zimmeck, S. et al. (2017), 'A Privacy Analysis of Cross-device Tracking', *Proceedings of the 26th USENIX Security Symposium*, p. 1402.

142 Schneier, B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, p. 29.

143 Ibid., p. 29.

144 Ibid., p. 29.

share.¹⁴⁵ Of course, certain tracking methods such as passive fingerprinting do not check whether users consent to being identified and tracked like modern cookies do via CMPs. In these instances, data we do not *realize* we are sharing can imply conclusions that we do not want to share.

Zuiderveen Borgesius summarizes the most common categories of data that are collected in the course of targeted advertising.¹⁴⁶ These categories are: web browsing data, media consumption data, search data, other intentional data, transaction and pre-transaction data, demographic data, psychographic data, communication contents, social data, communication contents, self-provided data, subscription data, location data (both fixed and mobile), contextual data, environmental data, time-related data, and offline data.¹⁴⁷ In addition, metadata such as timestamps and communication recipients is also harvested across most of the above data categories, particularly in the case of encrypted communications that prevent trackers from reading their contents.¹⁴⁸ In regard to predicting behavioural patterns of individuals and small groups, metadata may even be more valuable than the actual content of data, while still remaining useful for inferring other information regarding the data subject.¹⁴⁹

Thanks to inferential processing, it is possible to transform one type of data to another, e.g., inferring demographic data from web browsing data. New data types or sources appear as the technological and legal landscape develops. For example, the programmatic digital out-of-home advertising sector (i.e., digital billboards and signage) is currently expected to grow and make use of various visual sensors to observe passers-by.¹⁵⁰ While such data may be gathered outside of a webpage, this distinction is becoming meaningless thanks to trackers' aforementioned capabilities to unify user identities across devices and locations. Thus, a webpage advert may be auctioned off using data derived from sensors in a street billboard.

Using inferential processing and the vast array of data at their disposal, the largest trackers can monitor a formidable number of attributes for each of their users. Facebook, for example, is noted to keep track of up to 52,000 attributes in

145 Ibid., p. 29.

146 Zuiderveen Borgesius, F.J. (2015), *Improving Privacy Protection in the Area of Behavioural Targeting*, Ph.D diss, University of Amsterdam, p. 56.

147 Ibid., pp. 56–60.

148 Amnesty International (2019), 'Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights', Document POL 30/1404/2019, [<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>], p. 16.

149 Ibid., p. 16.

150 Giglia, L. (2020), 'Tech Advances in OOH Advertising', *Sign Media*, [<https://www.signmedia.ca/tech-advances-in-oooh-advertising/>].

its user profiles.¹⁵¹ This is reflective of the concentrated market power of the data industry – the actors with the broadest reach are also the ones with the most accurate, deterministic data and the largest troves of first-party information.¹⁵²

The economic dimension of behaviourally targeted advertising is staggering. As of 2021, programmatic advertisements in the RTB ecosystem have a market valuation of more than €40 billion in Europe and more than €150 billion worldwide.¹⁵³ The market penetration of the largest trackers is also formidable – a 2021 W3 Techs survey estimates that Google Analytics is integrated into 55.9% of the top 10 million websites in the world,¹⁵⁴ while summations from 2015 estimated the number to be between 30 to 50 million websites.¹⁵⁵

Overall, it can be concluded that online behavioural advertising is typified by a variety of characteristics: the speed of its transactions; the multitude of involved actors and their tendency to share data or assume multiple processing roles across the RTB ecosystem; the broad troves of data being amassed and the concentration of that data into the oligarchical power structures of the biggest first parties on the web; the variety and technological sophistication of tracking methods being employed to harvest data, and the power of the industry's inferential processing algorithms to transform data and reveal new insights regarding individuals.

151 Tiku, N. (2018), 'What's Not Included in Facebook's "Download Your Data"', *Wired*, [<https://www.wired.com/story/whats-not-included-in-facebooks-download-your-data/>].

152 Engelhardt, S. and Narayanan, A. (2016), 'Online Tracking: A 1-million-site Measurement and Analysis', Princeton University, [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf], p. 8; Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, p. 121.

153 Vou, A. (2021), 'Google and Facebook dominate behavioural advertising, even with the cookie crumbling', *European Data Journalism Network*, [<https://www.europeandatajournalism.eu/eng/News/Data-news/Google-and-Facebook-dominate-behavioural-advertising-even-with-the-cookie-crumbling>].

154 W3Techs, 'Usage Statistics and market share of Google Analytics for websites', [<https://w3techs.com/technologies/details/ta-googleanalytics>].

155 McGee, M. (2015), 'As Google Analytics Turns 10, We Ask: How Many Websites Use It?', *Martech*, [<https://martech.org/as-google-analytics-turns-10-we-ask-how-many-websites-use-it/>].

3 Adtech and the General Data Protection Regulation

3.1 Background to the GDPR

Since being adopted in April 2016 and entering into proper operation in May 2018, the General Data Protection Regulation has become the foundational *lex generalis* in the European Union's regulatory framework for the protection of personal data. It establishes both the general principles of data protection law and the more specific rights, duties, and administrative procedures that ground the principles. Other legal texts in the same field, including the current ePrivacy Directive,¹⁵⁶ its upcoming successor, the ePrivacy Regulation,¹⁵⁷ and the Data Protection Law Enforcement Directive,¹⁵⁸ all have a *lex specialis* relationship with the GDPR's *lex generalis* legal norms.¹⁵⁹

To understand the tension between the GDPR and behavioural targeting technologies in adtech, it is necessary to systematically apply the GDPR's definitions and standards to the adtech sector and observe any resulting incompatibilities. This entails beginning with the issues of material and territorial scope, moving on to the determination of roles vis-à-vis data controllers and processors, and then examining the fundamental need for an appropriate legal basis for process-

156 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 ('ePrivacy Directive'), 2002, O.J. L 201.

157 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('ePrivacy Regulation', adopted Council position), 2021, ST 6087/21. Note: this refers to the version of the Proposal formally adopted by the Council on 10 February 2021.

158 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016, O.J. L 119/89.

159 Leiser, M.R. and Custers, B.H.M. (2019), 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, vol. 5, no. 3, p. 367; European Data Protection Board (2019), 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities', p. 12; Council of the EU (2021), 'Confidentiality of electronic communications: Council agrees its position on ePrivacy rules', [<https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/>].

ing. As becomes clear from the following, consent is the sole applicable basis for data processing in regard to current behavioural targeting practices, and this gives way to an analysis of relevant standards of consent, security, and transparency.

3.2 Applicability of the GDPR

3.2.1 Material Scope

Article 2(1) GDPR establishes the Regulation's material scope as applying to 'the processing of personal data wholly or partly by automated means'.¹⁶⁰ Exemptions to the GDPR's applicability include the processing of personal data by Union bodies, personal data processing in the areas of crime and public security, activities falling outside of Union law, and the processing of personal data by a natural person in the course of a purely personal or household activity.¹⁶¹

Applying the IAB's definition of programmatic advertising as 'media or ad buying that uses technology to automate and optimize, in real time, the ad buying process',¹⁶² it is evident that a) the underlying behavioural targeting technologies are automated, and b) exist in furtherance of a commercial activity that goes well beyond advertisers' 'purely personal or household activities', per the standards set by the *Lindqvist* and *Ryneš* cases.¹⁶³ The question, then, is whether the various user information involved in behavioural targeting qualifies as 'personal data' and whether this information is 'processed'.

Article 4(1) GDPR offers a definition of 'personal data' consisting of 4 elements: (1) any information; (2) relating to; (3) an identified or identifiable; (4) natural person.¹⁶⁴ CJEU case law has confirmed that this definition is purposefully broad.

In regard to point (1), *Nowak* establishes that personal data encompasses both objective and subjective assessments of a person,¹⁶⁵ while Advocate General

¹⁶⁰ Art. 2(1) GDPR.

¹⁶¹ Art. 2(2) GDPR and Art. 3 GDPR.

¹⁶² IAB, 'Glossary of Terminology', [<https://www.iab.com/insights/glossary-of-terminology/>].

¹⁶³ CJEU Case C-101/01, *Lindqvist*, judgment of 6 November 2003 and CJEU Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, judgment of 11 December 2014. For elaboration, see Kranenborg, H. (2020), 'Article 2: Material Scope', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 60, 67-69.

¹⁶⁴ Art. 4(1) GDPR.

¹⁶⁵ CJEU Case C-434/16, *Peter Nowak v Data Protection Commissioner*, judgment of 20 December 2017, para. 34.

Sharpton's opinion in *YS* reveals that data may be personal regardless of its format or its relationship to either the private or the professional life of an individual.¹⁶⁶

In regard to point (2), *Nowak* echoes previous determinations by the Article 29 Working Party that data is linked to a person through either its content, its purpose, or its effect.¹⁶⁷ In other words, data relates to a person when it either describes some aspect of their individual life, is used to influence or evaluate their life, or even when its mere processing results in a person being treated differently as a result.

The third criterion, identifiability, is considered to be fulfilled under Article 4(1) GDPR when a natural person 'can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'¹⁶⁸ Recital 26 GDPR further describes identifiability as something firmly rooted in *de facto* considerations: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly" and "account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time."¹⁶⁹

Recital 30 GDPR also explicitly stipulates that online identifiers, including cookies, IP addresses, and RFID tags, may be used to profile natural persons, particularly when combined with other information.¹⁷⁰ The *Breyer* case demonstrates this logic in practice, finding that dynamic IP addresses in many cases constitute personal data and remarking that 'it is not required that all the information enabling the identification of the data subject must be in the hands of one person.'¹⁷¹ The CJEU also notes that a 'disproportionate effort in terms of time, cost and man-power' may tip the scales away from a finding of identifiabil-

166 CJEU Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v M and S*, Opinion of Advocate General Sharpston, delivered on 12 December 2013, para. 45.

167 CJEU Case C-434/16, *Peter Nowak v Data Protection Commissioner*, judgment of 20 December 2017, para. 35; Article 29 Data Protection Working Party (2007), 'Opinion 4/2007 on the concept of personal data', p. 10.

168 Art. 4(1) GDPR.

169 Recital 26 GDPR.

170 Recital 30 GDPR.

171 CJEU Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, judgment of 19 October 2016, para. 43.

ity, even if it is possible in theory.¹⁷² Finally, the Court in *Breyer* recognizes that the legality of any available means of identification is also a determinant of the ‘reasonableness’ of any likelihood of identification, from which it may be cautiously inferred that the legality of available means may ultimately correspond with an increased likelihood of reasonable identification.¹⁷³

The criterion of identifiability has historically been a problematic one for the somewhat Silicon Valley-centric adtech industry. Some actors – particularly in the USA – mistake identifiability under the GDPR as synonymous with the concept of Personally Identifiable Information (PII). PII is defined by the IAB as ‘user data that can be used to contact the user, either directly or through a lookup’¹⁷⁴ and by Google as ‘information that could be used on its own to directly identify, contact, or precisely locate an individual’.¹⁷⁵ These formulations are focused on direct identifiability, enabled by the data ‘on its own’. In contrast, the GDPR’s regime specifically takes into consideration the possibility for disparate data to be pooled together by one or more actors in order to ‘indirectly’ identify a person. Furthermore, whereas PII relies on precise identification or contactability, the GDPR considers even ‘singling out’¹⁷⁶ an individual to carry a significant threat of identifiability.¹⁷⁷

Indeed, the GDPR’s more flexible thresholds for identifiability are necessary in the digital advertising industry, where RTB actors engage in data-pooling and cookie-syncing as a matter of course. Furthermore, as described in Section 2.3, modern behavioural targeting relies on thousands of minute observations that are frequently meaningless by themselves but come together with machine learning to create unique identifiers and descriptors of individual users.

Finally, the criterion of ‘a natural person’ in Article 4(1) GDPR is straightforward in itself. Of note is the growing number of small, home-situated enterprises and one-person online businesses, which has led to many instances where information regarding a legal person is fundamentally intertwined with the

172 Ibid., para. 46.

173 Ibid., para. 49.

174 IAB, ‘Glossary of Terminology’, [<https://www.iab.com/insights/glossary-of-terminology/>].

175 Google, ‘Ad Manager and Ad Exchange program policies: Understanding PII in Google’s contracts and policies’, [<https://support.google.com/admanager/answer/7686480?hl=en>].

176 The term ‘singling out’ refers to isolating (‘individuating’) data elements or data sets that *may* be linked to a person. While this individuation does not constitute a linkage between data and a person in itself, it is an essential first step that sets the stage for said linkage and, as such, may indicate a likelihood of imminent identification. See: Bygrave, L.A. and Tosoni, L. (2021), ‘Article 4(1): Personal data’, in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*, Oxford University Press, pp. 23-24.

177 Recital 26 GDPR.

interests of the cognate natural person.¹⁷⁸ In the *Schecke* case, the CJEU established that, where a legal person's official title identifies one or more natural people, the legal entity would be entitled to privacy and personal data protections under the Charter of Fundamental Rights.¹⁷⁹ Therefore, should a behavioural targeting enterprise orient its activities towards small businesses whose names reflect the natural persons running them,¹⁸⁰ its data processing operations would likely still fall within the scope of Article 4(1) GDPR despite only tracking a legal entity. This is reasonable and guarantees that people such as entrepreneurs and craftsmen are not left at a disadvantage in regard to the level of personal data protection afforded to them under EU law.

Applying the four criteria of personal data in the GDPR to the practices of the RTB ecosystem, it is evident that all four criteria are fulfilled.

- (1) Section 2.3 of this report has already discussed how not only is there information being handled, but that information encompasses direct observations, metadata, and inferences relating to a myriad of categories.
- (2) Online behavioural data is also undoubtedly related to its data subjects: its contents describe habits, demographics, and interests, while its eventual usage by corporations is intended to influence future behaviour towards a given commercial or even socio-political course of action.
- (3) Moreover, accurately singling out individuals is the central mechanism by which behavioural targeting in digital advertising works in the first place. Everything from unique device fingerprints to complex browsing history and demographic inferences can be pooled together to identify an individual in milliseconds. Finally, technological cooperation between different entities is the rule rather than the exception. The identification of individuals via information is not just possible, but consistently pursued and achieved with little effort.
- (4) The average internet user is a natural person rather than a legal entity.

Therefore, targeted online advertising and its technologies interact with personal data, as defined by the GDPR.

The matter of 'processing' data is much simpler. Article 4(2) GDPR defines processing as 'any operation or set of operations which is performed on personal

178 cf. van der Sloot, B. (2015), 'Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system', *Computer Law and Security Review*, vol. 31, no. 1, pp. 26-45.

179 CJEU Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, judgment of 9 November 2010, para. 53.

180 Such businesses may usually be found on e-commerce platforms, e.g., Etsy.com.

data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.¹⁸¹ Processing is, therefore, a highly inclusive concept that is formulated to ensure a high degree of protection for personal data.¹⁸² As explained in Chapter 2 of this report, targeted advertising involves the collection, recording, organization, structuring, storage, retrieval, alteration, consultation, use, (extensive) disclosure by transmission, and combination of personal data via a variety of technologies. Consequently, behaviourally targeted online advertising and the RTB ecosystem involve the processing of personal data through automated means and fall within the material scope of the GDPR.

3.2.2 Pseudonymization, Anonymization, and Digital Advertising

Pseudonymization and anonymization of personal data are two issues that are closely related to identifiability and the GDPR's material scope. Recital 26 specifies that the GDPR in particular and the principles of data protection in general do not apply to anonymous data, i.e., 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.¹⁸³ Pseudonymized data is defined under Article 4(5) GDPR as 'personal data [that] can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.¹⁸⁴

In other words, pseudonymized data is still personal data, while anonymous data is not personal data and falls outside of the GDPR's scope. Therefore, it is important to consider the challenges of achieving data anonymity and how far this term could be applicable to the digital advertising industry in particular. This holds doubly true when novel technologies such as FLoC court the high standard of legal data anonymity by employing traditional anonymization tech-

181 Art. 4(2) GDPR.

182 Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(2): Processing', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, p. 119.

183 Recital 26 GDPR.

184 Art. 4(5) GDPR.

niques (e.g., aggregation¹⁸⁵ and k-anonymity¹⁸⁶). Could it be said that a technology aiming to achieve data subject tracking and identification may ever reach anonymity?

While this is a complex question that may warrant a dedicated paper, the present analysis attempts to summarize the most salient points. From a technical standpoint, achieving reliable data anonymity is extremely challenging, if not increasingly unrealistic. In recent years, Kondor et al. used statistical models to de-anonymize datasets from transportation and mobile networks.¹⁸⁷ They estimated that they were able to accurately identify individuals 17% of the time with a week's worth of data, 55% of the time with a month's worth of data, and 95% of the time with three months' worth of purportedly anonymous data. Even more tellingly, a different study by Rocher et al. demonstrated the ability to re-identify 99.98% of Americans using anonymous datasets with as little as 15 attributes.¹⁸⁸ Remarking on their results, Rocher et al. point out that 'even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.'¹⁸⁹ How, then, does the growing difficulty of data anonymization tie into the GDPR's legal regime and its applicability?

In the EU regulatory context, data anonymization is tightly linked to the concept of identifiability and, therefore, to *de facto* considerations, as described in Section 3.2.1 of this report. As explained by Finck and Pallas, there are currently several competing views regarding standards of anonymity within the EU regulatory framework.¹⁹⁰

The A29WP has adopted an objective and extremely strict standard of anonymity, wherein it considers that only data that has undergone 'irreversible de-iden-

185 ICO (2012), 'Anonymisation: managing data protection risk code of practice', [<https://ico.org.uk/media/1061/anonymisation-code.pdf>], p. 52.

186 Cohen, A. and Nissim, K. (2020), 'Towards formalizing the GDPR's notion of singling out', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 117, no. 15, pp. 8344-8352.

187 Kondor, D. et al. (2018), 'Towards Matching User Mobility Traces in Large-Scale Datasets', *IEEE Transactions on Big Data*, vol. 6, no. 4, pp. 714-726.

188 Rocher, L., Hendrickx, J.M., and de Montjoye, Y.-A. (2019), 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications*, vol. 10, Article Number 3069.

189 Ibid., p. 1.

190 Finck, M. and Pallas, F. (2020), 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, vol. 10, no. 1, p. 12.

tification' is truly anonymous.¹⁹¹ In the view of the A29WP, 'the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, as permanent as erasure.'¹⁹² Yet, the A29WP's views, though expert, hold only advisory value and current EU jurisprudence employs a different standard of identifiability and, consequently, anonymity.

In line with prior provisions in the Data Protection Directive (DPD),¹⁹³ Recital 26 GDPR and the *Breyer* case have established a more flexible and relativistic approach towards identifiability, where a 'reasonable likelihood' of re-identification by a first or third party is considered, based on various factors such as cost, time, and available technology.¹⁹⁴ Therefore, unlike the A29WP's more stringent stance towards anonymity, the current EU legal standard adopts a risk-based approach that judges a dataset's degree of anonymity based on the reasonable likelihood of re-identification rather than on the very possibility of re-identification.¹⁹⁵ Much like the reasonable likelihood of identification, the reasonable likelihood of re-identification in any given context is determined based on, *inter alia*, the means that may be employed to achieve re-identification, the legality of said means, and the time and costs associated with achieving re-identification.¹⁹⁶

In the context of this risk-based approach to anonymity and identifiability, the growing ability of machine learning networks and statistical models to re-identify individuals within purportedly anonymous datasets should serve as a warning signal to regulators. The risk of re-identification is rising dramatically in the current technological landscape and techniques and metrics that were previously approved by EU bodies are now being demonstrated as insufficient to prevent the singling out of individuals.¹⁹⁷ Therefore, claims of anonymized data should be considered with heightened criticality and caution. Prior statements

191 Article 29 Data Protection Working Party (2014), 'Opinion 05/2014 on Anonymisation Techniques', p. 7.

192 *Ibid.*, p. 6, cited in Finck, M. and Pallas, F. (2020), 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, vol. 10, no. 1, p. 15.

193 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('DPD'), 1995, O.J. L 281/1, Recital 26.

194 Finck, M. and Pallas, F. (2020), 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, vol. 10, no. 1, p. 18.

195 *Ibid.*, p. 15.

196 See Section 3.2.1.

197 cf. k-anonymity, which the A29WP once considered as preventing the singling-out of users but which researchers have now demonstrated does not in fact do so. See: Article 29 Data Protection Working Party (2014), 'Opinion 05/2014 on Anonymisation Techniques', p. 16 and Cohen, A. and Nissim, K. (2020), 'Towards formalizing the GDPR's notion of singling out', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 117, no. 15, p. 8346.

that de-identification is ‘no silver bullet’¹⁹⁸ have only been further substantiated by recent developments, and industries should face a high burden of proof should they ever seek to dodge the GDPR’s applicability via anonymization technologies.

All of this is doubly important in the case of behavioural targeting and ‘Big Data’ in digital advertising, where data linkage and inferential processing are the norm. Such practices are particularly conducive to re-identification in anonymized datasets. Considering the prevalence of these practices, the motivation of industry actors to accurately identify users, and the growing inadequacy of current anonymization techniques, the web advertising industry, insofar as it relies on behavioural targeting, is unlikely to be able to rely on anonymization as a way of escaping the scope of the GDPR. Instead, anonymization techniques may increasingly find use as privacy-enhancers in the future, rather than as privacy guarantors in themselves.

In sum, care should be taken that new methods of ‘group behavioural targeting’ based on purportedly anonymized or aggregated datasets such as FLoC should not be excluded from the GDPR’s scope. While a group-level identifier in itself may not immediately identify an individual person within the group, Sections 3.8.7 and 5 discuss how the current means available to behavioural tracking companies can and *are* being employed to consistently re-identify individual users from aggregated Cohort IDs. Therefore, the reasonable likelihood of re-identification is significant, if not almost guaranteed, and the GDPR’s additional rights and obligations should be engaged in regard to the new wave of group behavioural tracking technologies.

3.2.3 Territorial Scope

Article 3 GDPR establishes that three sets of circumstances fall within the Regulation’s territorial scope, of which the circumstances described in Article 3(1) and 3(2) GDPR are the most relevant to RTB and behavioural targeting.

According to Article 3(1), the Regulation ‘applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.’¹⁹⁹ Article 3(1) GDPR therefore establishes two distinct criteria that must be fulfilled: the existence of an establishment of a controller or proces-

198 Narayanan, A. and Felten, E.W. (2014), ‘No silver bullet: De-identification still doesn’t work’, Princeton University, [<https://www.cs.princeton.edu/~arvindn/publications/no-silver-bullet-de-identification.pdf>].

199 Art. 3(1) GDPR.

sor in the Union and the processing of personal data in the context of that establishment's activities.

Understanding precisely what 'establishment' denotes within the GDPR is necessary to make sense of the complex web of actors within the RTB ecosystem, where many of the biggest data aggregators such as Google and Facebook are multi-national entities. In regard to the meaning of 'establishment' in this context, Recital 22 GDPR clarifies that 'establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.'²⁰⁰ Legal arrangements, therefore, are merely a probative factor in the existence of an establishment.

Truly determining the existence of an establishment is a holistic exercise done on a case-by-case basis, which takes into account many factors to determine whether 'effective and real exercise of activity through stable arrangements' occurs. In *Weltimmo*, the stability of arrangements mentioned above was revealed by the presence of representatives and of equipment and infrastructure that facilitates the effective and real exercise of activity by the aforementioned representatives.²⁰¹ This includes legal and other non-physical infrastructure, such as bank accounts.²⁰² Furthermore, the CJEU in *Weltimmo* considered that a company's place of registration is an indication of establishment (although not of *sole* establishment).²⁰³ Querying Recital 36 GDPR, it is also evident that a 'main establishment' may be evidenced by the presence of an entity's 'central administration' or by the effective and real exercise of 'management activities determining the main decisions as to the purposes and means of processing through stable arrangements.'²⁰⁴ Logically, if these factors indicate a main establishment, they are also indicative of a mere establishment.

One factor that does not, however, play a part in Article 3(1) GDPR's territorial regime is the location where data processing itself is carried out, provided that said processing is done in the context of the activities of a data controller or processor established within the Union. Since data storage itself is also a form of processing, this also means that the physical location of data is not relevant for the GDPR's territorial scope, even though the equipment used in that storage

200 Recital 22 GDPR.

201 CJEU Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, judgment of 1 October 2015, para. 30.

202 Ibid., para. 33.

203 Ibid., para. 29.

204 Recital 36 GDPR.

may play a part in demonstrating the existence of an establishment.²⁰⁵ Overall, the EDPB's Guidelines on Article 3(1) note that 'the threshold for 'stable arrangement' can actually be quite low when the centre of activities of a controller concerns the provision of services online'.²⁰⁶ Since establishment may be demonstrated by even a minimal real and effective activity within the Union, conducted through stable arrangements, the most contentious part of Article 3(1) is likely to remain the determination of what 'processing of personal data in the context of activities of an establishment [. . .] in the Union' means.

When it comes to defining the 'context of activities' of an establishment, the EDPB recommends a case-by-case *in concreto* analysis that seeks to balance the broad interpretation of the phrase that ensures a high coverage of protection for data subjects with the more restrictive interpretation that does not unfairly equate a non-EU entity's data processing outside of the Union with a far-removed commercial activity inside the Union.²⁰⁷ Such consideration of the dynamics between establishments of multi-national corporations was evident when the CJEU in *Google Spain* held that, where a subsidiary of a multi-national corporation is established in a Member State and performs activities that are differentiated yet 'inextricably linked' to the data processing operations of its parent entity in a third state, the processing of personal data for the purposes of its parent entity is also considered to be carried out 'in the context of the activities' of the Union-based establishment and, therefore, within the territorial scope of the former Data Protection Directive that the GDPR replaces.²⁰⁸ The EDPB opines that the context of an establishment's activities and its relation to data processing by another entity may be clarified by asking whether the processing is inextricably linked to the establishment's activities or by asking whether the activities amount to revenue-raising inextricably linked to the processing of personal data.²⁰⁹

One notable gap that has been pointed out in Article 3(1)'s provisions is in the case of an EU data processor and non-EU controller.²¹⁰ In such an instance, the

205 Article 29 Data Protection Working Party (2017), 'Statement of the Article 29 Working Party: Data protection and privacy aspects of cross-border access to electronic evidence', p. 5.

206 European Data Protection Board (2019), 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', p. 6.

207 *Ibid.*, p. 7.

208 CJEU Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, judgment of 13 May 2014, paras. 55-56.

209 European Data Protection Board (2019), 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', p. 8.

210 Svantesson, D.J.B. (2020), 'Article 3: Territorial Scope', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 74, 86.

processor would be within the scope of the GDPR, but the controller would not, resulting in more limited obligations. However, as consequent sections in this report dealing with the definitions of data controllers and processors reveal, this is of relatively little significance in the case of adtech and behavioural targeting, since the majority of entities in the RTB ecosystem qualify as (joint) data controllers in and of themselves.

According to Article 3(2), the Regulation also applies if a controller or processor established outside of the Union processes the personal data of data subjects within the Union in relation to either the offering of goods or services to data subjects within the Union or, alternatively, to monitoring data subjects' behaviour insofar as that behaviour takes place within the Union.²¹¹ Under this Article, it is therefore relevant to consider three criteria: the requirement for data subjects to be within the Union, the offering of goods or services to data subjects, and the monitoring of data subjects' behaviour.

To begin with, the requirement that data subjects must be within the Union refers to their physical presence rather than to any legal arrangement such as citizenship or residence.²¹² This provides for a broad safety net that reflects the status of data protection as a fundamental right enjoyed by all natural persons, pursuant to Recital 1 GDPR.²¹³ However, processing the personal data of data subjects physically located within the Union alone is not sufficient to trigger the GDPR's applicability on its own – it must always be demonstrably accompanied by 'targeting'²¹⁴ via either the offering of goods or services to data subjects within the EU or by the monitoring of the same subjects.

The offering of goods or services is one of two possible manifestations of targeting under Article 3(2) GDPR. Pursuant to Recital 23 GDPR, an offer of goods or services is different from the mere accessibility of websites, but rather reflects a conscious 'envisaging' by a data controller or processor to offer its services to Union-based data subjects.²¹⁵ To help clarify the concept of offering goods and services under the GDPR, the EDPB's Guidelines on Article 3 GDPR refer to the distinct but closely-related concept of 'directing activity' within the meaning of

211 Art. 3(2) GDPR.

212 European Data Protection Board (2019), 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', p. 14.

213 Recital 1 GDPR.

214 European Data Protection Board (2019), 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', p. 15.

215 Recital 23 GDPR.

Article 15(1)(c) of Regulation No. 44/2001.²¹⁶ Based on the *Pammer and Alpenhof* cases, the EDPB therefore indicates the following non-exhaustive list of factors as probative in regard to the offering of goods and services:

The EU or at least one Member State is designated by name with reference to the good or service offered;

The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience;

The international nature of the activity at issue, such as certain tourist activities;

The mention of dedicated addresses or phone numbers to be reached from an EU country;

The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example '.de', or the use of neutral top-level domain names such as '.eu';

The description of travel instructions from one or more other EU Member States to the place where the service is provided;

The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;

The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states;

The data controller offers the delivery of goods in EU Member States.²¹⁷

In regard to the concept of 'monitoring', the EDPB's recommendations significantly expand and clarify the GDPR's provisions. Recital 24 of the GDPR states:

'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'²¹⁸

Going beyond the Recital, the EDPB aptly recommends that monitoring be considered not just in relation to tracking on the internet, but also tracking through

216 European Data Protection Board (2019), 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', p. 17.

217 Ibid., pp. 17-18.

218 Recital 24 GDPR.

other networks and technologies, such as wearables.²¹⁹ More interestingly, the EDPB considers that monitoring as an activity must always be qualified by the presence of specific intent on the part of the monitor, embodied in a purpose underlying the data processing.²²⁰ This would align the concept of monitoring under Article 3(2)(b) more closely with the ‘envisaged’ (and therefore, intended) offering of goods or services under Article 3(2)(a) and exclude the automatic categorization of ‘any online collection or analysis of personal data of individuals in the EU’²²¹ as monitoring. As monitoring activities, the EDPB includes, *inter alia*, ‘behavioural advertisement, geo-localisation activities, in particular for marketing purposes, online tracking through the use of cookies or other tracking techniques such as fingerprinting, personalised diet and health analytics services online, CCTV-Market surveys and other behavioural studies based on individual profiles, and monitoring or regular reporting on an individual’s health status’.²²²

Applying the territorial scope of the GDPR to the current state of the adtech industry and its behavioural targeting practices reveals that there is no single provision that perfectly encapsulates all industry actors. The largest actors, such as Facebook and Google, occupy several positions within the adtech ecosystem simultaneously across their subsidiaries. They act as DMPs (data brokers) insofar as they collect and sell user data to advertisers. Both companies also operate their own ad exchanges (Facebook Exchange and Google AdX), their own DSPs (Facebook Ad Manager and Google Ad Manager), their own ad networks (Facebook Audience Network and Google AdSense/AdMob) and their own publisher spaces within their social media website and search engine, respectively. Considered as a whole, these entities certainly engage in monitoring their users and profiling them for the purposes of behaviourally targeted advertising, thereby falling neatly within the scope of Article 3(2)(b) GDPR insofar as the monitored users are within the EU. However, multinational conglomerates such as Facebook and Google frequently employ subsidiaries to contract with users in the EU, such as Facebook Ireland Limited or Google Ireland limited. In cases where such local subsidiaries exist, Article 3(1) GDPR is likely to apply to their activities in the cases where the subsidiaries either directly process personal data or their activities are ‘inextricably linked’ to the multinationals’ primary adtech offerings.

219 European Data Protection Board (2019), ‘Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)’, p. 19.

220 Ibid., p. 20.

221 Ibid., p. 20.

222 Ibid., p. 20.

Looking past the largest multinational actors, the GDPR's territorial scope is most likely to extend to domestic RTB actors via Article 3(1) and to foreign actors processing the data of data subjects within the Union via Article 3(2)(b) by virtue of the fact that both first- and third-party data is compiled and shared for behavioural advertisement and marketing purposes, as explicitly provided for in the EDPB's Guidelines.²²³

Nevertheless, the EDPB's view that monitoring must always be qualified by intent and underlying purpose opens a curious loophole when juxtaposed with the formulation of Big Data's guiding principle by Schneier as 'save everything you can, and someday you'll be able to figure out some use for it all.'²²⁴ With falling data storage costs and ever more valuable inferential capacity by machine learning algorithms, it is indeed theoretically possible for larger tech companies to collect data on all kinds of user behaviours online without having a pre-existing purpose in mind and instead relying on machine learning algorithms to reveal emergent insights and applications for the data. In such a scenario, the EDPB's requirement for there to be 'intention' behind the behavioural data collection would open the possibility for a nonsensical exemption of such activities from being classified as 'monitoring' under the GDPR's territorial scope. As such, it appears reasonable that EU jurisprudence should adopt a broader and more flexible understanding of Article 3(2)(b) GDPR going forward, rather than tying it with the same requirements of intent inherent to Article 3(2)(a).

3.3 Assigning the Roles of RTB Actors

The precise obligations of an entity whose activities fall within the scope of the GDPR depend on whether it is classified as a data controller or a data processor. Notably, the roles of data controller and data processor are assigned in the context of each individual data processing operation, meaning that the same entity may be considered a controller in one instance and a processor in another, depending on which of its discrete activities is the subject of scrutiny.²²⁵ In cases where personal data processing involves a long chain of operations, it is also possible for entities to variously qualify as controllers (whether joint or sole) or processors depending on which stage of the operation chain is under consideration.²²⁶

223 Ibid., p. 20.

224 Schneier, B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, p. 29.

225 European Data Protection Board (2020), 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', p. 11.

226 Ibid., pp. 18-19.

Article 4(8) GDPR defines a processor as ‘a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’.²²⁷ This is a straightforward definition with two implications. First, that there is no processor without a corresponding controller and, second, that a processor is a separate entity from its controller.²²⁸

A controller, then, is defined under Article 4(7) GDPR as ‘the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data’.²²⁹ Such an entity’s control over determinations of the purposes and means of personal data processing is considered from a factual rather than a formalistic legal viewpoint,²³⁰ making it entirely possible for an entity to assume controllership as a result of its implicit competences or even as a result of its unlawful actions.²³¹

For the purposes of determining controllership over personal data, the EDPB notes that the means of data processing may be subdivided into ‘essential’ and ‘non-essential’ means, where the latter may be left to a processor’s discretion without impacting the controller-processor classification.²³² Examples of essential means of data processing include the type of personal data being processed, the duration of processing, the categories of recipients, and the categories of data subjects, while non-essential means may refer to minor technical or organizational choices, such as the choice of hardware, software, or detailed security measures.²³³ Even where non-essential elements are left to the processor’s discretion, the controller is required to fulfil its technical, organizational, and security obligations under Articles 24, 25, and 32 GDPR, which in themselves require the controller to stay fully informed regarding all the means that are being implemented during personal data processing operations.²³⁴ Therefore, delegation in itself does not justify ignorance on the part of the controller in regard to the delegated means.

227 Art. 4(8) GDPR.

228 Bygrave, L.A. and Tosoni, L. (2020), ‘Article 4(8): Processor’, in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 157, 159.

229 Art. 4(7) GDPR.

230 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, para. 20.

231 Article 29 Data Protection Working Party (2010), ‘Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’’, p. 9.

232 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, para. 13.

233 Ibid., p. 14.

234 Ibid., p. 15.

The act of ‘determining’ the purposes and means of processing has been interpreted broadly by the CJEU. Most recently, the *Fashion ID* case has reinforced prior rulings that the ‘exertion of influence for one’s own purposes’ and the ‘participation in the determination of purposes’ are sufficient thresholds for controller-ship over personal data processing.²³⁵ *Fashion ID* also confirmed that a joint controller need not have access to the processed data to be considered a joint controller,²³⁶ while the EDPB opines that this rationale extends to sole controllers as well.²³⁷

As the preceding paragraph already mentioned, it is also possible for controller-ship under the GDPR to be shared ‘where two or more controllers jointly determine the purposes and means of processing’.²³⁸ The threshold to qualify as a joint controller is not lowered or relaxed relative to the threshold for sole controller-ship; rather, each joint controller participates in the determination of the purposes and means of processing.²³⁹ Concurrently, however, the CJEU has confirmed in *Fashion ID* and *Wirtschaftsakademie* that joint controller-ship does not imply equal responsibility between controllers.²⁴⁰

The EDPB opines that joint participation in the determination of means and purposes may result from either a common decision reflecting common intentions or from converging decisions.²⁴¹ The latter refer to circumstances where two parties, each acting with its own purpose, make decisions that have a tangible impact on the determination of the means and purposes of processing, in such a way that the processing by each party is inextricably linked and the overall processing would not be possible without both parties’ participation.²⁴²

As an example of such inextricably tied determinations of means and purposes, the *Fashion ID* case revolved around a publisher’s (*Fashion ID*’s) inclusion of a web beacon (the Facebook ‘Like’ button) in its website to increase the publicity of its goods. The Like button transmitted the personal data of visitors to *Fashion*

235 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, para. 68.

236 *Ibid.*, para. 69.

237 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, p. 16.

238 Art. 26 GDPR.

239 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, p. 17.

240 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, para. 43.

241 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, p. 18.

242 *Ibid.*, p. 18.

ID's website over to Facebook Ireland Limited. In the context of this act of personal data processing, the CJEU ruled that Fashion ID's act of including the Like button web beacon in its website constituted a joint determination of the means and purposes of data processing alongside Facebook, the Like button's developer.²⁴³ Although Facebook and Fashion ID each acted with a different purpose (publicity increase versus the collection of data on user behaviour, respectively), their decisions converged under a common economic interest. Insofar as Facebook would not receive user data had Fashion ID not incorporated the Like button and Fashion ID would not have a Like button to incorporate had Facebook not developed it, the actions of both entities were inextricably linked and inseparable in their determination of the processing operations, leading to a finding of joint controllership.²⁴⁴

In the *Wirtschaftsakademie* case, the CJEU ruled that the administrator of a Facebook fan page was a joint controller alongside Facebook in setting up the fan page and logging page visits and user behaviour.²⁴⁵ Since the administrator had set the parameters of its Facebook fan page in accordance with a specific target audience and the particular goals of 'managing and promoting activity', it had acted to determine both the means and the purposes of the processing that would be carried out within Facebook's platform in regard to that fan page.

In *Jehovan todistajat*, the CJEU found that a religious community of Jehovah's Witnesses which organizes, coordinates, and encourages data collection, and subsequently processes the collected data, qualifies as a joint controller along with the community members who actually carry out the data collection.²⁴⁶ Notably, the community's joint controllership role arose despite the fact that it was somewhat 'hands-off' in regard to non-essential means of data collection. While Jehovah's Witnesses did not provide written guidelines or instructions for data processing activities, their general urging and mobilizing of members to conduct door-to-door preaching in order to spread their faith was found to constitute a sufficient determination of means and purposes.²⁴⁷

In *Wirtschaftsakademie*, *Fashion ID*, and *Jehovan todistajat* it is evident that the decision by an entity to employ a particular data processing infrastructure is

243 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, para. 81.

244 Ibid., para. 80.

245 CJEU Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, judgment of 5 June 2018, para. 75.

246 CJEU Case C-25/17, *Proceedings brought by Tietosuoja- ja valtuutettu (Jehovan todistajat)*, judgment of 10 July 2018, para. 70.

247 Ibid., para. 73.

sufficient to give rise to joint controllership between the entity and the infrastructure’s developer, provided that the consequent data processing operation is contingent on both the entity and the developer’s cooperation. It is also evident how restrained the context of data processing activities is – both Wirtschafts-akademie and Fashion ID were joint controllers in regard to the initial logging of user behaviour, but they were free of responsibility in regard to any consequent data processing (e.g., inferential processing) performed by Facebook.

Keeping in mind the GDPR’s provisions, the CJEU’s case law, and the EDPB’s guidelines, it is possible to apply the concepts of data controller and data processor to the various actors in the RTB ecosystem and the various users and developers of behavioural tracking technologies in order to begin establishing their legal responsibilities.

3.3.1 Users

Referring to the schematic of RTB actors in Section 2.2.1 of this report, the user is considered a data subject under Article 4(1) GDPR, being an identified or identifiable natural person whose personal data on behaviour is being processed as part of behavioural monitoring and targeted advertising.²⁴⁸

3.3.2 Publishers

When the user accesses a webpage engaged in behavioural monitoring, the publisher behind that webpage may be considered either a data controller or a joint data controller.

In instances where the publisher has implemented its own tracking and monitoring solutions (such as first-party cookies, Etags, web beacons, or first-party fingerprinting technologies), the publisher itself has defined both the purposes and the means of its data processing activities. However, as previously discussed, only the largest corporations such as Google or Facebook have the far-reaching online presence that allows for truly robust profiling solely through the use of first-party data. For the rest of the online sphere, an exclusively first-party tracking configuration is of limited value. To illustrate this, a study on browser fingerprinting by Al-Fannah et al. finds that as little as 2.4% of examined websites rely only on first-party fingerprinting and a further 13.1% rely on combined first-and-third-party fingerprinting.²⁴⁹ The remaining 84.5% of websites engaged in

248 Art. 4(1) GDPR.

249 Al-Fannah, N.M., Li, W., and Mitchell, C.J. (2019), ‘Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking’, *Proceedings of the 21st International Conference on Information Security*, p. 489.

fingerprinting relied exclusively on third-party trackers.²⁵⁰ Consequently, very few web page publishers are likely to be deemed sole data controllers.

In the significantly more common case of a publisher implementing third-party cookies, Etags, fingerprinting, etc., the CJEU's rationale in *Fashion ID* and *Wirtschaftsakademie* would render the publishers joint data controllers in the context of the data processing carried out by their third-party tracking solutions. This is due to the fact that the decision to implement a third-party tracking solution *per se*, combined with the necessary parameter-setting in regard to one's own website, all constitute a very real determination of means and purposes of personal data processing on the part of the publisher.

The situation becomes more complicated in the case of fourth-party tracking vendors, i.e., vendors that have no direct contact with the publisher, yet have their tracking technologies deployed in the publisher's website by the publisher's third-party partners. Insofar as the data collection by such entities falls within the means and purposes of data operations defined by the publisher in their dealings with third parties, it may be considered that the publisher is also a joint controller in the data operations of these fourth parties. However, in cases where the activities of fourth parties are separable and sufficiently divorced in means and/or purpose from the publisher's data processing, the publisher would likely not be considered a data controller despite the fourth parties' operations relying on the publisher's website. As noted by the CJEU in *Fashion ID*, 'a natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means.'²⁵¹ In essence, the deployment of fourth-party tracking technologies would necessitate the same legal test for controllership as third-party cookies, but in this case the extra degree of separation between publisher and tracking vendor may contribute to a finding of separation of data processing operations. This consideration may seem convoluted, but it is important in the case of the RTB ecosystem, where the multitude of parties involved in an auction and the dynamic nature of auctions make it very hard for publishers to predict what scripts or technologies may get embedded in their web pages across their chain of partners. As pointed out by Urban et al. in 2020 'before loading the directly embedded [third party], it is often not definite which other parties might be loaded—especially ad networks load various fluctuating partners.'²⁵²

250 Ibid., p. 489.

251 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, para. 74.

252 Urban, T. et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the '20 World Wide Web Conference*, p. 1284.

This does not mean that publishers may bear no responsibility for the data processing operations of fourth parties on their web pages, but rather that this responsibility derives from the principles of accountability and data integrity and confidentiality under Article 5 GDPR (as operationalized under Articles 24, 25, and 32 GDPR) as they relate to the publisher's own web page. If publishers do not wish to be engaged in additional data controller responsibilities, they must maintain sufficiently high standards of data security and audit their partners and data flow to prevent leakage. In short, there is no room for unsupervised fourth-party operations – either such operations are sanctioned by the publisher as a joint controller, or they are forestalled through appropriate technical and organizational safeguards.

3.3.3 Actors in FLoC and FLEDGE

Newer technologies such as FLoC and FLEDGE are still in the development stage and, consequently, the manner in which they interface with the regulatory framework of personal data protection may change alongside their technical specifications.

In the case of FLEDGE, it stands to reason that the owners of interest groups, be they publishers, advertisers, or other third parties, constitute data controllers due to the act of defining and maintaining an interest group's membership. However, the case with FLoC's cohorts is less clear and the technology has elicited questions as to whether Google itself is not also a joint data controller. To date, the corporation has considered itself a data processor in the context of operating the Google Chrome browser.²⁵³ Due to FLoC's increased reliance on the browser for in-browser computation to scan individuals' browsing histories and assign them identifiers for the conduct of on-device auctions, it seems likely that a European regulator would reconsider Google's position as a mere processor. The fact that Google develops and implements the back-end enabling and directing FLoC's classification of users indicates that Google may have determined both the technical means and purposes of FLoC's personal data processing operations. On the most basic level, Google has conceptualized FLoC as a method to derive (group-level) identifiers for use in targeted advertising, which indicates a determination of purposes in regard to processing those identifiers. Subsequently, although identifiers are the result of an algorithmic computation and not a manual assignment by Google, Google is the entity that defines how that algorithm clusters users, what inputs it takes, and the duration of identifier storage before cohort recalculation, therefore determining the parameters and means of data processing. In parallel, any other browser vendor developing and

253 Google (2020), 'Data Processing Amendment to Chrome Agreements', [https://www.google.com/chrome/terms/dpa_terms.html].

implementing its own FLoC model could likewise be considered a data controller.

3.3.4 Advertisers

Beyond all these tracking technologies that may be employed on a webpage, however, the RTB process also involves the constant syncing, sharing, and sale of information between advertisers and trackers. Of these, the advertisers are invariably considered joint controllers of data processing insofar as their advertising campaigns define and ask for personal data inputs, then bid on data subjects' impressions based on those inputs. Pursuant to *Wirtschaftsakademie*, the act of defining target audience parameters and soliciting relevant personal data, thereby causing its processing by trackers, is sufficient to render advertisers joint data controllers.²⁵⁴

3.3.5 SSPs, DSPs, Networks, Exchanges, and Brokers

Many of the remaining actors, including supply-side platforms, ad networks, ad exchanges, data brokers, and demand-side platforms, are hard to classify in broad strokes. Depending on the specifics of their operations, they may be anything from processors to joint controllers or sole controllers. The determining factor here would usually be the extent to which any given data processing operation by these entities is directed by an advertiser or other RTB actor. As an actor exercises greater independence in data gathering and processing and derives greater personal benefits from the data processing activity (outside of mere remuneration for a closely-directed task), the likelihood increases that this actor is a sole or joint controller rather than a processor. Of note is that ad networks, data brokers, demand-side platforms, and supply-side platforms frequently track a broad array of audience attributes and bid analytics, which may then be selectively requested by advertisers or reported by publishers. In such instances, where the aforementioned actors play a role in defining their own audience tracking parameters, they engage in joint controllership over the transmission upon request of this data with advertisers, publishers, or with each other, as well as in relation to the data's initial procurement from a publisher-user interface. Due to the prevalence of data transmission and syncing within the RTB landscape, joint controllership scenarios are expected to be pervasive.²⁵⁵

254 CJEU Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, judgment of 5 June 2018, para. 39.

255 Veale, M. and Zuiderveen Borgesius, F.J. (2021), 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>], p. 31.

3.3.6 CMPs

Consent management platforms are a particularly problematic element in the RTB ecosystem, beginning with their basic role in data processing. As pointed out by Santos et al., the two most popular CMPs in Europe are Quantcast and OneTrust.²⁵⁶ The legal terms and conditions of both Quantcast and OneTrust specify that they act as data processors under the GDPR,²⁵⁷ and so too does the IAB's Transparency and Consent Framework (TCF) policy document regarding CMPs.²⁵⁸ Insofar as these entities solely carry out the management of user consent, as specifically directed by contracting publishers, they would indeed be processors.

Yet, Santos et al. demonstrate that many CMPs integrate additional functionalities that go beyond the scope of their role as processors.²⁵⁹ For instance, Quantcast installs a tracking pixel for audience insights into a webpage along with its consent pop-up. This leads to an entirely separate act of data processing whose purposes and means (audience insight generation and tracking cookie, respectively) are determined by the CMP itself, rendering it a data controller. Furthermore, Santos et al. demonstrate that the installation process for the Quantcast CMP makes it extremely onerous for publishers to manually select and exclude vendors one-by-one, while OneTrust's free service gives publishers no control over the vendor list whatsoever.²⁶⁰ As a result, publishers are unable to play an effective role in selecting vendors (and their corresponding purposes) to be presented to the end user for the latter's provision of consent, defaulting instead to a blanket acceptance of all IAB-registered vendors. This leaves the CMPs, the entities that designed the restrictive publisher-facing interface in such a way so as to presuppose the adoption of hundreds of IAB-registered vendors, as *de-facto* determinators of the purposes (via vendors) of data processing that the publisher will eventually offer the end user.²⁶¹ Finally, the researchers point out that the choice of many CMPs to employ manipulative dark patterns in the design of their consent banners goes beyond the mere implementation of consent registra-

256 Santos, C. et al. (2021), 'Consent Management Platforms under the GDPR: processors and/or controllers?', *Annual Privacy Forum 2021*, p. 49.

257 Quantcast (2020), 'Quantcast Choice Terms of Service', [<https://www.quantcast.com/legal/quantcast-choice-terms-of-service/>], 5.1.1(b); OneTrust (2019), 'OneTrust Terms and Conditions – Cloud Deployment', [<https://www.onetrust.com/terms/OneTrustTermsConditionsUSCloudOneTrustStore.pdf>], p. 10, para. 1.2.

258 IAB Europe (2021), 'IAB Europe Transparency & Consent Framework Policies', [https://iabeurope.eu/wp-content/uploads/2021/05/TCF_v2-0_PolicyVersion_2021-05-27-3.3.pdf], p. 11, para. 11.

259 Santos, C. et al. (2021), 'Consent Management Platforms under the GDPR: processors and/or controllers?', *Annual Privacy Forum 2021*, pp. 47-69.

260 Ibid., p. 58.

261 Ibid., p. 59.

tion mechanisms. When a CMP nudges users towards a particular choice and even designs the implemented dark pattern itself, it may qualify as acting as a controller determining the means of data processing rather than a processor implementing technical or computational measures.²⁶²

Therefore, the roles of CMPs in reality are frequently different from their idealized portrayal as impartial data processors. Rather, many CMPs either engage in data processing operations of their own design, therefore becoming controllers, or play an active role in the determination of the means and purposes of data processing operations, leading to CMPs' joint controllership with publishers and advertisers.

3.3.7 The IAB

Uniquely positioned among the various advertisers, exchanges, DSPs, SSPs, and publishers is the overarching trade association that is the Interactive Advertising Bureau. The IAB is an advertising industry body whose chief concern is the promulgation of industry guidelines and technical specifications that enable programmatic advertising practices to operate in harmony with the law. To begin with, the IAB is responsible for adopting the existing OpenRTB infrastructure as an industry standard.²⁶³ More fundamentally, IAB Europe publishes the TCF that regulates the functioning of CMPs and consent collection mechanisms and provides legal and operational advice for adtech actors.²⁶⁴ An affiliated entity – the IAB Tech Lab – defines the IAB Taxonomies, whose shared industry codes and audience/content segments give structure to individual data profiles and facilitate easy data syncing between trackers.²⁶⁵ IAB Europe does not directly collect or sell user data, with the exception of its role in managing the domain used for the collection and sharing of user consent strings by CMPs – *consensu.org*.²⁶⁶

262 Ibid., p. 61.

263 IAB, 'openrtb', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md>].

264 IAB (2020), 'A Guide to the Post Third-Party Cookie Era', [https://designrr.s3.amazonaws.com/mardare_at_iabeurope.eu_80924/_5449.pdf]; IAB Europe (2021), 'New Guide: GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR', [<https://iabeurope.eu/knowledge-hub/guide-gdpr-data-protection-impact-assessments-dpia-for-digital-advertising-under-gdpr/>]; IAB Europe, 'TCF – Transparency and Consent Framework', [<https://iabeurope.eu/transparency-consent-framework/>].

265 IAB Tech Lab, 'Audience Taxonomy', [<https://iabtechlab.com/standards/audience-taxonomy/>].

266 IAB, 'Transparency and Consent String with Global Vendor & CMP List Formats', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md>].

The IAB itself rejects any notion that it is engaged in data controllership under the GDPR, reasoning that all its actions merely constitute the management of a ‘best practice standard’.²⁶⁷ Yet, a recent report by the Belgian DPA’s investigative department has identified IAB Europe as a data controller due to its role in managing the TCF.²⁶⁸ The DPA ruled that IAB Tech Lab was not a data controller,²⁶⁹ yet it also held IAB Europe accountable for the failure of its TCF and its OpenRTB protocol to adequately regulate the processing of sensitive personal data.²⁷⁰

One possibility is that IAB Europe qualifies as a data controller by determining the purposes of data processing. Indeed, the IAB’s TCF Policies document defines ten purposes and two ‘special purposes’ for personal data processing under Appendix A, pursuant to Chapter I(1)(12) of the Policies, which may be chosen and adapted by TCF participants.²⁷¹ Each of the listed purposes is accompanied by the IAB’s pre-formulated legal description, user-friendly text, and vendor-oriented guidance. Despite claims to the contrary,²⁷² the mere delineation of possible purposes is arguably not the same as actual determination. There is a finite number of logically plausible purposes for personal data processing in online behavioural targeting and compiling this closed list for ease of reference can hardly be seen as equivalent to an active determination or selection of any of these individual purposes. Insofar as a purpose is the causative force behind any personal data processing operation,²⁷³ it seems unreasonable to assume that simply listing possible reasons for undertaking a course of action is equivalent to actually bringing about that course of action. In other words, pointing out why one *could do* something is not equivalent to determining why one *does* or *should do* something. Therefore, it is doubtful that the IAB is actively

267 IAB Europe, ‘IAB Europe Submits Response to Preliminary Report of The Belgian Data Protection Authority’, 2020, [<https://iab europe.eu/blog/iab-europe-submits-response-to-preliminary-report-of-the-belgian-data-protection-authority/>].

268 IAB Europe (2020), ‘IAB Europe Submits Response to Preliminary Report of The Belgian Data Protection Authority’, [<https://iab europe.eu/blog/iab-europe-submits-response-to-preliminary-report-of-the-belgian-data-protection-authority/>].

269 IAB Tech Lab (2020), ‘IAB & IAB Tech Lab Respond with Support for OpenRTB and IAB Europe’s Transparency & Consent Framework’, [<https://iabtechlab.com/iab-and-tech-lab-respond-with-support-for-open-rtb-and-iab-europes-transparency-consent-framework/>].

270 Irish Council for Civil Liberties (2020), ‘Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR’, [<https://www.iccl.ie/digital-data/apd-iab-findings/>].

271 IAB Europe (2021), ‘IAB Europe Transparency & Consent Framework Policies’, [https://iab europe.eu/wp-content/uploads/2021/05/TCF_v2-0_PolicyVersion_2021-05-27-3.3.pdf], Appendix A.

272 Bielova, N. and Santos, C. (2020), ‘Feedback regarding EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, *Inria*, [<https://hal.inria.fr/hal-03117323/document>], p. 3.

273 European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, para. 31.

determining the purposes of data processing operations via its published standards.

However, it is less clear whether the IAB's published standards constitute a determination of essential means. Fundamentally, IAB Europe's TCF establishes that online behavioural tracking should be contingent on mechanisms such as a global consent string.²⁷⁴ The TCF also incorporates the APIs that will be used by CMPs to access and modify said string, with the API acting as a 'unified interface for seamless interaction between the parties in the advertising industry'.²⁷⁵ Moreover, IAB Europe itself stores (i.e., processes) global consent strings and controls CMPs' access thereto.²⁷⁶ Insofar as the mechanism of establishing and sharing a lawful basis for processing amounts to a vital means of personal data processing operations, and insofar as IAB Europe operates such a consent mechanism without delegation or instruction by a specific controller, it is pertinent to ask at what point IAB Europe's active facilitation of data processing translates to a determination of essential means.²⁷⁷ The answer to these questions lies in whether the IAB's TCF (and/or other standards such as IAB Tech Lab's Audience Taxonomy and OpenRTB protocol) are closer to a 'best practice standard',²⁷⁸ a 'fundamental architecture for a large information system',²⁷⁹ or a 'tool or other system allowing the processing of personal data' comparable to the Facebook 'Like' button.²⁸⁰ Logically, the former two are unlikely to trigger a finding of controllership, while the latter is likely to invite joint controllership.²⁸¹

Unlike a purely normative best practice guideline, the IAB's TCF includes concrete technical specifications developed by the IAB itself. The shared global consent string and approved CMP/vendor lists may be considered essential new concepts and tools purpose-built for the realization of data processing, render-

274 IAB, 'IAB Europe Transparency and Consent Framework Implementation Guidelines', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md>].

275 *Ibid.*

276 IAB, 'CMP Mask', [<https://register.consensu.org/CMP/>].

277 Bielova, N. and Santos, C. (2020), 'Feedback regarding EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR', *Inria*, [<https://hal.inria.fr/hal-03117323/document>], p. 2.

278 IAB Europe (2020), 'IAB Europe Submits Response to Preliminary Report of The Belgian Data Protection Authority', [<https://iabeurope.eu/blog/iab-europe-submits-response-to-preliminary-report-of-the-belgian-data-protection-authority/>].

279 Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(7): Controller', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 145, 151.

280 European Data Protection Board (2020), 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', para. 65.

281 *Ibid.*, para. 65.

ing the IAB's TCF not just a mere technical implementation outlined by a third entity, but a novel design and an ongoing, active determination of means. The IAB's global consent sharing mechanism may have served to elicit data processing operations that would otherwise not have been possible in its absence, particularly due to, for example, data subjects neglecting or declining to give separate tracking consent to every individual website they visit. The IAB's proactivity, creativity, and technical specificity in implementing an industry processing framework may thus conspire to bring about a determination of controllership.

Furthermore, the fact that the OpenRTB protocol is specifically intended for the collection and transmission of personal data in furtherance of the advertising industry's singular economic activity, rather than being a more 'general purpose' ICT protocol such as HTTP, may indicate that the OpenRTB protocol is to be considered a specific 'tool or other system allowing the processing of personal data' rather than a 'fundamental architecture for a large information system'. Through its activity in developing and stewarding the OpenRTB protocol, including specifying permissible attributes and fields for each object in the bid-stream, IAB Europe may be seen as determining the essential means of data processing that underly many RTB operations, leading to joint data controllership obligations.²⁸²

Ultimately, it is beyond the scope of this report to conclude with certainty whether IAB Europe is a mere processor or, rather, a joint controller of data processing operations under its TCF and OpenRTB, acting with a convergent purpose to other adtech entities and determining the essential means of data processing. For now, the investigative findings of the Belgian DPA and the EDPB's views that the usage of third-party tools likely triggers joint controllership obligations are both an admitted cause for concern at IAB Europe²⁸³ and may be indicative of future regulatory trends.

3.3.8 Summary of RTB Roles and the Morass of Joint Controllership

In sum, the RTB ecosystem is typified by a state of affairs where many actors declare themselves mere processors, but beneath such declarations lie pervasive *de facto* joint controllership arrangements. This is a particularly problematic state of affairs when the joint controllership arrangements involve RTB actors that the data subject has no ready access to, as it serves to undermine the effec-

282 Ryan, J. (2018), 'Critical data protection problems in the IAB's new OpenRTB 3.0 Spec', *Brave*, [<https://brave.com/iab-rtb-problems/>].

283 IAB Europe (2020), 'IAB Europe submission to the EDPB public consultation on Guidelines 08/2020 on the targeting of social media users', [https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/iab_europe_-_response_to_edpb_guidelines_08-2020.pdf], p. 5.

tive protections of the GDPR. As noted by AG Bobek in *Fashion ID*, ‘effective protection of something tends to dramatically decrease if everyone is made responsible for it.’²⁸⁴ Pervasive joint controllership is problematic not just in regard to *ex post facto* correctional enforcement and culpability in the face of noncompliance, but also in regard to proactively ensuring GDPR compliance in the first place. The Regulation imposes high standards of consent, transparency, and accountability, all of which are extremely difficult to adequately maintain when dozens (or hundreds) of RTB actors simultaneously act as joint controllers. This problem is further discussed in Sections 3.5 – 3.9, but the basic structure of the RTB ecosystem invites tension between its myriad actors and the GDPR. This is not so much a problem with the GDPR, but rather with the current RTB system, since its ‘data free-for-all’²⁸⁵ and multiplicity of controllers conflict with a regulated data protection regime that seeks to delineate, identify, and hold accountable all involved actors for the benefit of the data subject.

3.4 The Seven Principles of Personal Data Processing

At the heart of the European Union’s data protection regime lie the seven principles of data processing established in Article 5 GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Of these principles, two are particularly implicated in the case of RTB and behaviourally targeted advertising: lawfulness, fairness and transparency under Article 5(1)(a), and integrity and confidentiality under Article 5(1)(f).

Many foundational issues arise early on, starting with RTB companies’ obligation to select an appropriate basis for lawful processing and fulfilling all relevant requirements thereof.

284 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Opinion of Advocate General Bobek, delivered on 10 December 2018, para. 92.

285 Ryan, J. (2020), ‘The Commission’s obligation to refuse an ‘adequacy decision’ to the United Kingdom due to inadequacy of enforcement of personal data protection in that jurisdiction’, *Irish Council for Civil Liberties*, [<https://www.euractiv.com/wp-content/uploads/sites/2/2020/10/Letter-Brexit-Commission-data-ICO-12Oct2020.pdf>], p. 1.

3.5 Legal Basis for Behavioural Tracking: Why it Never Hurts to Ask²⁸⁶

Article 6(1) GDPR establishes six possible legal bases that may be used to justify personal data processing. These are, in summary: consent, necessity in the performance of a contract, necessity in the compliance with a legal obligation, necessity in the protection of vital interests, necessity in the performance of a task in the public interest, and necessity for the purposes of a controller's legitimate interests. Of these, the bases most relevant for RTB are contractual performance, consent, and legitimate interests.

3.5.1 Contractual Performance

Article 6(1)(b) GDPR establishes the legal base of contractual performance, wherein 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. As far as this relates to behavioural advertising, it must be questioned when there exists a contract between the tracked data subject and when tracking is 'necessary' for the performance of this contract. In general, Zuiderveen Borgesius notes that contracts under private and international law only arise following explicit assent and that silence is not an acceptable indicator of contractual acceptance.²⁸⁷ Hence, online tracking by entities whose terms of service a data subject has not explicitly consented to (e.g., during the course of account creation) cannot be said to be done under contract just because the data subject accessed a given web page.

Even when a user has specifically contracted with a company, such as when creating an account, behavioural tracking is unlikely to ever be considered 'necessary' for the purposes of the contract. CJEU case law has established that 'necessity' is to be interpreted strictly when derogating from or limiting the fundamental right to data protection.²⁸⁸ Under this strict interpretation of necessity, the EDPB points out that data processing is very rarely essential for a contract's performance and is more often simply unilaterally imposed by controllers in their contracts.²⁸⁹ Hence, the EDPB rightly concludes that contractual

286 The general analytical direction of Section 3.5 is very much informed by Veale and Zuiderveen Borgesius (2021) pp. 13-20, particularly regarding the unsuitability of the contractual performance and legitimate interests legal bases. Reference: Veale, M. and Zuiderveen Borgesius, F.J. (2021), 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>].

287 Zuiderveen Borgesius, F.J. (2015), 'Personal data processing for behavioural targeting: which legal basis?', *International Data Privacy Law*, vol. 5, no. 3, p. 166.

288 CJEU Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy*, judgment of 16 December 2008, para. 56.

289 European Data Protection Board (2019), 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', p. 9.

necessity is not an appropriate legal basis for data processing related to behavioural advertising, since behavioural advertising is never the core product or service that a data subject requests, even if it aids the financing of another the requested goods or services.²⁹⁰

In sum, contractual performance should not be relied upon to justify the processing of behavioural data for targeted advertising.

3.5.2 Legitimate Interests

Another justification for data processing lies in Article 6(1)(f)'s basis of legitimate interests, where 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.' As stated, legitimate interests may only be relied upon to justify personal data processing where they are not outweighed by the rights and freedoms of the data subject. Recital 47 GDPR further specifies that a key element in the balancing act between the interests of the data subject and the data controller are the '*reasonable expectations of data subjects based on their relationship with the controller*'.²⁹¹ Furthermore, the CJEU's ruling in *Fashion ID* establishes that where there exists joint data controllership in regard to a data processing operation, each joint controller must define and assess their own legitimate interest separately.²⁹²

The CJEU established a three-stage test of legitimate interests in *Fashion ID*.²⁹³ Step 1 involves the determination of a legitimate interest to be pursued; step 2 involves demonstrating that the legitimate interest strictly necessitates the processing of personal data; and step 3 involves balancing the legitimate interests and relevant data processing operations against any fundamental rights or freedoms of the data subject that may take precedence. This formulation is similar to a classic test of proportionality in other areas of EU law, which is not surprising since the legal basis of legitimate interests involves a balancing act between the rights of data subjects and the interests of data controllers.

Applying the requirements for the basis of legitimate interests to behavioural advertising, the first question is what legitimate purpose a publisher or vendor is pursuing in tracking users and sharing their data via RTB. Most RTB actors may

290 Ibid., p. 14.

291 Emphasis added.

292 CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, para. 96.

293 Ibid., para. 95.

point to specific legitimate interests, such as carrying out direct marketing (specifically provided for under Recital 47 GDPR). Others go further, notably claiming that their role in targeted behavioural advertising is in furtherance of maintaining a free and openly accessible online environment that would not be possible without ad revenue.²⁹⁴ This latter claim seems to overstate the noble intentions of adtech companies but, even if it were entirely true, it would still flounder alongside the legitimate interest of direct marketing under a consideration of strict necessity.

The second step of the CJEU's test requires us to consider whether the personal data processing currently employed by RTB actors is strictly necessary for the achievement of these objectives, where strict necessity also requires that there is no less-intrusive alternative available in achieving one's objectives.²⁹⁵ In terms of marketing modalities, there certainly exist alternatives to behavioural targeting that do not rely on the collection of detailed personal data. Contextual advertising, with the aid of machine learning and artificial intelligence technologies mentioned in Section 2.1, is once again a viable approach to marketing. As demonstrated by Nederlandse Publieke Omroep, the Dutch public broadcaster, a switch from behavioural to contextual advertisements in 2020 resulted in comparable or even more effective audience conversion rates.²⁹⁶ Contextual advertisement's effectiveness is further confirmed by studies from private firms showing its increased cost efficiency compared to behavioural targeting.²⁹⁷ The legitimate interest of keeping the web open and accessible via successful advertising activity is, therefore, conceivably achievable through less-intrusive contextual advertisements. If such more privacy-preserving alternatives to behavioural tracking are available and demonstrably efficient in their newest case studies, adtech actors cannot claim that behavioural tracking and targeting practices are necessary in achieving their legitimate interests.

In regard to step 3 of the CJEU's test for legitimate interests, the balancing of interests, we must begin by recalling the prism of reasonable expectations based on the data subject–controller relationship provided for under Recital 47 GDPR.

294 Forbrukerrådet (2020), 'Out of Control: How consumers are exploited by the online advertising industry', [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 176.

295 Kotschy, W. (2020), 'Article 6: Lawfulness of processing', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 321, 338.

296 Ster (2020), 'A Future Without Advertising Cookies?', [https://www.ster.nl/media/h5ehvtx3/ster_a-future-without-advertising-cookies.pdf], p. 11.

297 GumGum HQ (2020), 'Understanding Contextual Relevance and Efficiency', *dentsu*, [<https://insights.gumgum.com/hubfs/DAN%20Research%20Study/GumGum%20Contextual%20Research%20Paper-1.pdf>].

We must also recall that reliance solely on first-party data is an extreme outlier in the modern targeted advertising industry. The previously mentioned statistic that only 2.5% of data-collecting websites rely exclusively on first-party fingerprinting²⁹⁸ is illustrative. Consequently, the data subject has no direct relationship with the majority of entities processing its personal data within the RTB ecosystem. Narayanan et al. point out that, due to the tangled web of RTB participants and fourth-party dynamics, it is often the case that not even the publisher has a direct relationship with the vendors that deploy particularly privacy-invasive tracking on their web pages, introducing an additional degree of opacity between data subject and tracker.²⁹⁹ Finally, a data subject cannot predict precisely which third-party trackers will be loaded during any given page visit, since ad networks' partners constantly fluctuate.³⁰⁰ All of this is to say that the opaque nature of the RTB environment makes it not just unlikely, but outright impossible for the data subject to have a direct relationship with a tracking partner who is not the publisher.

As to data subjects' expectations regarding online privacy, the European Court of Human Rights has established that the concept of 'private life' under Article 8 of the European Convention on Human Rights (ECHR)³⁰¹ extends to the online sphere and that individuals are entitled to a reasonable expectation of privacy, an expectation that is only strengthened when they have not created an account or provided contact data.³⁰² Indeed, besides unique first-party identifiers, most online tracking technologies do not at all rely on the user registering or providing contact details. Additionally, following Apple's recent shift to opt-in app tracking in iOS 14.5, statistics show that 96% of users in the US had chosen to opt out.³⁰³ While preference is not the same as expectation, it still reflects users' views of how things 'should be' in regard to their online activities. In sum, it is evident that data subjects should not reasonably expect to be tracked

298 Al-Fannah, N.M., Li, W., and Mitchell, C.J. (2019), 'Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking', *Proceedings of the 21st International Conference on Information Security*, p. 489.

299 Engelhardt, S., Acar, G., and Narayanan, A. (2018), 'Website operators are in the dark about privacy violations by third-party scripts', *Freedom to Tinker* via Princeton University, [<https://freedom-to-tinker.com/2018/01/12/website-operators-are-in-the-dark-about-privacy-violations-by-third-party-scripts/>].

300 Urban, T. et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the '20 World Wide Web Conference*, p. 1284.

301 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 1950, ETS 5.

302 ECtHR Case 62357/14, *Case of Benedik v. Slovenia*, judgment of 24 April 2018, paras. 116-117.

303 Axon, S. (2021), '96% of US users opt out of app tracking in iOS 14.5, analytics find', *Ars Technica*, [<https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/>].

during their private internet activities, especially when this tracking is carried out by RTB actors with whom they have neither a relationship, nor even direct knowledge.

Taking into account the lack of a relationship between the data subject and most data controllers in the RTB ecosystem, the reasonable expectation of data subjects for privacy on the internet, and the fact that the right to personal data protection is a fundamental right under Union law,³⁰⁴ it is almost impossible to argue that ‘legitimate interests’ is a compelling legal basis for behavioural tracking online. Numerous national DPAs have adopted this view, including the Norwegian³⁰⁵ and British³⁰⁶ agencies. The A29WP and the EDPB have also stated several times that legitimate interests would not be a valid lawful basis for ‘intrusive profiling and tracking practices for marketing and advertising purposes’ and that consent should be used instead.³⁰⁷

Yet, there is a reason that the inadequacy of legitimate interests for online behavioural tracking must still be pointed out: the continued practice of advertisers relying on this basis for processing users’ data. In May 2020, Matte et al. found that, out of roughly 650 advertisers registered with the IAB’s TCF, 175 still rely on the basis of legitimate interests to create a personalized ads profile and 199 do so to create a personalised content profile.³⁰⁸ Considering that advertisers who have made the effort to register with the IAB’s framework, as a group, are more likely to be engaged with problems of transparency and consent than advertisers who have not registered with the TCF, the ratio of advertisers using legitimate interests for behavioural tracking ‘in the wild’ may be even higher. Therefore, RTB vendors who rely on an inappropriate legal basis constitute a significant compliance issue for the GDPR’s data protection regime. This compliance issue is not a mere formality, since data controllers would have significantly different obligations towards data subjects if they operated under the umbrella of consent as a legal basis, as the following Section 3.5.3 demonstrates.

304 Recital 1 GDPR.

305 Forbrukerrådet (2020), ‘Out of Control: How consumers are exploited by the online advertising industry’, [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>], p. 177.

306 ICO (2019), ‘Update report into adtech and real time bidding’, [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>], p. 18.

307 European Data Protection Board (2021), ‘Guidelines 8/2020 on the targeting of social media users’, para. 56.

308 Matte, C., Santos, C., and Bielova, N. (2020), ‘Purposes in IAB Europe’s TCF: which legal basis and how are they used by advertisers?’, *Annual Privacy Forum 2020*, p. 178.

3.5.3 Consent

As already mentioned, the EDPB considers consent necessary for data processing that involves tracking individuals across multiple websites, locations, devices, services, or data-brokering.³⁰⁹ Consent is a powerful legitimizing force – it is a reflection of the principle of informational self-determination that first arose in the context of German data protection in 1983 and subsequently informed the European supranational data protection regime.³¹⁰ Through consent, data subjects may exercise a measure of autonomy from the paternalistic confines of data protection law and decide for themselves what data processing they wish to be subjected to. As such, consent may easily legitimize even data processing activities that track or profile users, which are otherwise seen as infringing on an individual's privacy.

However, due to the potency of consent as a legal basis for processing, the GDPR has instituted strict requirements regarding the quality of consent and the data subject rights that flow from consent. Recital 32 GDPR stipulates that consent must be 'given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her'. Recital 32 further notes that 'silence, pre-ticked boxes or inactivity' do not meet the threshold of a 'clear affirmative act'. Moreover, Recital 32 establishes that consent requested through electronic means must be 'clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'. Besides consent itself having to be freely given, specific, informed, and unambiguous per Article 4(11) GDPR and the largely overlapping definition under Recital 32, Article 7 GDPR establishes that choosing consent as a legal basis for processing activates several subsequent rights and obligations. These include:

- the obligation of a controller to demonstrate the data subject's consent under Article 7(1) GDPR;
- the obligation that the request for consent is presented 'in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language' under Article 7(2) GDPR;
- the provision that data subjects have the right to withdraw consent at any time, just as easily as they have given it, and the obligation of data processors to inform subjects of this right prior to consent being given, all under Article 7(3) GDPR;

309 Article 29 Data Protection Working Party (2018), 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', p. 15.

310 van Casteren, D.C.J. (2017), *Consent now and then*, LLM diss., Tilburg University, p. 40.

- a stipulation under Article 7(4) GDPR that consent cannot be freely given if the performance of a contract is conditional on consenting to personal data processing that is not necessary for that contract's performance.

Overall, consent under the GDPR is subject to strict and extensive requirements. Unfortunately, the prevailing practices of the behavioural targeting industry when it comes to securing consent are largely inadequate in meeting these requirements.

3.6 Requirements for Consent under the GDPR

3.6.1 Freely Given Consent

Consent under the GDPR must be freely given by the data subject. The EDPB notes that 'if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid'.³¹¹ As stated in Article 7(4) GDPR, it is untenable to claim that consent has been freely given while simultaneously bundling a contract with consent to personal data processing that is not necessary for the contract's performance. Furthermore, the requirement that the data subject's freedom of choice must be 'real' rather than only *pro forma* has been reflected in CJEU jurisprudence, specifically in the *Orange România case*, where 'genuine freedom of choice' was established as a precondition for freely given consent.³¹² Hence, the determination of freely given consent relies on *de facto* consideration of whether a data subject was constrained, unduly influenced, or otherwise obstructed in the exercise of free will rather than on a simply formalistic analysis of whether some sort of choice was presented to the data subject.

To date, much regulatory attention has centred around so-called 'cookie walls', which restrict website functionality or accessibility, in whole or in part, unless a user consents to non-essential tracking cookies first. Pursuant to GDPR Articles 4(11) and Article 7(4), the EDPB's Guidelines on Consent and a variety of national DPAs have pointed out the inadequacy of these 'take-it-or-leave-it' cookie walls in obtaining freely given consent.³¹³ Nevertheless, cookie walls con-

311 European Data Protection Board (2020), 'Guidelines 05/2020 on consent under Regulation 2016/679', para. 13.

312 CJEU Case C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, judgment of 11 November 2020, para. 41.

313 European Data Protection Board (2020), 'Guidelines 05/2020 on consent under Regulation 2016/679', para. 39; Santos, C., Bielova, N., and Matte, C. (2020), 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *Technology and Regulation 2020*, p. 104, Table 9.

tinue to be a compliance hurdle in the wild, although their relative incidence in popular EU websites is expected to be significantly less than 7% since 2018.³¹⁴

Cookie walls are far from the only challenge to freely-given consent, however. A related, yet much more widespread and legally-indeterminate phenomenon is that of dark patterns in consent collection mechanisms. Dark patterns are defined as ‘interface designs that try to guide end users into desired behaviour through malicious interaction flows’.³¹⁵ They are an emanation of ‘nudging’ practices, where inherent human psychological biases are leveraged to guide human behaviour without explicitly overriding an individual’s freedom of choice. In other words, dark patterns are a set of psychological manipulation techniques. In everyday life, these techniques may come in dozens of different forms of varying ethicality, from the common and normalized practice of ‘psychological pricing’, where prices are set at just below a round number to appear cheaper than they really are, to outright deceptive practices such as fake countdown timers and declarations of limited exclusivity.³¹⁶

In regard to web advertising and behavioural tracking under the GDPR, dark patterns are most relevant to the collection of consent for user tracking. Frequently, the request for consent is designed in such a way that the option to give consent is more visible, more attractive, or easier for the user to select and submit. The next page shows two online consent requests, retrieved from the desktop versions of healthline.com and theguardian.com, which serve as a case study for the typical obstacles to freely given consent posed by dark patterns and cookie walls.

314 Utz et al. found that only 7% of consent banners blocked interaction with the website before a choice regarding consent was made and, of these, it is likely that many allow rejection of tracking cookies. Reference: Utz, C. et al. (2019), ‘(Un)informed Consent: Studying GDPR Consent Notices in the Field’, *ACM Conference on Computer and Communications Security* ‘19, p. 976, Table 1.

315 Nouwens, M. et al. (2020), ‘Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 3.

316 Narayanan, A. et al. (2020), ‘Dark Patterns: Past, Present, and Future. The evolution of tricky user interfaces’, *Communications of the ACM*, vol. 63, no. 9, pp. 42-47.

Please accept our privacy terms

You can change your preferences at any time by clicking on "Privacy Settings" in the footer at the bottom of the page.

We believe that trustworthy health information should be free to everyone and we rely on advertising to make that possible. Providing authoritative experiences that are reviewed by physicians and other health and wellness professionals is expensive, but it's an invaluable service. We collect and securely process your personal data to deliver a relevant experience and support our business, so we ask that you allow cookies in order to access all of our content and features.

We and [our partners](#) process your personal data in the following ways:

- cookies or unique IDs, for storing and/or accessing information on your device
- personalized ads and content
- ad and content measurement
- audience insights and product development
- ensuring security, preventing fraud, and debug
- technically deliver ads or content

Your personal data use applies only while using Healthline Media Websites and Apps. Some of our partners do not ask for your consent to process your data and rely on their legitimate business interest. You can modify your setting or object by clicking on "Manage Settings."

At this time, we cannot provide the full site experience if you disallow any purposes, features, or partners. Instead, we will provide a version of our site that shows 10 of our most popular articles without ads, cookies, or tracking technologies.

ACCEPT AND CONTINUE TO SITE

MANAGE SETTINGS

Consent Banner 1: healthline.com

It's your choice

When we make the Guardian available to you online, we use cookies and similar technologies to help us to do this. Some are necessary to help our website work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways.

For instance, we and our [partners](#) use information about you, your devices and your online interactions with us to provide, analyse and improve our services. This includes personalising content or advertising for you.

We use cookies and similar technologies for the following purposes:

- ✓ Store and/or access information on a device
- ✓ Personalised ads and content, ad and content measurement, audience insights and product development

You can find out more in our [privacy policy](#) and [cookie policy](#), and manage the choices available to you at any time by going to 'Privacy settings' at the bottom of any page.

Are you happy to accept cookies?

To manage your cookie choices now, including how to opt out where our partners rely on legitimate interests to use your information, [click on Manage my cookies](#).

Yes, I'm happy

Manage my cookies

Consent Banner 2: theguardian.com

Dark Pattern 1: Unequal Visibility In both examples, the button to consent to tracking cookies is more saturated and visible, whereas the option that leads to rejecting cookies is desaturated, blends in with the background colour, and, in the Healthline example, even lacks a fill colour. The increased relative visibility of affirmative consent buttons focuses the attention of users, inclining them towards accepting cookies and disinclining them from their other options.

Dark Pattern 2: Manipulative Language In the case of The Guardian's consent banner, the phrasing of 'Yes, I'm happy' is in itself problematic due to its wording. It couples positive, emotionally affective statements with its consent button, while the cookie rejection button remains impartial and matter-of-fact in tone. Clicking 'I'm happy' reinforces the data subject's own positive state of mind and is, therefore, a much more attractive option than the more drily-worded alternative.

Dark Pattern 3: Unequal Ease of Choices A further example of dark patterns is found in both of the above consent popups, where both make it more difficult for the user to reject cookies than to accept them. A blanket acceptance of cookies requires only one click on the first layer of each popup, while there is no equivalent option of immediate blanket rejection. Rather, users are forced to enter a separate submenu where they may reject tracking cookies. Users seeking a fast and convenient browsing experience are naturally more inclined to accept tracking cookies rather than to browse submenus. A 2020 study by Nouwens et al. found that this type of dark pattern is pervasive, with only 12.6% of studied websites having a 'reject all cookies' button that is as easy to access as the 'accept all cookies' button.³¹⁷

A Torpedo of Free Consent: Cookie Wall and Gating of Functionality The final relevant issue is found in Healthline's cookie request, wherein full access to the site's articles is available only to those users who consent to advertising cookies. Those who reject advertising cookies are only able to browse a curated list of 10 articles at any time due to financial considerations on the part of Healthline. The request for consent itself is delivered in the form of a popup, making it impossible for users to legitimately access the site without consenting to cookies in the popup. This is essentially a cookie wall, masquerading as a consent banner that gives a user the illusion of choice in accepting or rejecting tracking cookies or specific adtech partners, since doing so blocks access to the full site. A closer inspection of Healthline's settings page also reveals that many

317 Nouwens, M. et al. (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 5.

of the partners even rely on the legal basis of legitimate interests for purposes such as the creation of personalized ad profiles, which this report has already pointed out to be inappropriate.

The above dark patterns and cookie walls are representative of the everyday manipulations that a typical data subject may be exposed to on the internet. Their compliance with the GDPR has so far not been considered by the CJEU, yet national DPAs and various advisory bodies have found many of these practices irreconcilable with the notion of freely given consent.

3.6.2 Freely Given Consent and Dark Patterns

Manipulation is frequently described as influence that subverts rational deliberation.³¹⁸ Legal philosopher Joseph Raz recognized that ‘manipulation, unlike coercion, does not interfere with a person’s options. Instead, it perverts the way that person reaches decisions, forms preference, or adopts goals’.³¹⁹ With this definition in mind, the dark patterns that this report has described, the ones that are most frequently used in the procurement of consent for behavioural tracking, are most certainly manipulative. Trackers implementing dark patterns expect to extract consent not because the dark patterns deliver an impartial choice or rational argument to the user, but rather because the affirmative option is brighter and more visible, magnetic through its affective language, or simply less of a hassle for the user to find and select. None of these considerations are rationally relevant to the user’s choice of giving or withholding consent, rendering their influence on the user’s decision a manipulative one.

Yet, manipulation *per se* is not expressly forbidden under the GDPR’s Articles or Recitals relating to consent and the EDPB’s Guidelines on Consent are likewise silent, focusing instead on ‘deception, intimidation, coercion, or significant negative consequences’ when analysing freely given consent.³²⁰ Therefore, the mere fact that dark patterns are manipulative is not sufficient to find that their employment precludes freely given consent. It is also difficult to pinpoint the precise moment when a manipulation becomes so onerous that it renders a data subject’s free will moot. Yet, that precise moment is not relevant in the case of dark patterns in consent mechanisms – several studies have demonstrated that the three dark patterns described above not just influence, but wholly direct data subject choices regarding online tracking.

318 Noggle, R. (2020), ‘The Ethics of Manipulation’, in Zalta, E.N. (ed.), *The Stanford Encyclopedia of Philosophy*, [<https://plato.stanford.edu/entries/ethics-manipulation/>].

319 Raz, J. (1988), *The Morality of Freedom*, Oxford University Press, p. 377.

320 European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’, para. 47.

Graßl et al. found that 93.8% of users ($N = 228$) agreed to tracking when their consent banners employed dark patterns such as aesthetic manipulation (relating to unequal visibility), obstruction of one option (relating to unequal ease of choice), or pre-ticked selections.³²¹ When these patterns were reversed in the other direction (favouring the privacy-friendly options), only 53.2% of people ($N = 255$) still consented to being tracked. Notably, the authors also suspected the existence of a phenomenon known as ‘event survival’, where continued conditioning via dark patterns resulted in users establishing behavioural routines that saw them automatically consent to cookies even after the removal of dark patterns.³²²

Nouwens et al. found that removing the ‘reject all’ option from the first layer of consent banners increased the rate at which users consent to tracking cookies by 22-23 percentage points ($N = 40$).³²³

Finally, Utz et al. established that consent notices asking users to check or uncheck specific categories of cookies (necessary vs analytics, marketing, etc.) had a drastically lower acceptance rate than other types of consent notices.³²⁴ Based on a sample of 36,395 participants, the researchers found that desktop users faced with a simple binary accept/reject option ignored the consent banner 66-68% of the time and accepted the tracking cookies 20% of the time in both the nudging and non-nudging conditions. In the case of desktop consent notices asking to select categories of cookies, pre-checked selections elicited an ignore rate of 82.5% and an acceptance rate of 11.9%. In the case where selections were not pre-checked, the ignore rate of consent notices remained at 83.7% while the blanket acceptance rate fell to zero and partial acceptance of cookies hovered below 1%. Therefore, the authors claim that an implementation of data protection by default and purpose-based consent design principles would lead to less than 0.1% of users consenting to third-party cookies.³²⁵

There are several takeaways from the body of literature available regarding dark patterns. The most immediate of these is that users are somewhat indolent when it comes to choices regarding online tracking. One possible explanation for this

321 Graßl, P. (2021), ‘Dark and Bright Patterns in Cookie Consent Requests’, *Journal of Digital Social Research*, vol. 3, no. 1, p. 12.

322 Ibid., p. 24.

323 Nouwens, M. et al. (2020), ‘Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 8.

324 Utz, C. et al. (2019), ‘(Un)informed Consent: Studying GDPR Consent Notices in the Field’, *ACM Conference on Computer and Communications Security* ‘19, p. 981.

325 Ibid., p. 986.

behaviour may be what is known in behavioural economics as the ‘default bias’: the tendency for people to accept pre-set courses of action. When dark patterns manipulate a choice’s visibility or phrasing so that it appears as the ‘default’ choice, this may exert a powerful effect on user behaviour. Indeed, quantitative studies have demonstrated how the default effect is one of the most powerful ‘nudges’ available.³²⁶ Another cause of this consent indolence is likely what the EDPB refers to as ‘click fatigue’ – a progressive wearing down of the warning effect of consent notices as users become saturated with such notices.³²⁷ Yet, whatever the cause, the consequence of consent indolence is that users absent-mindedly choose the options that are most visible, easiest to pick, or simply the ones that they have been conditioned to select.

With this in mind, dark patterns that hinder the ease of choice (e.g., by hiding options in submenus) have been convincingly shown to have a decisive influence on the decision-making of users and should therefore be seen as precluding freely-given consent. On the other hand, dark patterns that deal with the simple highlighting and visibility manipulation of buttons have not been firmly shown as decisive determinants of user behaviour. This may or may not be due to event survival and similar psychological conditioning. Yet, there is a separate legal rationale that may render dark patterns around button visibility noncompliant with the GDPR: the logic of the *Planet49* case before the CJEU regarding pre-selected boxes and its interpretation by the German regional court of Rostock in the national *Advocado* case.

In *Planet49*, the CJEU ruled that preselected checkboxes in consent notices are incapable of securing active or informed consent.³²⁸ The Court considered that there was no active element in abiding by a pre-selected checkbox, nor was there any guarantee that abiding by said checkbox meant that a user had noticed it or informed themselves regarding the terms attached to the checkbox. Based on that logic, the German Landgericht Rostock in the *Advocado* case remarked that a consent notice in which one option is highlighted and more visible to the user, causing the other option to take a back seat, leads the user to perceive the high-

326 Hummel, D. and Maedche, A. (2019), ‘How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies’, *Journal of Behavioral and Experimental Economics*, vol. 80, pp. 47-58.

327 European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’, para. 87.

328 CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, judgment of 1 October 2019, paras. 52 and 55.

lighted option as a pre-selected choice.³²⁹ According to the German court, the less visible option is therefore unlikely to be perceived as an equivalent consent option by many consumers.³³⁰

This logic is a neat fit with the generally user-centric approach of the GDPR in evaluating valid consent. Since the user is the person who decides on whether to provide consent to data processing, the user's subjective perception of their own choice comes to define their behaviour in reality. Thus, even if the mere highlighting of one option is not functionally equivalent to pre-selection, in that no consent is presumed or registered in a system configuration before a choice is made by the data subject, a highlighted option leaves the data subject with an impression, whether conscious or not, that the choice has been made for them and that going counter to that choice is the exception to the rule. In short, visual dark patterns are reasonably likely to restrict agency in data subjects' decision-making by framing their consent as a default assumption. As already mentioned, the default bias is a powerful psychological drive whose elicitation compromises an individual's genuine freedom of choice.

The takeaway from this state of affairs is that a major portion of data subjects' consent to online behavioural tracking has not been freely given due to the employment of various dark patterns, rendering this consent invalid under Article 4(11) GDPR and, therefore, unsuitable as a legal basis for data processing. The precise incidence of such invalid consent has not been determined, but considering that only 12.6% of consent banners queried by Nouwens et al. even have a 'reject all' option in the same layer as the 'accept all' option,³³¹ and that, of those 12.6%, a great many are likely to employ some sort of visual dark patterns in their framing of choices, it is evident that the online behavioural tracking industry is in systemic violation of the GDPR's requirements regarding freely-given consent.

While several national DPAs have issued guidance stating that nudging and dark pattern practices are incompatible with the GDPR's standards on consent, including the French, Danish, UK, Greek, and Irish DPAs,³³² it is possible that

329 Landgericht Rostock Case 3 O 762/19, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV gegen advocado GmbH*, judgment of 15 September 2020, p. 22.

330 *Ibid.*, p. 22.

331 Nouwens, M. et al. (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 5.

332 Santos, C., Bielova, N., and Matte, C. (2020), 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *Technology and Regulation 2020*, p. 117, Table 16.

the Union's courts may soon rule on the matter. The NGO Noyb has begun sending hundreds of GDPR complaints relating, *inter alia*, to dark patterns and other insufficiencies in cookie consent notices, and it is not unreasonable to assume that some of these complaints may be escalated to the courts.³³³

3.6.3 Freely Given Consent and Cookie Walls

In regard to the practice of gating functionality solely behind tracking walls, it has already been pointed out that the majority of advisory and regulatory bodies consider this gating to be noncompliant with the GDPR, including the EDPB, the European Data Protection Supervisor (EDPS), and the Dutch, French,³³⁴ German, Danish, Greek, Irish, Belgian, Austrian, and Spanish DPAs.³³⁵ However, this stance does not mean that all internet publications must be wholly free to access. Rather, a growing number of regulatory and advisory bodies seem to favour the notion that offering a choice between a free experience with tracking and an 'equivalent' (possibly paid) experience with no tracking is an acceptably open choice for data subjects that allows for their consent to be freely given.

In 2018, the Austrian DPA decided that the Austrian newspaper Der Standard was justified in offering three options for site access: a free option with tracking cookies and full site functionality, a free option with no cookies but limited site functionality, and a paid version with a subscription fee of 6 euros a month and full site functionality.³³⁶ The Austrian DPA opined that there was sufficient freedom of choice between the free option with tracking cookies and the subscription option, especially considering that the subscription fee was not 'a disproportionately expensive alternative'.³³⁷ By the Austrian DPA's reasoning, pricing and affordability are relevant factors that may determine whether a data subject is truly able to make a free choice between the options and, therefore, to give valid consent. In 2019, the Dutch DPA published guidance on its website, stating that requesting payment from people who refuse tracking cookies is an accept-

333 Noyb (2021), 'noyb aims to end 'cookie banner terror' and issues more than 500 GDPR complaints', [<https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints>].

334 The CNIL's latest guidelines advocate for a case-by-case consideration of cookie walls due to a desire not to establish hard law (which is outside of the CNIL's competence), yet they also note that cookie walls are unlikely to be compliant *per se*. Reference: CNIL (2020), 'Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookieset autres traceurs»'.

335 Santos, C., Bielova, N., and Matte, C. (2020), 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *Technology and Regulation 2020*, p. 104, Table 9; AEPD (2020), 'Guía sobre el uso de las cookie'.

336 DSB (2018), 'GZ: DSB-D122.931/0003-DSB/2018'.

337 Ibid., p. 7.

able alternative to simply barring these people from accessing a given service due to their refusal.³³⁸ Even the EDPB's 2020 Guidelines on Consent consider there to be genuine choice where there is 'an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes'.³³⁹ This rationale is seemingly finding favour with the Council of the European Union. The Council's latest position adopted in regard to the upcoming *lex specialis* ePrivacy Regulation stipulates that cookie walls may permit free consent in instances where the user may choose between 'an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand'.³⁴⁰ In this passage, which mirrors the wording of the previously-quoted EDPB 2020 Guidelines, the meaning of the word 'equivalent' is not clarified further, but it may contextually be understood to refer to equivalence in terms of monetary value to the provider and in terms of functionality to the data subject. Provided that this is the intended interpretation, Recital 20aaaa of this ePrivacy Regulation draft may guide courts and regulators in concluding that it is possible to obtain valid consent from a user who is faced with a consent wall offering both a free option with tracking and a 'reasonably priced' paid alternative that represents a viable choice for the average customer.

In theory, such an approach is an appropriate solution that strikes a balance between fundamental rights and freedoms – the right of data subjects to personal data protection on one hand, and the freedom of individuals to conduct a business on the other.³⁴¹ In practice, however, it is unlikely that digital cookie-or-pay walls would ensure an ongoing high level of personal data protection. Scholarly studies point out that smaller publications such as local newspapers struggle to secure digital subscriptions,³⁴² with industry actors confirming that paid access 'usually only works for the very top tier of services and high-end publications'.³⁴³ A shift towards a cookie-or-pay model would either result in users restricting their browsing behaviour, congregating around the few large publications they feel comfortable paying for, and harming media plurality, or,

338 AP, 'Cookies', [<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies>].

339 European Data Protection Board (2020), 'Guidelines 05/2020 on consent under Regulation 2016/679', para. 37.

340 Recital 20aaaa, ePrivacy Regulation Proposal ST 6087/21, 2021.

341 Art. 16 EU Charter of Fundamental Rights.

342 Chyi, H.I. and Ng, Y.M.M. (2020), 'Still Unwilling to Pay: An Empirical Analysis of 50 U.S. Newspapers' Digital Subscription Results', *Digital Journalism*, vol. 8, no. 4, pp. 526-547.

343 KPMG (2019), 'CJEU: Users must give 'active consent' for cookies', [<https://web.archive.org/web/20210516185309/https://home.kpmg/be/en/home/insights/2019/11/ta-cjeu-users-must-give-active-consent-for-cookies.html>].

more likely, continuing to agree to being tracked by the myriad websites that they visit while feeling that subscribing to all of them is not a realistic proposition, resulting in the same broad surveillance and lack of freely-given consent that plagues the current digital landscape. The modern internet has been lauded by EU officials precisely by virtue of being ‘open and independent’, a ‘global, common resource’ offering ‘non-discriminatory access to knowledge’.³⁴⁴ Normatively speaking, fragmenting the online sphere into separate, paid walled-gardens would run precisely counter to the EU’s publicly stated vision for the internet. Moreover, a regulatory approach that readily advocates for widespread paid subscriptions as an ‘equivalent’ alternative to behavioural tracking technologies risks turning personal data protection into a privilege rather than a right, where only rich data subjects can afford a diverse internet browsing experience that does not involve the exposure of their personal data. At the same time, it is inane to expect private businesses to provide users with a free service.

This report proposes that the focus on cookie walls equates to an inability to see the forest for the trees. Tracking walls are a symptom of digital publishers’ over-reliance on behaviourally-targeted advertising and personal data processing. Rather than legislating the legal landscape into a corner where users and websites must choose between behavioural tracking or digital fragmentation, legislators may instead opt to recognize that current behavioural tracking and RTB practices are incompatible with the GDPR *per se* (for reasons made clear in Sections 3.5 – 3.9) and thereby steer the digital ecosystem back towards more privacy-friendly alternatives, such as the now-resurgent contextual advertising. In such a scenario, the choice facing users would not be between tracking and subscriptions, but rather between advertisements and subscriptions. The latter case does not lead to any significant compromise of fundamental rights and freedoms, be they tied to personal data protection or the freedom to conduct business.

3.6.4 Specific Consent

Per Article 4(11) GDPR, consent must be specific to a particular data processing operation. Recital 32 also indicates that a single instance of consent ‘should cover all processing activities carried out for the same purpose or purposes’. At first glance, this appears to indicate that the main thrust of the specificity criterion is purpose-oriented. This is further evidenced by the EDPB’s Guidelines on Consent, wherein specificity of consent is discussed almost entirely with regard

344 EU Directorate-General for Communications Networks (2017), Content and Technology, ‘Internet Governance Forum 2017: Joint Declaration from European Commissioner Mariya Gabriel and Members of the European Parliament’, [<https://digital-strategy.ec.europa.eu/en/news/internet-governance-forum-2017-joint-declaration-european-commissioner-mariya-gabriel-and-members>].

to the purpose limitation and purpose-specificity of data processing operations.³⁴⁵

In the adtech industry, the IAB is presently engaged with securing ‘global consent’ i.e., consent secured via a CMP that then shares and applies this consent across a variety of participating publishers for the same purpose.³⁴⁶ The Article 29 Working Party has previously opined that such a mechanism would be desirable, since it would lead to a lower number of consent requests for the average data subject over an extended period of time.³⁴⁷

Nevertheless, there are both legal and practical considerations that raise questions around the desirability of global consent sharing among behavioural tracking partners. Practically, consent sharing between publishers and CMPs is likely to magnify the detrimental effects of any improperly obtained or registered consent by one party. For example, if a single publisher unlawfully registers positive consent for behavioural tracking prior to a data subject’s acceptance of cookies or even following the data subject’s explicit rejection of cookies, this would usually be a problem localized to that publisher and any of their immediate joint controllers. However, if the same publisher or its CMP participates in the IAB’s TCF or another global consent mechanism, then any improperly registered consent is transmitted to other publishers, rendering them liable for data processing operations performed using improperly collected consent and promulgating the breach of personal data protection principles.³⁴⁸

This scenario is not a mere thought exercise: a 2020 study by Matte et al. found that, out of 126 queried websites setting a shared tracking cookie, 26 did not respect a user’s explicit consent and set the cookie anyway.³⁴⁹ With this in mind, another paper by the same group points out that a global consent system places a high burden on individual publishers, who have no way of constantly monitoring the consent collection practices of all other partners in the global consent

345 European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’, p. 14; IAB Europe (2021), ‘IAB Europe Transparency & Consent Framework Policies’, [https://iabeurope.eu/wp-content/uploads/2021/05/TCF_v2-0_PolicyVersion_2021-05-27-3.3.pdf], p. 8, para. 19(c).

346 IAB Europe, *ibid.*, p. 8, para. 19(c).

347 Article 29 Data Protection Working Party (2011), ‘Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising’, p. 11.

348 Santos, C., Bielova, N., and Matte, C. (2020), ‘Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners’, *Technology and Regulation* 2020, p. 128.

349 Matte, C., Bielova, N., and Santos, C. (2020), ‘Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework’, *2020 IEEE Symposium on Security and Privacy*, p. 802.

sharing scheme, yet are expected to invite significant legal risk by blindly trusting these partners' consent signals.³⁵⁰ It is for this reason that the authors justifiably consider this arrangement 'unsustainable',³⁵¹ and trade-associations representing media companies have sometimes decried the global consent scheme as a 'non-starter' that 'pushes all liability to the publisher'.³⁵²

Legally, Veale and Zuiderveen Borgesius point out that each publisher-tracker partnership constitutes a separate joint controllership arrangement and that a data subject's consent may be considered specific and informed in relation to the particular controllers in that arrangement.³⁵³ A data subject may not be willing to trust a different publisher or other joint controller under this scheme, yet the global purpose-specific consent cookie shared across an entire industry does not give the data subject the opportunity to discriminate. Veale and Zuiderveen Borgesius further point out that, under the rationale of global consent cookies, it is therefore possible to have joint controllership arrangements that do not even involve the original data controllers who established consent, which is essentially a legal 'Ship of Theseus conundrum' with negative implications for the privacy rights of data subjects.³⁵⁴

As already mentioned, the GDPR does not include within its specificity requirements any mention that consent is strictly controller-specific. However, prior proposals for the DPD at one point included such language, stating that a data subject's consent 'must relate to a particular data processing operation concerning the data subject carried out by a **particular** controller and for particular purposes'.³⁵⁵ The fact that this wording has since been removed indicates that legislators may have purposefully intended to allow for consent to be shared between controllers depending on the circumstances of the data processing arrangement. Both the current silence of operative EU law regarding consent

350 Santos, C., Bielova, N., and Matte, C. (2020), 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *Technology and Regulation 2020*, p. 128.

351 Ibid., p. 128.

352 Kint, J. (2018), 'Why the IAB GDPR Transparency and Consent Framework is a non-starter for publishers', *Digital Content Next*, [<https://digitalcontentnext.org/blog/2018/03/19/iab-gdpr-consent-framework-non-starter-publishers/>].

353 Veale, M. and Zuiderveen Borgesius, F.J. (2021), 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>], p. 27.

354 Ibid., p. 27.

355 Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(11): Consent', in Kuner, C., Bygrave, L.A., and Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, pp. 174, 183.

sharing and the outright endorsement of advisory bodies such as the EDPB indicate that consent sharing arrangements are not inherently unlawful.

Yet, CJEU jurisprudence and the recitals to the GDPR infer that the specificity criterion of consent is flexible, becoming broader or more restrictive depending on the nature and purpose of data processing operations being carried out. For example, Recital 33 GDPR concedes that the identification of a specific purpose is sometimes at odds with the conduct of effective scientific research, and therefore allows for personal data to be processed for scientific research based on less-specific consent relating to general ‘areas of research’ rather than specific purposes. Similarly, as pointed out by Veale and Zuiderveen Borgesius, the *Deutsche Telekom* case saw the CJEU and the Advocate General adopt a teleological approach when analysing the acceptability of transfer of consent between public directory providers under the ePrivacy directive.³⁵⁶ Since an overly strict standard of consent applied to the publication of public telephone directories would severely compromise a legitimate objective of an EU public service, specificity of consent was more broadly interpreted in order to reconcile it with the public policy objectives of other EU legal instruments and the transfer of consent between different public directory providers was permitted.³⁵⁷ Therefore, the specificity of data subject consent that must be secured in any given context depends on the objectives of data processing and the presence and weight of any countervailing interests.

As discussed in Section 3.5.2, the legitimate interests of a business seeking to conduct behavioural tracking and user profiling in the RTB ecosystem cannot not be seen as prevailing over or restricting a data subject’s fundamental right to personal data protection. Hence, it may yet be legally justified under EU law to impose a stricter standard of specificity of consent in the context of online behavioural tracking. Such a stricter standard would entail specificity of consent to both purposes of data processing and to controllers of data processing. As a result, the implementation of globally transmitted consent to behavioural tracking would be restricted in whole or in part. Perhaps, considering the particular problems of unreliably-registered global consent in the TCF ecosystem, it may be desirable for publishers to only transmit *negative* consent between each other,

356 Veale, M. and Zuiderveen Borgesius, F.J. (2021), ‘Adtech and Real-Time Bidding under European Data Protection Law’, *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>], p. 28; CJEU Case C-543/09, *Deutsche Telekom AG v Federal Republic of Germany*, Opinion of Advocate General Trstenjak, delivered on 17 February 2011, para. 126.

357 Opinion of Advocate General Trstenjak, *ibid.*, para. 125.

as this would neither risk diminishing the protection afforded to individual data subjects, nor would it risk inviting extra liability for publishers.³⁵⁸

3.6.5 Informed Consent

Pursuant to Article 4(11) GDPR, valid consent must be ‘informed’. The CJEU has established that the concept of an informed data subject requires, at minimum and *inter alia*, that the subject is made aware of ‘the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing.’³⁵⁹ In addition to these criteria, the EDPB also predicates ‘informed’ consent upon a conveyed right to withdraw consent, information about the use of data for automated decision-making where relevant under Article 22(c) GDPR, and any data transfer risks under Article 46 GDPR.³⁶⁰ Crucially, the mere provision of this information in itself is insufficient to guarantee that data subjects are informed. Rather, the manner and format in which this information is delivered is decisive in securing informed consent.

Since personal data protection law derives from and safeguards the fundamental rights of natural persons, its provisions take into account the subjective state of mind of an ‘average European consumer who is reasonably well informed and reasonably observant and circumspect’³⁶¹ in order to ensure that individuals are afforded an appropriate level of protection. In regard to informed consent, the subjective requirements of the GDPR dictate that the provided information must be in an ‘intelligible and easily accessible form, using clear and plain language’ and must ‘enable the data subject to be able to determine easily the consequences of any consent’.³⁶² Article 12 GDPR specifically requires that communications to the data subject are delivered in a “concise, transparent, intelligible, and easily accessible form, using clear and plain language”.³⁶³ As Veale and Zuiderveen Borgesius point out, the GDPR’s standard of informed consent is less a standard of formalistic, technical notification and more a standard of conscious

358 Santos, C., Bielova, N., and Matte, C. (2020), ‘Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners’, *Technology and Regulation* 2020, p. 128.

359 CJEU Case C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, judgment of 11 November 2020, para. 40.

360 European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’, para. 64.

361 CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, Opinion of Advocate General Szpunar, delivered on 21 March 2019, para. 113.

362 CJEU Case C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, judgment of 11 November 2020, para. 40.

363 Art. 12 GDPR.

enlightenment.³⁶⁴ All of this is to say that the information unloaded unto a data subject may be incomprehensible and, therefore, insufficient for informed consent for a variety of reasons.

One cause for incomprehensibility may be the format or language of the provided information. Entities seeking consent for behavioural tracking must therefore ensure that relevant information is not just plainly and clearly phrased, but also easily obtainable from a single source with a small number of clicks from a central information portal. For example, several national DPAs have found that Google, at various points in time, provided its users with information that was either too ambiguous or too disparately disseminated across a variety of documents, precluding adequately informed consent.³⁶⁵ Yet, ultimately, it is possible to structure and phrase information in an accessible, jargon-free, and GDPR-compliant manner by adhering to guidelines such as those of the EDPB.³⁶⁶

Yet, a fundamental issue with informed consent to behavioural tracking does not so much concern the style of information provided to a user, but rather the magnitude of its substance. Open RTB auctions involve hundreds of partners across both the supply and demand sides. Per Nouwens et al., CMPs asked users to provide consent to data processing by a median of 315 trackers and a maximum of 542 trackers in the case of the popular QuantCast platform.³⁶⁷ As of June 2021, the IAB's TCF 2.0 vendor list includes a total of 745 participating entries.³⁶⁸ Of the canvassed sites, 76.47% offered descriptions of each vendor with a mean combined length of 7,985 words, but reading these descriptions would take more than 30 minutes per website for the average reader.³⁶⁹

Furthermore, even though a user who reads the myriad vendor descriptions in a CMP may understand the purposes, types, and modalities of data collection by

364 Veale, M. and Zuiderveen Borgesius, F.J. (2021), 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>], p. 28.

365 AP (2013), 'Onderzoek CBP naar het combineren van persoonsgegevens door Google. Rapport definitieve bevindingen', pp. 68-70; CNIL (2019), 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC', para. 145.

366 European Data Protection Board (2020), 'Guidelines 05/2020 on consent under Regulation 2016/679', paras. 66-72.

367 Nouwens, M. et al. (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 6.

368 IAB Europe, 'Vendor List TCF v2.0', [<https://iabeuropa.eu/vendor-list-tcf-v2-0/>].

369 Nouwens, M. et al. (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 6.

each vendor, they would still need to read each of these vendors' individual privacy policies to familiarize themselves with any consequent data sharing ('syncing') or other post-impression processing performed by these third parties. Additional actions and user familiarization may also be needed in regard to any vendors who are implemented on a website, yet are not part of any regulated framework such as the TCF.³⁷⁰ As pointed out by both detractors³⁷¹ and defenders³⁷² of the TCF, neither the TCF nor the RTB architecture itself has built-in technical safeguards against further processing or dissemination of personal data by third parties, relying instead on the lawful conduct of individual vendors to justify or arrest such activities as the circumstances warrant. This state of affairs, coupled with the pervasive syncing habits of data brokers and DSPs affecting the 'totality of internet users',³⁷³ means that a data subject cannot assuredly be in control of their personal data flow unless they either read the vendor list and individual privacy policies of nearly every single entity in the RTB ecosystem or make the conscious effort to reject every single tracking request they receive.³⁷⁴

As a result of the RTB ecosystem's multiplicity of actors and opaque functioning, it seems that data subjects are faced with an inherent information overload. In the *Planet49* case, Advocate General Szpunar recognizes that cookies are typified by 'technical complexity', 'asymmetrical information between provider and user', and 'the lack of knowledge of any average internet user', and concludes that 'the average internet user cannot be expected to have a high level of knowledge of the operation of cookies'.³⁷⁵ Regardless of how eloquent and plainly-put a cookie consent banner is, the unknowledgeable average internet user would still have to familiarize themselves with hundreds of joint controllers, their respective privacy policies and fourth-party partners, and the general concept of RTB auctions and cookie syncing, all just to have a sufficient grasp of their

370 ICO (2019), 'Update report into adtech and real time bidding', [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>], p. 19.

371 Ryan, J. (2018), 'Report from Dr Johnny Ryan – Behavioural advertising and personal data', *Brave*, [<https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf>], p. 6.

372 Kapur, S. and Savare, M. (2018), 'Fear of Brave? An Analysis of GDPR Challenges to Behavioral Advertising', *Lowenstein Sandler*, [<https://www.lowenstein.com/media/4692/20181113-tech-group-an-analysis-of-gdpr-challenges-to-behavioral-advertising.pdf>], p. 4.

373 Papadopoulos, P., Kourtellis, N., and Markatos, E. (2019), 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask', *Proceedings of the '19 World Wide Web Conference*, p. 1437.

374 van de Waerdt, P.J. (2020), 'Information asymmetries: recognizing the limits of the GDPR on the data-driven market', *Computer Law and Security Review*, vol. 38, Article Number 105436, p. 14.

375 CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, Opinion of Advocate General Szpunar, delivered on 21 March 2019, para. 114.

data choices and make an ‘informed’ choice. The GDPR’s standards of informed consent are easily attainable by companies who are not ‘fundamentally driven by the collection, analysis and monetization of personal data’,³⁷⁶ yet online behavioural advertising creates an environment where information obligations may be fulfilled *pro forma* but customers may be left overwhelmed and *de facto* incapable of informational self-determination. In other words, their informed consent would be precluded.

It is questionable whether such an industry arrangement is fair towards data subjects. Individuals may be expected to shoulder certain reasonable burdens or tolerate legal derogations in the name of a prevailing public interest. Yet, behaviourally targeted advertising is a purely profit-driven industry that places an extraordinary onus on data subjects simply to maintain control over their personal data flows. Recital 7 GDPR, *vis-à-vis* Recital 6 GDPR, explicitly establishes that the Regulation’s goal is ensuring the continued control of natural persons over their own data *in spite* of the unprecedented scale of modern data collection and sharing practices. A corollary to this goal is that, *ceteris paribus*, the interests of data subjects, insofar as they embody a fundamental right, should take precedence over an industry’s commercial practices. Therefore, if the basic open-ended and multitudinous structure of the behavioural advertising industry imposes informational overload on data subjects, then the industry must alter its structure lest it preclude being able to obtain informed consent.

While an exact solution for the behavioural advertising industry is far beyond the scope and ability of this report, it appears that simply shrinking the number of third-party actors (and, therefore, tracking partners) may be insufficient by itself. Doing so raises certain concerns regarding competition law³⁷⁷ and the centralization of power by large tech corporations who already oversee the most valuable troves of first-party data.³⁷⁸ Rather, the shift from third-party cookies to first-party data may serve as a precipitant for a general reorientation towards a more privacy-friendly advertising alternative, e.g., contextual advertisements.

3.6.6 Unambiguous Consent

As already explained in Section 3.5.3 of this report, Recital 32 GDPR requires a data subject’s consent to be provided via a ‘clear and affirmative act establishing [...] unambiguous indication of the data subject’s agreement’. In practice, the

376 van de Waerd, P.J. (2020), ‘Information asymmetries: recognizing the limits of the GDPR on the data-driven market’, *Computer Law and Security Review*, vol. 38, Article Number 105436, p. 12.

377 Vestager, M. (2021), ‘E-000274/2021 Answer given by Executive Vice-President Vestager on behalf of the European Commission’.

378 Mellet, K. and Beauvisage, T. (2019), ‘Cookie Monsters. Anatomy of a digital market infrastructure’, *Consumption Markets and Culture*, vol. 23, no. 2, p.121.

CJEU has interpreted this criterion as requiring ‘active behaviour’ on the part of the data subject and rendering pre-selected checkboxes an inadequate consent mechanism.³⁷⁹ The criterion of unambiguous consent under Article 4(11) is tied to Article 7(1)’s provision that a controller bears the burden of proof in demonstrating a data subject’s consent.³⁸⁰ Without an unambiguous indication of consent by the data subject, a controller would be unable to prove that they have secured consent when asked by a regulator, automatically rendering their data processing operations unlawful under the GDPR.

With online behavioural tracking technologies, there are no inherent barriers to securing unambiguous consent. As long as tracking banners follow an opt-in design and avoid manipulative dark patterns, user acceptance would be active and unambiguous. Whenever a user rejects (or fails to accept) cookies and other tracking technologies, in whole or in regard to a specific adtech vendor, a corresponding negative consent string is attached to outgoing RTB bid requests. The negative consent string may lead to bid requests being pruned from personal data, denied to certain partners the user has not consented to, spared from cookie syncing, and more.

In reality, behavioural targeting is presently plagued by a relatively high level of incompliance in securing and respecting user choices. As mentioned in the previous section, neither the TCF standard nor the OpenRTB/Authorized Buyers protocols include a mechanism to guarantee trackers’ compliance with user consent choices. In other words, ad exchanges may ignore the consent string and broadcast bid requests freely, while trackers may store cookies in contravention of a user’s choices. It is unfair to presume that any adtech actors engage in such unlawful practices just because they are theoretically able to, but quantitative studies demonstrate that improper conduct by RTB actors is far from incidental.

In late 2019, researchers found that consent was stored before an inputted user choice in 66/560 popular websites, pre-selected choices were present in 236/508 popular websites, and 39/508 popular websites wrongfully register a positive choice after the user rejects cookies.³⁸¹ In a sweep carried out several months later, in part following the landmark *Planet49* case in which the CJEU ruled against pre-selected checkboxes, the Irish DPA found that only 1 out of 38 pop-

379 CJEU Case C-61/19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, judgment of 11 November 2020, para. 36.

380 *Ibid.*, para. 42.

381 Matte, C., Bielova, N., and Santos, C. (2020), ‘Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe’s Transparency and Consent Framework’, *2020 IEEE Symposium on Security and Privacy*, p. 799.

ular websites did not set non-essential cookies immediately upon landing.³⁸² The DPA further found that 10/38 websites relied on pre-checked boxes and 1 website had an entirely non-functioning CMP where unchecking any boxes did not actually prevent tracking cookies from being set.³⁸³ Finally, only a small number of the canvassed websites declared the use of tracking technologies besides HTTP cookies, yet the DPA had grounds to suspect the presence of undeclared web beacons.³⁸⁴

Two years after these studies, the situation has not markedly improved. A 2021 crawl of 26,000 websites employing 300,000 labelled cookies using the Cookie-Bot, OneTrust, and Termly CMPs found that 15.45% of Google Analytics cookies were mislabelled in regard to their stated purpose and 2.88% of the total Google Analytics cookies were labelled as ‘strictly necessary’.³⁸⁵ More worryingly, the study found that 42.21% of cookies were entirely undeclared in the consent notice, with such undeclared cookies being found in 86.08% of analysed websites.³⁸⁶

These persistent online problems with preloaded, undeclared, or pre-selected trackers are a significant hurdle for data controllers who wish to demonstrate unambiguous consent to tracking. A pre-loaded cookie is essentially an unlawful data processing operation carried out prior to consent being secured through unambiguous acts. An undeclared or mislabelled cookie is likewise indicative of data processing that has not been adequately conveyed to the end user, frustrating their informed, unambiguous, and specific consent. Finally, pre-selected checkboxes cannot unambiguously prove that a user has noticed them and actually given consent to his or her personal data being processed.³⁸⁷

Reducing ambiguity in online behavioural tracking notices is a challenging prospect for publishers, who frequently operate under limited budgets, choice-restricting CMP design, and an opaque understanding of what third- and fourth-party scripts are loaded into their webpages. As noted by several researchers, website operators frequently lack the technical knowledge to fully

382 DPC (2020), ‘Report by the Data Protection Commission on the use of cookies and other tracking technologies’, p. 7.

383 Ibid., p. 12.

384 Ibid., p. 13.

385 Bollinger, D. (2021), *Analyzing Cookies Compliance with the GDPR*, Msc diss., ETH Zurich, p. 61.

386 Ibid., p. 64.

387 CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, judgment of 1 October 2019, para. 55.

audit all third-party scripts and trackers deployed on their pages.³⁸⁸ Automated tracker auditing tools have yet to achieve sufficient coverage and uptake so as to address these issues. Nevertheless, web development best practices and other soft law may be a promising avenue by which to promulgate tracker auditing tools, empower publishers, and ensure that the publisher-user interface is as informative and comprehensive as possible in regard to behavioural tracking.

As the largest modern web browsers shift away from third-party cookies, there is significant promise for reducing opacity and, therefore, ambiguity in consent collection mechanisms. A lack of third-party cookies means that publishers may exercise greater control over the tracking mechanisms deployed on their webpages. Yet, third-party HTTP cookies only comprise a part of the online tracking toolset. Third-party stateless trackers, such as web beacons and fingerprinting scripts, are still poised to carry out personal data harvesting and user profiling, meaning that regular web page audits and comprehensive consent notices will remain necessary to dispel any ambiguity surrounding data subjects' consent.

Furthermore, the shift towards first-party cookies has seen trackers attempt to circumvent their newfound limitations by way of techniques such as CNAME cloaking. CNAME cloaking is a method of circumventing the same origin policy of a web browser by fooling it into treating third-party subdomains as part of the first party origin.³⁸⁹ Studies have demonstrated that CNAME-based trackers are rapidly gaining in popularity as third-party cookie trackers wane,³⁹⁰ with researchers concluding that 10.7% of popular websites deploy such cloaking methods to hide a third-party tracking and advertising service.³⁹¹ Of those 10.7%, half were demonstrated to also leak their first-party cookies to the cloaked third-party advertisers.³⁹²

388 Bollinger, D. (2021), *Analyzing Cookies Compliance with the GDPR*, Msc diss., ETH Zurich, p. 64; Engelhardt, S., Acar, G., and Narayanan, A. (2018), 'Website operators are in the dark about privacy violations by third-party scripts', *Freedom to Tinker* via Princeton University, [<https://freedom-to-tinker.com/2018/01/12/website-operators-are-in-the-dark-about-privacy-violations-by-third-party-scripts/>].

389 Ren, T. et al. (2021), 'An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections', *2021 Workshop on Measurements, Attacks, and Defenses for the Web*, [<https://web.cs.wpi.edu/~ldecarli/docs/papers/madweb21-cloaking.pdf>], p. 1.

390 Dimova, Y. et al. (2021), 'The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion', *2021 Proceedings on Privacy Enhancing Technologies*, no. 3, p. 402.

391 Aliyeva, A. and Egele, M. (2021), 'Oversharing Is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies', *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, p. 129.

392 Ibid., p. 130.

Findings such as these indicate that purely technical hurdles will do little to dispel ambiguity for users, forestall trackers acting in bad faith or without due diligence, or safeguard data subjects' rights. Noncompliant consent mechanisms, privacy-invasive data collection, and opaque industry workings will continue to harm end users until legal enforcement mechanisms are brought to bear by national DPAs, courts, or Union bodies. Ambiguous, broad, and ill-informed consent is ultimately profitable, if not for publishers, then at least for data brokers and advertisers. Only a countervailing and consistent negative economic incentive (e.g., fines) is likely to induce a change in behaviour for the behavioural tracking industry and remedy ongoing compliance failures.

3.7 Special Categories of Personal Data

Special categories of personal data constitute another potential concern for RTB and behavioural tracking compliance with the GDPR. Article 9(1) GDPR prohibits the processing of an exhaustive list of special data categories: 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. A closer reading of Article 9(1) indicates that its prohibition is to be applied broadly, not just to data that directly pinpoints special categories of personal data, but even to data that may indirectly 'reveal' such sensitive information regarding a data subject. Recital 51 GDPR clarifies the rationale for this expansive prohibition by explaining that such data 'are, by their nature, particularly sensitive in relation to fundamental rights and freedoms'.

Due to the power of modern inferential processing, seemingly innocuous data points have the potential to reveal sensitive information to a well-trained machine learning algorithm.³⁹³ To avoid classifying all data as specially protected personal data, the British DPA recommends that regulators adopt a nuanced approach when it comes to inferential processing operations. Under this approach, the classification of inferential data processing operations that risk revealing special categories of personal data depends on the given inference's degree of reasonable certainty and whether the inference is being deliberately drawn.³⁹⁴

³⁹³ See Section 3.2.2. on anonymized datasets.

³⁹⁴ ICO, 'Guide to the General Data Protection Regulation (GDPR): What is special category data?', [<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>].

Despite the broad processing prohibition laid down in Article 9(1) GDPR, there are exceptions under Article 9(2) GDPR that may be invoked to justify the processing of special categories of personal data. The sole exception that may be relevant in the context of behaviourally targeted advertising is that of explicit consent under Article 9(2)(a) GDPR. Specifically, processing of special categories of personal data is possible if ‘the data subject has given explicit consent to the processing of those personal data for one or more specified purposes’. In this context, the criterion of ‘explicit’ consent denotes a higher standard than even the criterion of ‘unambiguity’ for regular consent under Article 4(11) GDPR. The EDPB clarifies that explicit consent is distinguished by the manner in which the data subject expresses consent.³⁹⁵ It becomes evident, then, that explicitness imposes specific structural requirements on the consent collection process. The data controller must approach the data subject with a specific request for consent to clearly defined data processing operations, whereupon the data subject must engage with that request in particular and provide an answer. In other words, explicit consent has the formalistic dimensions of a dialogue more so than regular consent. An indicative, affirmative action that leaves no room to doubt the data subject’s wishes and informedness would therefore be unambiguous, but without serving as a response to a specific consent request, it cannot be considered explicit.

Both the OpenRTB and Authorized Buyers protocols for real-time bidding include fields that denote special categories of personal data. Using OpenRTB as an example,³⁹⁶ these fields are derived from one of two taxonomies – the Audience Taxonomy, which directly serves to flag users according to predefined attributes,³⁹⁷ and the Content Taxonomy, which categorises the content of websites rather than their visitors.³⁹⁸ Version 1.0 of the Audience Taxonomy previously included flags for political beliefs, medical conditions, and religious beliefs, among others.³⁹⁹ These flags were later removed in version 1.1 of the Audience Taxonomy, but individual adtech platforms are free to employ either version and some choose to rely on the nomenclature of version 1.0.⁴⁰⁰

395 European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’, para. 93.

396 Google’s Authorized Buyers program has equivalent taxonomies, cf. <https://storage.googleapis.com/adx-rtb-dictionaries/publisher-verticals.txt>

397 IAB Tech Lab, ‘Audience Taxonomy’, [<https://iabtechlab.com/standards/audience-taxonomy/>].

398 IAB Tech Lab, ‘Content Taxonomy’, [<https://iabtechlab.com/standards/content-taxonomy/>].

399 Ryan, J. (2020), ‘Submission to the Irish Data Protection Commission’, *Irish Council for Civil Liberties*, [<https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>], p. 13.

400 Ibid., p. 14.

The Content Taxonomy includes fields tied to special categories of personal data even in its most recent 2.2 iteration.⁴⁰¹ Since the Content Taxonomy describes the content of webpages rather than the interests of visitors, the taxonomy's classifiers themselves do not refer to the personal data of natural persons. The danger to individuals arises when an RTB tracker receives a bid request containing both a data subject's ID and the detailed classification of the web page content they are currently viewing, allowing said tracker to make reliable inferences about sensitive personal data relating to health, politics, philosophy, or religion.

A 2020 complaint submitted to the Irish DPA by the Irish Council for Civil Liberties illustrates how bid requests may be intercepted by DSPs and shared with trackers to profile users based on special categories of personal data.⁴⁰² Using data from bid requests, a variety of data brokers were shown to have profiled individuals based on sexuality, health issues, religion, political activism, and homelessness, then to have operationalized these datasets for a variety of purposes, including influencing political elections.⁴⁰³

A 2019 report by the British DPA noted that the consent requests employed under the TCF and Authorized Buyers frameworks were noncompliant with the standard of explicit consent required for the processing of special data categories facilitated by these same frameworks.⁴⁰⁴ Existing consent mechanisms do not distinguish between regular personal data processing activities and the processing of special categories of personal data that some DSP platforms facilitate. They therefore fail to attain the heightened dialogical standard of explicit consent previously discussed in this section.

In October 2020, the Belgian DPA's investigative division also found that current RTB mechanisms were noncompliant with the GDPR: 'The TCF does not provide adequate rules for the processing of special categories of personal data. However, the OpenRTB standard, framed by IAB Europe's TCF, does allow the processing of special categories of personal data'.⁴⁰⁵

401 E.g., IDs 287-318.

402 Ryan, J. (2020), 'Submission to the Irish Data Protection Commission', *Irish Council for Civil Liberties*, [<https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>], p. 4.

403 Ibid., pp. 4-12.

404 ICO (2019), 'Update report into adtech and real time bidding', [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>], p. 16.

405 Irish Council for Civil Liberties (2020), 'Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR', [<https://www.iccl.ie/digital-data/apd-iab-findings/>].

The main issue surrounding the processing of special categories of personal data in RTB is therefore one of inadequate security and regulation. To better understand the duties of RTB data controllers, the following Section 3.8 discusses relevant security and confidentiality obligations under the GDPR.

3.8 Security under the GDPR

Security under the GDPR is both an overarching principle and a specific obligation. Article 5(1)(f) GDPR establishes the principle of integrity and confidentiality, which states that personal data must be ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.’

This principle is later operationalized under Article 32 GDPR as a duty of both controllers and processors to ensure an appropriate level of data security. Pursuant to Article 32(1) GDPR, the appropriate level of data security depends on the context of any given data processing operation. In particular, the required security level is proportional to the risk towards the rights and freedoms of data subjects, while the most suitable technical and organizational measures to achieve said level of security are determined by practical considerations (state of the art, cost of implementation), by the ‘nature, scope, context and purposes of processing’, and by the specific risks tied to the processing operations. In the *Digital Rights Ireland* case, the CJEU clarified that the need for safeguards is particularly important wherever there is automatic processing of personal data or a significant risk of unlawful access to the data.⁴⁰⁶

There is no exhaustive list of possible appropriate safeguards, but Article 32(1) GDPR includes four examples of security measures that may be useful in fulfilling the security obligations: ‘the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing’.

406 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, interveners: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12)*, Michael Seitlinger, Christof Tschohl and others, judgment of 8 April 2014, para. 55.

3.8.1 Nature of Processing: Multimodal, Automatic, and Possibly Sensitive

Applying the aforementioned considerations under Article 32 GDPR to the context of online behavioural advertising, an urgent need for reliable security safeguards is evident. The nature of personal data processing operations in a behavioural advertising context involves the collection, recording, retrieval, transmission, structuring, adaptation, consultation, use, and combination of internet users' personal data via algorithmically-automated means, in fractions of a second. In other words, behavioural advertisement relies on multimodal and far-reaching data processing to achieve its aims. Furthermore, as discussed in Section 3.7, the technical underpinnings of RTB systems make it possible for trackers to readily infer or reveal special categories of personal data.

3.8.2 Scope of Processing: Broad

The business of online behavioural advertising and RTB encompasses the data of billions of individuals, with one of the largest data brokers, Oracle, boasting a dataset of more than 5 billion unique IDs⁴⁰⁷ and a data marketplace with 'actionable' data on 300 million users.⁴⁰⁸

3.8.3 Context of Processing: Broad and Unrestrictive

As established in Section 2, the majority of modern programmatic advertising is carried out through open auctions. The personal data processing operations of open auctions involve an entire ecosystem of hundreds of adtech entities, the vast majority of which have no direct relationship to the publisher. By extension and as already discussed, most of these entities lack a direct relationship with the data subject as well, who is frequently unfamiliar or even unaware of their activities.

3.8.4 Purposes of Processing: Profiling of Individuals

Behavioural advertising is centred around the creation of accurate profiles of data subjects, with the goal of evaluating, at minimum, the latter's personal preferences, interests, and behaviour. Since this evaluation is conducted on the basis of personal data and through the use of automated processing, these data processing operations fulfil the criteria for 'profiling' under Article 4(4) GDPR. Profiling in itself is not legally prohibited, but the creation and processing of detailed user profiles creates heightened risks to data subjects' privacy should such profiles be improperly accessed, transmitted, or otherwise subject to data leakage. Therefore, while behavioural profiling in itself is a legally permissible purpose

407 Christl, W. (2017), 'Corporate Surveillance in Everyday Life', *Cracked Labs Institute for Critical Digital Culture*, [<https://crackedlabs.org/en/corporate-surveillance>].

408 Oracle Data Management Platform Help Center, 'Oracle Data Marketplace', [<https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html>].

for data processing, it is a purpose that exists in a state of natural tension with data subject privacy rights, presupposes heightened security risks, and therefore necessitates appropriate safeguards.

3.8.5 Specific Risks

The most striking risk associated with the RTB ecosystem is that of data leakage due to an inordinate number of data recipients, coupled with the possibility (and economic desirability) of further data exchanges and downstream processing. The flow of bid requests, known as the ‘bidstream’, is intended to pass through SSPs, ad exchanges, DSPs, and advertisers solely for the conduct of bids. Yet, any of these bid request recipients may choose to harvest the bid requests for valuable personal data, which they then retain and use to enrich their own datasets.⁴⁰⁹ There is currently no technical limitation preventing the widespread practice of bidstream harvesting beyond user ID or IP pseudonymization, which are currently applied inconsistently at the discretion of publisher and SSP settings.⁴¹⁰

While data security need not be absolute, it needs to be commensurate with the risks of any given set of operations. Considering that each additional data controller or processor has a multiplicative effect on the likelihood of a data leak by a bad actor and taking into account the hundreds of participating vendors in even a regulated list such as that of IAB Europe, the British ICO⁴¹¹ and the Belgian APD-GBA⁴¹² have both indicated that the existing purely contractual controls are inadequate and technical safeguards are needed in order to ensure an adequate level of security for RTB under the GDPR.

3.8.6 Conclusion on Appropriate Security Level

The data processing operations carried out in the course of behavioural tracking and targeted advertising in an RTB context are typified by multimodal and automatic manipulation of (possibly sensitive) personal data, a broad scope of processing that affects most internet users and results in datasets on subjects numbering in the hundreds of millions, an open and unrestrictive ecosystem where participation has little barriers, a profit-oriented motivation centred

409 For an explanation of bidstream harvesting, see BPA Worldwide (2020), ‘What is Data Leakage and How to Prevent it in the Bidstream’, [https://issuu.com/bpaworldwide/docs/data_leakage_and_the_bidstream_-_sept_2020].

410 ‘Site names, IP addresses, and cookies are hidden or anonymized based on the seller’s settings’ Reference: Google, ‘Real-time bidding for developers’, [<https://support.google.com/authorized-buyers/answer/6146609?hl=en>].

411 ICO (2019), ‘Update report into adtech and real time bidding’, [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>], p. 21.

412 Irish Council for Civil Liberties (2020), ‘Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR’, [<https://www.iccl.ie/digital-data/apd-iab-findings/>].

around the profiling of data subjects, and significant special risks related to data leakage. Taken together, these factors necessitate a very high level of corresponding security through strong technical measures, whereas the current behavioural advertising landscape is typified by an over-reliance on weak contractual controls between industry actors.

3.8.7 Achieving an Appropriate Level of Security

Arriving at a precise technical solution for security is beyond this report's scope, but it is possible to briefly consider some approaches to enhancing security in online advertising and RTB. Firstly, the general trend of phasing out third-party cookies is an improvement in overall online privacy and security, but does not prevent bidstream harvesting, which would still be possible via what are referred to as 'deterministic IDs' and similar technologies.⁴¹³

Secondly, the potential of new initiatives such as FLoC and FLEDGE to allay RTB's security concerns in particular is questionable. To quote an analysis by Rescorla and Thomson, 'FLoC still allows for significant linkability of user behaviour, both via measuring the longitudinal evolution of cohort IDs as proposed by Wilander and in combination with existing partial identifiers such as IP address, geolocation and browser fingerprinting.'⁴¹⁴ In other words, applying adtech's state of the art and widely used tracking techniques, it is possible to negate the privacy benefits of FLoC, leading to criticism of the initiative.⁴¹⁵

Another proposal for improving security in the RTB ecosystem comes from Microsoft in the form of 'PARAKEET',⁴¹⁶ PARAKEET proposes to enhance privacy by making a user's browser act as an intermediary in the bid request pipeline. Ad requests would be processed by the browser to anonymize user and publisher information in a consistent and extensive manner, and only then would the anonymized ad request be sent to an ad network for bidding. Since PARAKEET is the newest proposed solution, relative to FLoC and FLEDGE, there are currently few technical appraisals of its practical value for data security.

413 Schiff, A. (2020), 'Can LiveRamp Survive The Cookie Apocalypse?', AdExchanger, [<https://www.adexchanger.com/data-exchanges/can-liveramp-survive-the-cookie-apocalypse/>].

414 Rescorla, E. and Thomson, M. (2021), 'Technical Comments on FLoC Privacy', Mozilla, [https://mozilla.github.io/ppa-docs/floc_report.pdf].

415 Arrieta, A. (2021), 'Am I FLoCed? A New Site to Test Google's Invasive Experiment', *Electronic Frontier Foundation*, [<https://www.eff.org/deeplinks/2021/04/am-i-floced-launch>].

416 Private and Anonymized Requests for Ads that Keep Efficacy and Enhance Transparency Reference: Web Incubator CG, 'privacy-preserving-ads - PARAKEET', *GitHub repository*, [<https://github.com/WICG/privacy-preserving-ads/blob/main/Parakeet.md>].

Whether PARAKEET is technically feasible or not, both it and FLoC serve to enhance the power of the tech giants developing them (Microsoft and Google, respectively). Both proposals would position their developers centrally in the advertising ecosystem and, as such, are likely to invite scrutiny in other respects of the law, such as competition law.⁴¹⁷

Another possible security enhancement involves a wholesale reorientation towards contextual advertising. This is perhaps the most drastic solution for the security issues inherent in adtech, but its drastic nature also makes it the most likely to accommodate the law (if not the current behavioural targeting industry). If user profiling is eliminated from the marketing instrumentarium and personal data is no longer being processed, then most issues stemming from personal data processing, not just in regard to security, would also be nil. While this proposition is a dramatic one *per se*, there are certain considerations that render it even more extreme if it is to be applied in practice.

Namely, such a reorientation is an all-or-nothing prospect – the deployment of advanced contextual advertising technologies without a concomitant retreat from behavioural tracking would only increase the security and privacy risks faced by end users. Detailed contextual information, obtained by advanced machine learning and AI models referenced in Section 2.1, may easily be combined with personal data for powerful inferential analysis. If half of the adtech industry processes advanced contextual data, while the other half continues to process behavioural data and engage in user profiling, data syncing and brokerage will allow the latter half to simply enrich its user profiles even further. Therefore, a break from behavioural tracking, if it is to occur at all, must be done in whole rather than in part.⁴¹⁸

There is no easy answer to the security dilemma in RTB and behaviourally targeted advertising, but it is hopeful that one or more of the technical proposals described above may be developed to a genuinely useful and applicable state. Failing that, it would be hard to imagine an adtech ecosystem that adheres to the GDPR's security requirements without significant structural and operational reforms.

417 Vestager, M. (2021), 'E-000274/2021 Answer given by Executive Vice-President Vestager on behalf of the European Commission'.

418 Cross, T. (2020), 'Is Contextual Targeting Safe in a Privacy-First World?', *VideoWeek*, [<https://videoweek.com/2020/03/17/is-contextual-targeting-safe-in-a-privacy-first-world/>].

3.9 Transparency Issues

Beyond the previously discussed requirements for informed consent, the GDPR also imposes transparency obligations onto data controllers. Similarly to security, data transparency is foremost a general principle of data processing under Article 5(1)(a) GDPR, where it is established that ‘Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’). Transparency is operationalized under, *inter alia*, Articles 13 and 14 GDPR, which describe the information that must be provided by a data controller when personal data have been obtained directly from the subject or from a different source, respectively.

Of the various elements that data subjects need to be made aware of, there is one common element between Articles 13 and 14 that may prove particularly problematic for the RTB ecosystem: ‘the recipients or categories of recipients of the personal data, if any’ (Articles 13(1)(e) and 14(1)(e) GDPR). The concept of ‘recipient’ is broadly defined under Article 4(9) GDPR as ‘a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not’. To ensure that such information is properly conveyed, Article 12(1) GDPR stipulates that the controller must employ ‘a concise, transparent, intelligible and easily accessible form, using clear and plain language’. Summing up these provisions, it is evident that the data subject must be made aware of any entity to whom his or her personal data will be disclosed, regardless of whether that entity is a data processor, controller, joint controller, or third party.

In the context of RTB, where user data passes through hundreds of individual companies across the supply and demand chains, it appears difficult to convey the identities of data recipients to data subjects in any meaningful way. The A29WP Transparency Guidelines, which have since been endorsed by the EDPB,⁴¹⁹ specify: ‘In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects.’⁴²⁰ The Working Party states that such information should either be the named recipients or, in the case of categories of recipients, a maximally specific identification of the type of recipient based on the activities it carries out, its industry/sector/sub-sector, and its location.⁴²¹ A data controller engaged in behavioural tracking and real-time bidding would have difficulty ensuring transparency for much the same reasons it would have difficulty obtaining

419 See: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/transparency_en

420 Article 29 Data Protection Working Party (2018), ‘Guidelines on Transparency under Regulation 2016/679’, p. 37.

421 Ibid., p. 37.

informed consent: the industry's opacity, complexity, and multitudes of recipients would be extremely difficult to convey to data subjects in a manner that is both concise and intelligible. Identifying individual recipients would entail listing every partnered SSP, ad exchange, DSP, advertiser, and data broker in a given RTB implementation, which is practically an impossibility given that these entities number in the hundreds and are constantly in a flux.

On the other hand, merely delineating broad categories of adtech partners is particularly unhelpful for data subjects given the opacity of the RTB ecosystem. First and foremost, broad categories such as SSP, ad exchange, DSP, advertiser, and data broker are likely unintelligible to the average internet user.⁴²² Secondly, the fact that a great many entities in the RTB ecosystem fulfil several of these functions at once through various subsidiaries or simply through parallel data processing operations renders the distinction largely meaningless outside the sphere of legal or technical analysis. When, for example, a CMP carries out analytics, an entity simultaneously operates both an SSP and a DSP, or a DSP harvests bidstream data to sell off as a broker, then any generalized distinction regarding these categories becomes innately uninformative to the layperson. Or, to put it simply, individual classifications are vapid in an industry where everyone tends to do everything.

In the case of an industry with little in the way of appropriate technical safeguards,⁴²³ it is arguably all the more important for a data subject to be able to differentiate between individual entities in whom they may or may not place their trust. For example, the individual branches of a government body with strict internal procedures may somewhat justifiably be referred to under a common denominator – the data subject has similar assurances and expectations towards most such entities. Yet, in the case of the adtech industry, contractual terms and provisions are inconsistent,⁴²⁴ while partner audits are rarely conducted by the majority of the industry,⁴²⁵ making it harder for users to reasonably put their trust in 'adtech' in a blanket manner. As such, it seems to be a violation of the principle of fairness towards data subjects to assume that their trust is transitive between publishers and the latter's various adtech partners. The fact

422 cf. CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, Opinion of Advocate General Szpunar, delivered on 21 March 2019, para. 114.

423 See Section 3.8 on Security Obligations.

424 PricewaterhouseCoopers (2020), 'ISBA Programmatic Supply Chain Transparency Study', ISBA, [<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>], p. 22.

425 PricewaterhouseCoopers, *ibid.*, p. 21; Davies, J. (2016), 'Confessions of an ad tech veteran: "Publishers need to audit their exchanges"', *Digiday*, [<https://digiday.com/media/confessions-ad-tech-veteran-header-bidding-perpetuating-ad-tech-tax/>].

that the RTB industry in particular and the web's security policies in general assume such transitivity of trust is problematic from both a practical and an ethical perspective.⁴²⁶

Overall, it seems difficult to reconcile the GDPR's transparency requirements regarding recipients of data with the open-ended, undefined, multitudinous, and unstandardized structure of the RTB ecosystem.

426 Acar, G., Engelhardt, S., and Narayanan, A. (2020), 'No boundaries: data exfiltration by third parties embedded on web pages', *2020 Proceedings on Privacy Enhancing Technologies*, no. 4, p. 232.

4 Conclusion

Behavioural targeting currently plays a major role in financing the consumer-facing side of the internet. It is the prevailing mode of revenue generation for vast swathes of online publishers, including journalistic outlets and social media platforms, with an estimated market value of more than €40 billion in Europe and more than €150 billion worldwide.⁴²⁷ If behavioural targeting were to disappear with no replacement, the basic financial backbone of the internet economy would be broken.

Yet, the importance of adtech and RTB practices for the economy cannot preclude critical appraisals of their compatibility with the law and fundamental rights and freedoms of the European Union. Indeed, this report's analysis has shown that contemporary behavioural targeting technologies fall squarely within the remit of the General Data Protection Regulation, the foundation of the Union's personal data protection framework, yet currently face extreme compliance hurdles due to a variety of technical, operational, structural, and normative issues.

A key issue is the impossibility for the behavioural targeting industry to secure a lawful basis for data processing operations in its current state. Consent is the only appropriate basis for the majority of data processing operations tied to online behavioural advertising, yet the industry's fundamental opacity and complexity preclude informed consent, the systemic employment of deeply manipulative dark patterns and nudges serves to preclude freely given consent, the present global consent-sharing mechanisms exist in tension with specific consent, and the industry's lack of standardization and inter-actor awareness create significant barriers for unambiguous consent. All of this is compounded by data processing operations that see entities fulfilling several roles in the RTB ecosystem at once, leading to widespread instances of joint data controllership that render any legal enforcement or investigation an arduous and slow process.

The widespread profiling of data subjects coupled with the ready possibility (and proven occurrence) of processing of special categories of data necessitate a high standard of technical and organizational safeguards to guarantee an appropri-

⁴²⁷ Vou, A. (2021), 'Google and Facebook dominate behavioural advertising, even with the cookie crumbling', *European Data Journalism Network*, [<https://www.europeandatajournalism.eu/eng/News/Data-news/Google-and-Facebook-dominate-behavioural-advertising-even-with-the-cookie-crumbling>].

ate level of personal data protection. Yet, such technical and organizational safeguards are largely absent, with the multitude of industry actors relying chiefly on inappropriate contractual controls to achieve security. Even were such controls to be considered appropriate, intra-industry audits and transparency are rare and lacking.

Naturally, the opacity and complexity of the RTB and behavioural tracking industry are problematic for GDPR standards of transparency, too. The inability to furnish data subjects with appropriate and practically useful information regarding data recipients frustrates the former's capacity to exercise their data protection rights.

Although not explicitly included in this report's analysis in the interest of focusing on the most salient points, other principles of personal data processing under the GDPR may also be imperilled in the current state of the behavioural tracking industry. For example, it is relevant to question how '*data minimisation*' under Article 5(1)(c) GDPR may be achieved under an industry focused predominantly on '*data maximisation*', where the entire ecosystem is 'premised on generating, hoarding, and linking as much data as possible in the hope that value and insight can be leveraged from them.'⁴²⁸ Such considerations may indicate a more deep-seated incompatibility between modern user data-driven enterprises that see individual data as a raw resource that can and should be exploited on one hand, and a rights-based privacy and data protection framework on the other.

Indeed, briefly stepping back from the GDPR and taking stock of the broader problems plaguing the behavioural targeting ecosystem may allow for a more holistic and effective solution to any market failures in the data-driven industry. Taking into account the frequent disempowerment and opacity facing not just users, but also publishers,⁴²⁹ indicates the need to address basic power asymmetries stemming from data hoarding and oligarchical power arrangements in the adtech industry. To this end, attempting to resolve the underlying issues with only the toolset of a rights-based data protection framework may amount to trying to fit a square peg into a round hole.⁴³⁰ The political implications of

428 Kitchin, R. and Lauriault, T.P. (2018), 'Toward Critical Data Studies. Charting and Unpacking Data Assemblages and their Work', in Thatcher, J., Eckert, J., and Shears, A. (eds.), *Thinking Big Data in Geography: New Regimes, New Research*, University of Nebraska Press, p. 16.

429 Engelhardt, S., Acar, G., and Narayanan, A. (2018), 'Website operators are in the dark about privacy violations by third-party scripts', *Freedom to Tinker* via Princeton University, [<https://freedom-to-tinker.com/2018/01/12/website-operators-are-in-the-dark-about-privacy-violations-by-third-party-scripts/>].

430 See for example the issue of cookie walls under the ePrivacy Regulation in Section 3.6.3.

behavioural targeting are already spurring the Union to pursue a Democracy Action Plan, while the particular industry arrangements that frustrate straightforward GDPR enforcement are being addressed via the upcoming EU Digital Services Act and Digital Markets Act's focus on effective digital governance.⁴³¹ In addition, several scholars and national courts are probing the utility of competition law and consumer protection law in constraining data-harvest overreach and the employment of manipulative practices.⁴³²

GDPR-based legal complaints against trackers are currently being filed *en masse* by private actors, reaching companies,⁴³³ DPAs,⁴³⁴ and national courts.⁴³⁵ The legal ramifications of these various initiatives remain to be seen, but their sheer volume indicates that decisive judgments on adtech practices will eventually have to be made, one way or another. These findings are inevitably going to come in the context of a changing technological landscape. While third-party cookies are being phased out, first-party data harvesting practices, bidstream harvesting, and same origin policy tricks by third party trackers remain pressing concerns. Replacement technologies, such as FLoC, FLEDGE, and PARAKEET are still undergoing tests and active development, making it difficult to conclusively rule on their adequacy. Yet, current impressions from FLoC in particular demonstrate that it is not only unlikely to be a magical bullet for privacy, but

431 European Commission (2021), 'Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee, and The Committee of the Regions on the European democracy action plan', [[https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)790](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)790)], p. 5.

432 See e.g., van de Waerdt, P.J. (2020), 'Information asymmetries: recognizing the limits of the GDPR on the data-driven market', *Computer Law and Security Review*, vol. 38, Article Number 105436, p. 18; Galli, F. (2021), 'Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD', in Ebers, M., and Gamito, M.C. (eds.), *Algorithmic Governance and Governance of Algorithms*, Springer, p. 135.

433 Noyb (2021), 'noyb aims to end 'cookie banner terror' and issues more than 500 GDPR complaints', [<https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints>].

434 Simon, E. (2019), 'Prevent the Online Ad Industry from Misusing Your Data - Join the #Stop-SpyingOnUs Campaign', *Liberties*, [<https://www.liberties.eu/en/stories/stop-spying-on-us-fix-ad-tech-campaign/275>].

435 Lomas, N. (2021), 'Adtech 'data breach' GDPR complaint is headed to court in EU', *TechCrunch*, [<https://techcrunch.com/2021/06/16/adtech-data-breach-gdpr-complaint-is-headed-to-court-in-eu/>]; The Privacy Collective (2020), 'Dagvaarding', [<https://www.rechtspraak.nl/SiteCollectionDocuments/RBAMS-dagvaarding-collectieve-vordering-Oracle-Nederland-BV-SFDC-Netherlands-BV-Oracle-Corporation-Oracle-America-Inc-Salesforce.pdf>].

may even serve to worsen tracking and inferential processing in the behavioural targeting industry.⁴³⁶

Even though FLoC trials have barely begun, behavioural trackers are already using FLoC IDs to enrich personal data profiles,⁴³⁷ hinting at a deeper conundrum in resolving the adtech industry's privacy market failure. Namely, partial band-aids are unlikely to work. Merely substituting one identifier for another or offering deeper contextual data while data brokers still build and sync behavioural profiles simply affords trackers more inputs with which to enrich their datasets. Considering this and the foregoing arguments regarding the principal and structural deficiencies of the behavioural tracking industry, it is an open question whether a wholesale legal and technical transition away from such technologies is not desirable. Unarguably, this would constitute a dramatic and disruptive shift, but a consideration of such a move would coincide with the EU's present struggle to regulate other inherently privacy-dangerous technologies such as AI facial recognition. In the same way that a ban on remote biometric identification in public spaces is being championed by the EDPS despite the recent Artificial Intelligence Act,⁴³⁸ it may also be time to countenance a correspondingly holistic (albeit possibly less severe) regulatory intervention in the context of online behavioural tracking and real-time bidding practices.

From the perspective of free and open internet governance, behavioural targeting is not irreplaceable. Research has quantified the revenue increase enjoyed by publishers due to cookie (and therefore, behavioural tracking) availability as roughly 4%, or \$0.00008 per impression.⁴³⁹ Yet even this figure is further undercut when one considers that it does not capture the 'adtech tax' – the further costs associated with partnering with adtech middlemen and ensuring legal compliance with personal data protection standards. If these costs are accounted for, claims and case studies arise indicating that 'marketers and publishers are

436 Kaye, K. (2021), 'As ad tech firms test ways to connect Google's FLoC to other data, privacy watchers see fears coming true', *Digiday*, [<https://digiday.com/marketing/as-ad-tech-firms-test-ways-to-connect-googles-floc-to-other-data-privacy-watchers-see-fears-coming-true/>]; Rescorla, E. and Thomson, M. (2021), 'Technical Comments on FLoC Privacy', *Mozilla*, [https://mozilla.github.io/ppa-docs/floc_report.pdf].

437 Kaye, K., *ibid*.

438 European Data Protection Supervisor (2021), 'Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary', [https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en].

439 Marotta, V., Abhishek, V., and Acquisti, A. (2019), 'Online Tracking and Publishers' Revenues: An Empirical Analysis', *2019 Workshop on the Economics of Information Security*, [https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf].

making more money by using less adtech',⁴⁴⁰ provided that they implement an alternative to behavioural advertising.

Such an alternative may come in the form of personal data-free technologies that bolster contextual advertisements with machine learning-driven automatic content classification. Considering the inherent incompatibility between the behavioural tracking industry's structure and the fundamental rights to privacy and data protection, a market intervention may be needed to eliminate the excessive negative externalities posed by invasive online data harvesting. In their stead, existing privacy-friendly advertising technologies may support a free and profitable internet ecosystem while still ensuring compliance with the EU's legal order.

Whatever solution is eventually decided on, whether a return to contextual advertising or something else, it is clear that the current state of behavioural tracking in web advertising regularly breaches both the letter and the spirit of Union data protection law and requires urgent correction.

440 Fou, A. (2020), 'Marketers And Publishers Are Making More Money By Using Less Adtech', *Forbes*, [<https://www.forbes.com/sites/augustinefou/2020/08/07/marketers-and-publishers-are-making-more-money-by-using-less-adtech/>].

5 Bibliography

5.1 Legislation

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 1950, ETS 5.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Data Protection Directive'/'DPD'), 1995, OJ L 281/1.

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 ('ePrivacy Directive'), 2002, OJ L 201.

Charter of Fundamental Rights of the European Union, 2016, OJ C 202/389.

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

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016, OJ L 119/89.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('ePrivacy Regulation', adopted Council position), 2021, ST 6087/21.

5.2 Case Law

CJEU Case C-101/01, *Lindqvist*, judgment of 6 November 2003 (ECLI:EU:C:2003:596).

CJEU Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy*, judgment of 16 December 2008 (ECLI:EU:C:2008:727).

CJEU Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, judgment of 9 November 2010 (ECLI:EU:C:2010:662).

CJEU Case C-543/09, *Deutsche Telekom AG v Federal Republic of Germany*, judgment of 5 May 2011 (ECLI:EU:C:2011:279).

CJEU Case C-543/09, *Deutsche Telekom AG v Federal Republic of Germany*, Opinion of Advocate General Trstenjak, delivered on 17 February 2011 (ECLI:EU:C:2011:90).

CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others*, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

CJEU Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, judgment of 13 May 2014 (ECLI:EU:C:2014:317).

CJEU Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v M and S*, judgment of 17 July 2014 (ECLI:EU:C:2014:2081).

CJEU Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v M and S*, Opinion of Advocate General Sharpston, delivered on 12 December 2013 (ECLI:EU:C:2013:838).

CJEU Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, judgment of 11 December 2014, (ECLI:EU:C:2014:2428).

CJEU Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információs-
abadság Hatóság*, judgment of 1 October 2015 (ECLI:EU:C:2015:639).

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

CJEU Case C-434/16, *Peter Nowak v Data Protection Commissioner*, judgment
of 20 December 2017 (ECLI:EU:C:2017:994).

ECtHR Case 62357/14, *Case of Benedik v. Slovenia*, judgment of 24 April 2018
(ECLI:CE:ECHR:2018:0424JUD006235714).

CJEU Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schle-
swig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, judgment of 5
June 2018 (ECLI:EU:C:2018:388).

CJEU Case C-25/17, *Proceedings brought by Tietosuoja valtuutettu (Jehovan
todistajat)*, judgment of 10 July 2018 (ECLI:EU:C:2018:551).

CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW
eV*, judgment of 29 July 2019 (ECLI:EU:C:2019:629).

CJEU Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW
eV*, Opinion of Advocate General Bobek, delivered on 10 December 2018
(ECLI:EU:C:2018:1039).

CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Ver-
braucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*,
judgment of 1 October 2019 (ECLI:EU:C:2019:801).

CJEU Case C-673/17, *Bundesverband der Verbraucherzentralen und Ver-
braucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*,
Opinion of Advocate General Szpunar, delivered on 21 March 2019
(ECLI:EU:C:2019:246).

Landgericht Rostock Case 3 O 762/19, *Bundesverband der Verbraucherzen-
tralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV
gegen advocado GmbH*, judgment of 15 September 2020.

CJEU Case C-61/19, *Orange România SA v Autoritatea Națională de
Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, judgment
of 11 November 2020 (ECLI:EU:C:2020:901).

5.3 Guidelines, Advisory Opinions, Investigations, and EU Press Releases

AEPD (2020), ‘Guía sobre el uso de las cookies’.

AP (2013), ‘Onderzoek CBP naar het combineren van persoonsgegevens door Google. Rapport definitieve bevindingen’.

AP, ‘Cookies’, [<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies>].

Article 29 Data Protection Working Party (2007), ‘Opinion 4/2007 on the concept of personal data’.

Article 29 Data Protection Working Party (2010), ‘Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’.

Article 29 Data Protection Working Party (2011), ‘Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising’.

Article 29 Data Protection Working Party (2014), ‘Opinion 05/2014 on Anonymisation Techniques’.

Article 29 Data Protection Working Party (2017), ‘Statement of the Article 29 Working Party: Data protection and privacy aspects of cross-border access to electronic evidence’.

Article 29 Data Protection Working Party (2018), ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679’.

Article 29 Data Protection Working Party (2018), ‘Guidelines on Transparency under Regulation 2016/679’.

CNIL (2019), ‘Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC’.

CNIL (2020), ‘Délibération n° 2020-092 du 17 septembre 2020 portant adoption d’une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookieset autres traceurs»’.

Council of the EU (2021), ‘Confidentiality of electronic communications: Council agrees its position on ePrivacy rules’, [<https://www.consilium.europa>].

[eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/](https://ec.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/)].

DPC (2020), ‘Report by the Data Protection Commission on the use of cookies and other tracking technologies’.

DSB (2018), ‘GZ: DSB-D122.931/0003-DSB/2018’.

EU Directorate-General for Communications Networks (2017), Content and Technology, ‘Internet Governance Forum 2017: Joint Declaration from European Commissioner Mariya Gabriel and Members of the European Parliament’, [<https://digital-strategy.ec.europa.eu/en/news/internet-governance-forum-2017-joint-declaration-european-commissioner-mariya-gabriel-and-members>].

European Commission (2021), ‘Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee, and The Committee of the Regions on the European democracy action plan’, [[https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)790](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)790)].

European Data Protection Board (2019), ‘Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)’.

European Data Protection Board (2019), ‘Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities’.

European Data Protection Board (2019), ‘Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects’.

European Data Protection Board (2020), ‘Guidelines 05/2020 on consent under Regulation 2016/679’.

European Data Protection Board (2020), ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’.

European Data Protection Board (2021), ‘Guidelines 8/2020 on the targeting of social media users’.

European Data Protection Supervisor (2021), ‘Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary’, [https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en].

ICO (2012), ‘Anonymisation: managing data protection risk code of practice’, [<https://ico.org.uk/media/1061/anonymisation-code.pdf>].

ICO, ‘Guide to the General Data Protection Regulation (GDPR): What is special category data?’, [<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>].

ICO (2019), ‘Update report into adtech and real time bidding’, [<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>].

Publications Office of the European Union (2020), *Sources of European Union law*, [<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGIS-SUM%3A114534>].

Vestager, M. (2021), ‘E-000274/2021 Answer given by Executive Vice-President Vestager on behalf of the European Commission’.

5.4 Scholarship

Acar, G. et al. (2015), ‘Facebook Tracking Through Social Plug-ins’, [<https://www.esat.kuleuven.be/cosic/publications/article-2555.pdf>].

Acar, G., Engelhardt, S., and Narayanan, A. (2020), ‘No boundaries: data exfiltration by third parties embedded on web pages’, *2020 Proceedings on Privacy Enhancing Technologies*, no. 4, pp. 220-238.

Al-Fannah, N.M., Li, W., and Mitchell, C.J. (2019), ‘Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking’, *Proceedings of the 21st International Conference on Information Security*, pp. 481-501.

Aliyeva, A. and Egele, M. (2021), ‘Oversharing Is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies’, *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 123-134.

Amnesty International (2019), 'Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights', Document POL 30/1404/2019, [<https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>].

Anderson, J. and Rainie, L. (2020), 'Concerns about democracy in the digital age', *Pew Research Center*, [<https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/>].

Avenson, M.D. et al. (2011), 'Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning', [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390].

Bashir, M.A. (2019), *On the Privacy Implications of Real Time Bidding*, Ph.D. diss., Northeastern University.

Bielova, N. and Santos, C. (2020), 'Feedback regarding EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR', *Inria*, [<https://hal.inria.fr/hal-03117323/document>].

Bollinger, D. (2021), *Analyzing Cookies Compliance with the GDPR*, Msc diss., ETH Zurich.

Bujlow, T. et al. (2017), 'A Survey on Web Tracking: Mechanisms, Implications, and Defenses', *Proceedings of the IEEE*, vol. 195, no. 8, pp. 1476-1510.

Bygrave, L.A. (2021), 'Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions', in Ienca, M. et al. (eds.), *Cambridge Handbook of Life Sciences, Information Technology and Human Rights*, (forthcoming).

Christl, W. (2017), 'Corporate Surveillance in Everyday Life', *Cracked Labs Institute for Critical Digital Culture*, [<https://crackedlabs.org/en/corporate-surveillance>].

Chyi, H.I. and Ng, Y.M.M. (2020), 'Still Unwilling to Pay: An Empirical Analysis of 50 U.S. Newspapers' Digital Subscription Results', *Digital Journalism*, vol. 8, no. 4, pp. 526-547.

Cohen, A. and Nissim, K. (2020), 'Towards formalizing the GDPR's notion of singling out', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 117, no. 15, pp. 8344-8352.

Davis, P. (2020), ‘Facial Detection and Smart Billboards: Analysing the “Identified” Criterion of Personal Data in the GDPR’, *European Data Protection Law Review*, vol. 6, no. 3, p. 365-377.

Dimova, Y. et al. (2021), ‘The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion’, *2021 Proceedings on Privacy Enhancing Technologies*, no. 3, pp. 394-412.

Engelhardt, S. and Narayanan, A. (2016), ‘Online Tracking: A 1-million-site Measurement and Analysis’, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1388-1401. Here cited: extended version available at [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf].

Finck, M. and Pallas, F. (2020), ‘They who must not be identified—distinguishing personal from non-personal data under the GDPR’, *International Data Privacy Law*, vol. 10, no. 1, pp. 11-36.

Forbrukerrådet (2020), ‘Out of Control: How consumers are exploited by the online advertising industry’, [<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>].

Freitas, S. and Levene, M. (2005), ‘Spam’, in Ghaoui, C. (ed.), *Encyclopedia of Human Computer Interaction*, IGI Global, pp. 553-558.

Galli, F. (2021), ‘Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD’, in Ebers, M., and Gamito, M.C. (eds.), *Algorithmic Governance and Governance of Algorithms*, Springer, pp. 109-135.

George, D., Reutimann, K. and Tamò-Larrieux, A. (2019), ‘GDPR bypass by design? Transient processing of data under the GDPR’, *International Data Privacy Law*, vol. 9, no. 4, pp. 285-298.

Gonzalez, R. et al. (2017), ‘The cookie recipe: Untangling the use of cookies in the wild’, *Proceedings of the 1st Network Traffic Measurement and Analysis Conference*, pp. 1-9.

Graßl, P. (2021), ‘Dark and Bright Patterns in Cookie Consent Requests’, *Journal of Digital Social Research*, vol. 3, no. 1, pp. 1-38.

Hummel, D. and Maedche, A. (2019), 'How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies', *Journal of Behavioral and Experimental Economics*, vol. 80, pp. 47-58.

Jokinen, J. (2018), *Personal Internet Privacy and Surveillance: Implementation and evasion of user tracking*, MSc diss., JAMK University of Applied Sciences.

Karaj, A. et al. (2019), 'WhoTracks.Me: Shedding light on the opaque world of online tracking', [<https://arxiv.org/abs/1804.08959>].

Kitchin, R. and Lauriault, T.P. (2018), 'Toward Critical Data Studies. Charting and Unpacking Data Assemblages and their Work', in Thatcher, J., Eckert, J., and Shears, A. (eds.), *Thinking Big Data in Geography: New Regimes, New Research*, University of Nebraska Press, pp. 3-20.

Kondor, D. et al. (2018), 'Towards Matching User Mobility Traces in Large-Scale Datasets', *IEEE Transactions on Big Data*, vol. 6, no. 4, pp. 714-726.

Korolova, A. and Sharma, V. (2018), 'Cross-App Tracking via Nearby Bluetooth Devices', *CODASPY'18*, pp. 43-52.

Krishnamurthy, B. and Wills, C.E. (2009), 'Privacy Diffusion on the Web: A Longitudinal Perspective', *Proceedings of the '09 World Wide Web Conference*, pp. 541-550.

Kristol, D. (2001), 'HTTP Cookies: Standards, Privacy, and Politics', *ACM Transactions on Internet Technology*, vol. 1, no. 2, pp. 151-198.

Kuner, C., Bygrave, L.A., and Docksey, C. (eds.) (2020), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press. Chapters:

Kranenborg, H. (2020), 'Article 2: Material Scope', pp. 60-73.

Svantesson, D.J.B. (2020), 'Article 3: Territorial Scope', pp. 74-99.

Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(2): Processing', pp. 116-122.

Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(7): Controller', pp. 145-156.

Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(8): Processor', pp. 157-162.

Bygrave, L.A. and Tosoni, L. (2020), 'Article 4(11): Consent', pp. 174-187.

Kotschy, W. (2020), 'Article 6: Lawfulness of processing', pp. 321-344.

Kuner, C., Bygrave, L.A., and Docksey, C. (eds.) (2021), *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles*, Oxford University Press.

Bygrave, L.A. and Tosoni, L. (2021), 'Article 4(1): Personal data', pp. 22-27.

Kurtz, A. et al. (2016), 'Fingerprinting Mobile Devices Using Personalized Configurations', *Proceedings on Privacy Enhancing Technologies*, vol. 4, no. 19, pp. 4-19.

Laperdrix, P. et al. (2020), 'Browser Fingerprinting: A Survey', *ACM Transactions on the Web*, vol. 14, no. 2, Article Number 8.

Leader, W.G. and Kyriasis (1994), N., *Fundamentals of Marketing*, Nelson Thornes, pp. 194-234.

Leiser, M.R. and Custers, B.H.M. (2019), 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review*, vol. 5, no. 3, pp. 367-378.

Lombard, M. and Snyder-Duch, J. (2017), 'Digital Advertising in a New Age: The Power of (Tele)Presence', in Rodgers, S. and Thorson, E. (eds.), *Digital Advertising: Theory and Research*, Routledge, pp. 169-187.

Marotta, V., Abhishek, V., and Acquisti, A. (2019), 'Online Tracking and Publishers' Revenues: An Empirical Analysis', *2019 Workshop on the Economics of Information Security*, [https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf].

Matte, C., Bielova, N., and Santos, C. (2020), 'Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework', *2020 IEEE Symposium on Security and Privacy*, pp. 791-809.

Matte, C., Santos, C., and Bielova, N. (2020), 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?', *Annual Privacy Forum 2020*, pp. 163-185.

Mellet, K. and Beauvisage, T. (2019), 'Cookie Monsters. Anatomy of a digital market infrastructure', *Consumption Markets and Culture*, vol. 23, no. 2, pp. 110-129.

Nadler, A., Crain, M., and Donovan, J. (2018), 'Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech', *Data & Society Research Institute, Inc.*, [https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf].

Narayanan, A. and Felten, E.W. (2014), 'No silver bullet: De-identification still doesn't work', Princeton University, [<https://www.cs.princeton.edu/~arvindn/publications/no-silver-bullet-de-identification.pdf>].

Narayanan, A. et al. (2020), 'Dark Patterns: Past, Present, and Future. The evolution of tricky user interfaces', *Communications of the ACM*, vol. 63, no. 9, pp. 42-47.

Noggle, R. (2020), 'The Ethics of Manipulation', in Zalta, E.N. (ed.), *The Stanford Encyclopedia of Philosophy*, [<https://plato.stanford.edu/entries/ethics-manipulation/>].

Nouwens, M. et al. (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1-13.

Olejnik, L. and Castelluccia, C. (2014), 'To bid or not to bid? Measuring the value of privacy in RTB', [<https://lukaszolejnik.com/rtb2.pdf>].

Papadopoulos, P., Kourtellis, N., and Markatos, E. (2018), 'Exclusive: How the (synced) Cookie Monster breached my encrypted VPN session', *Proceedings of the 11th European Workshop on Systems Security*, pp. 1-6.

Papadopoulos, P., Kourtellis, N., and Markatos, E. (2019), 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask', *Proceedings of the '19 World Wide Web Conference*, pp. 1432-1442.

Raz, J. (1988), *The Morality of Freedom*, Oxford University Press, pp. 369-395.

Ren, T. et al. (2021), 'An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections', *2021 Workshop on Measurements, Attacks, and Defenses for the Web*, [<https://web.cs.wpi.edu/~ldecarli/docs/papers/mad-web21-cloaking.pdf>].

Rescorla, E. and Thomson, M. (2021), 'Technical Comments on FLoC Privacy', *Mozilla*, [https://mozilla.github.io/ppa-docs/floc_report.pdf].

Rocher, L., Hendrickx, J.M., and de Montjoye, Y.-A. (2019), 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications*, vol. 10, Article Number 3069.

Ryan, J. (2018), 'Report from Dr Johnny Ryan – Behavioural advertising and personal data', *Brave*, [<https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf>].

Ryan, J. (2020), 'Submission to the Irish Data Protection Commission', *Irish Council for Civil Liberties*, [<https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>].

Santos, C. et al. (2021), 'Consent Management Platforms under the GDPR: processors and/or controllers?', *Annual Privacy Forum 2021*, pp. 47-69.

Santos, C., Bielova, N., and Matte, C. (2020), 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners', *Technology and Regulation 2020*, pp. 91-135.

Schneier, B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company.

Sipior, J.C., Ward, B.T., and Mendoza, R.A. (2011), 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons', *Journal of Internet Commerce*, vol. 10, no. 1, pp. 1-16.

Summers, C.A., Smith, R.W., and Reczek, R.W (2016), 'An Audience of One: Behaviorally Targeted Ads as Implied Social Labels', *Journal of Consumer Research*, vol. 43, no. 1, pp. 156-178.

Urban, T. et al. (2018), 'The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR', [<https://arxiv.org/abs/1811.08660>].

Urban, T. et al. (2020), 'Beyond the Front Page: Measuring Third Party Dynamics in the Field', *Proceedings of the '20 World Wide Web Conference*, pp. 1275-1286.

Utz, C. et al. (2019), '(Un)informed Consent: Studying GDPR Consent Notices in the Field', *ACM Conference on Computer and Communications Security '19*, pp. 973-990.

van Casteren, D.C.J. (2017), *Consent now and then*, LLM diss., Tilburg University.

van de Waerdt, P.J. (2020), 'Information asymmetries: recognizing the limits of the GDPR on the data-driven market', *Computer Law and Security Review*, vol. 38, Article Number 105436.

van der Sloot, B. (2015), 'Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system', *Computer Law and Security Review*, vol. 31, no. 1, pp. 26-45.

Veale, M. and Zuiderveen Borgesius, F.J. (2021), 'Adtech and Real-Time Bidding under European Data Protection Law', *German Law Journal* (forthcoming), [<https://osf.io/preprints/socarxiv/wg8fq/>].

Wang, J., Zhang, W., and Yuan, S. (2017), 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting', *Foundations and Trends in Information Retrieval*, vol. 11, no. 4-5, pp. 297-435.

Yuan, H. et al. (2018), 'Cross-device tracking through identification of user typing behaviours', *Electronic Letters*, vol. 54, no. 15, pp. 957-959.

Zimmeck, S. et al. (2017), 'A Privacy Analysis of Cross-device Tracking', *Proceedings of the 26th USENIX Security Symposium*, pp. 1391-1408.

Zuiderveen Borgesius, F.J. (2015), *Improving Privacy Protection in the Area of Behavioural Targeting*, Ph.D diss, University of Amsterdam.

Zuiderveen Borgesius, F.J. (2015), 'Personal data processing for behavioural targeting: which legal basis?', *International Data Privacy Law*, vol. 5, no. 3, pp. 163-176.

5.5 Web Resources and Media

Ahamed, R. (2020), 'What is Header Bidding & How it Works', *automatad*, [<https://headerbidding.co/header-bidding/>].

Arrieta, A. (2021), 'Am I FLoCed? A New Site to Test Google's Invasive Experiment', *Electronic Frontier Foundation*, [<https://www EFF.org/deeplinks/2021/04/am-i-floxed-launch>].

Axon, S. (2021), '96% of US users opt out of app tracking in iOS 14.5, analytics find', *Ars Technica*, [<https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/>].

Barker, A. (2020), 'Digital ad market set to eclipse traditional media for first time', *Financial Times*, [<https://www.ft.com/content/d8aaf886-d1f0-40fb-abff-2945629b68c0>].

Bell, L. (2016), 'Machine learning versus AI: what's the difference?', *Wired*, [<https://www.wired.co.uk/article/machine-learning-ai-explained>].

BPA Worldwide (2020), 'What is Data Leakage and How to Prevent it in the Bidstream', [https://issuu.com/bpaworldwide/docs/data_leakage_and_the_bidstream_-_sept_2020].

Cross, T. (2020), 'Is Contextual Targeting Safe in a Privacy-First World?', *VideoWeek*, [<https://videoweek.com/2020/03/17/is-contextual-targeting-safe-in-a-privacy-first-world/>].

Davies, J. (2016), 'Confessions of an ad tech veteran: "Publishers need to audit their exchanges"', *Digiday*, [<https://digiday.com/media/confessions-ad-tech-veteran-header-bidding-perpetuating-ad-tech-tax/>].

Dutton, S. (2021), 'What is FLoC?', *Google*, [<https://web.dev/floc/>].

EFF, 'Cover Your Tracks', *Electronic Frontier Foundation*, [<https://coveryourtracks.eff.org/about>].

Engelhardt, S., Acar, G., and Narayanan, A. (2018), 'Website operators are in the dark about privacy violations by third-party scripts', *Freedom to Tinker* via Princeton University, [<https://freedom-to-tinker.com/2018/01/12/website-operators-are-in-the-dark-about-privacy-violations-by-third-party-scripts/>].

Fou, A. (2020), 'Marketers And Publishers Are Making More Money By Using Less Adtech', *Forbes*, [<https://www.forbes.com/sites/augustinefou/2020/08/07/marketers-and-publishers-are-making-more-money-by-using-less-adtech/>].

Gary, J. and Soltani, A. (2019), 'First Things First: Online Advertising Practices and Their Effects on Platform Speech', *Knight First Amendment Institute* at Columbia University, [<https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech>].

Germain, T. (2019), 'Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads.', *Consumer Reports*, [<https://www.consumerreports.org/privacy/digital-billboards-are-tracking-you-and-they-want-you-to-see-their-ads/>].

Giglia, L. (2020), 'Tech Advances in OOH Advertising', *Sign Media*, [<https://www.signmedia.ca/tech-advances-in-oooh-advertising/>].

Google (2020), 'Data Processing Amendment to Chrome Agreements', [https://www.google.com/chrome/terms/dpa_terms.html].

Google, 'About Contextual Targeting', [<https://support.google.com/google-ads/answer/2404186>].

Google, 'Ad Manager and Ad Exchange program policies: Understanding PII in Google's contracts and policies', [<https://support.google.com/admanager/answer/7686480?hl=en>].

Google, 'OpenRTB Integration', [<https://developers.google.com/authorized-buyers/rtb/openrtb-guide>].

Google, 'Real-time bidding for developers', [<https://support.google.com/authorizedbuyers/answer/6146609?hl=en>].

Google, 'Real-Time Bidding', [<https://developers.google.com/authorized-buyers/rtb/start>].

Grant, N. (2021), 'Google to Let Android Users Opt Out of Tracking, Following Apple', *Bloomberg*, [<https://www.bloomberg.com/news/articles/2021-06-03/google-to-let-android-users-opt-out-of-tracking-following-apple>].

GumGum HQ (2020), 'Understanding Contextual Relevance and Efficiency', *dentsu*, [<https://insights.gumgum.com/hubfs/DAN%20Research%20Study/GumGum%20Contextual%20Research%20Paper-1.pdf>].

Gumgum, 'How we Process Images', [<http://view.ceros.com/gumgum/howwe-processimages/p/1>].

IAB (2013), 'Cookies on Mobile 101', [<https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf>].

IAB (2020), 'A Guide to the Post Third-Party Cookie Era', [https://designrr.s3.amazonaws.com/mardare_at_iabeurope.eu_80924/_5449.pdf].

IAB Europe (2020), 'IAB Europe submission to the EDPB public consultation on Guidelines 08/2020 on the targeting of social media users', [https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/iab_europe_-_response_to_edpb_guidelines_08-2020.pdf].

IAB Europe (2020), 'IAB Europe Submits Response to Preliminary Report of The Belgian Data Protection Authority', [<https://iabeurope.eu/blog/iab-europe-submits-response-to-preliminary-report-of-the-belgian-data-protection-authority/>].

IAB Europe (2021), 'IAB Europe Transparency & Consent Framework Policies', [https://iabeurope.eu/wp-content/uploads/2021/05/TCF_v2-0_PolicyVersion_2021-05-27-3.3.pdf].

IAB Europe (2021), 'New Guide: GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR', [<https://iabeurope.eu/knowledge-hub/guide-gdpr-data-protection-impact-assessments-dpia-for-digital-advertising-under-gdpr/>].

IAB Europe, 'TCF – Transparency and Consent Framework', [<https://iabeurope.eu/transparency-consent-framework/>].

IAB Europe, 'Vendor List TCF v2.0', [<https://iabeurope.eu/vendor-list-tcf-v2-0/>].

IAB Tech Lab (2020), 'IAB & IAB Tech Lab Respond with Support for Open-RTB and IAB Europe's Transparency & Consent Framework', [<https://iabtechlab.com/iab-and-tech-lab-respond-with-support-for-open-rtb-and-iab-europes-transparency-consent-framework/>].

IAB Tech Lab, 'Audience Taxonomy', [<https://iabtechlab.com/standards/audience-taxonomy/>].

IAB Tech Lab, 'Content Taxonomy', [<https://iabtechlab.com/standards/content-taxonomy/>].

IAB, 'CMP Mask', [<https://register.consensu.org/CMP>].

IAB, 'Glossary of Terminology', [<https://www.iab.com/insights/glossary-of-terminology/>].

IAB, 'IAB Europe Transparency and Consent Framework Implementation Guidelines', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md>].

IAB, 'openrtb', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md>].

IAB, 'Programmatic and Automation – The Publishers' Perspective', [https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf].

IAB, 'Transparency and Consent String with Global Vendor & CMP List Formats', *GitHub repository*, [<https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md>].

Irish Council for Civil Liberties (2020), 'Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR', [<https://www.iccl.ie/digital-data/apd-iab-findings/>].

Kamkar, S. (2010), 'evercookie', [<https://samy.pl/evercookie/>].

Kapur, S. and Savare, M. (2018), 'Fear of Brave? An Analysis of GDPR Challenges to Behavioral Advertising', *Lowenstein Sandler*, [<https://www.lowenstein.com/media/4692/20181113-tech-group-an-analysis-of-gdpr-challenges-to-behavioral-advertising.pdf>].

Kaye, K. (2021), 'As ad tech firms test ways to connect Google's FLoC to other data, privacy watchers see fears coming true', *Digiday*, [<https://digiday.com/marketing/as-ad-tech-firms-test-ways-to-connect-googles-floc-to-other-data-privacy-watchers-see-fears-coming-true/>].

Kint, J. (2018), 'Why the IAB GDPR Transparency and Consent Framework is a non-starter for publishers', *Digital Content Next*, [<https://digitalcontentnext.org/blog/2018/03/19/iab-gdpr-consent-framework-non-starter-publishers/>].

Koetsier, J. (2020), 'Apple Just Crippled IDFA, Sending an \$80 Billion Industry Into Upheaval', *Forbes*, [<https://www.forbes.com/sites/johnkoetsier/2020/06/24/apple-just-made-idfa-opt-in-sending-an-80-billion-industry-in-to-upheaval/>].

Kostiuk, I. (2020), 'Ad Network vs. Ad Exchange – Programmatic Business Model', *Admixer*, [<https://blog.admixer.com/ad-network-vs-ad-exchange/>].

KPMG (2019), 'CJEU: Users must give 'active consent' for cookies', [<https://web.archive.org/web/20210516185309/https://home.kpmg/be/en/home/insights/2019/11/ta-cjeu-users-must-give-active-consent-for-cookies.html>].

McGee, M. (2015), 'As Google Analytics Turns 10, We Ask: How Many Websites Use It?', *MarTech*, [<https://martech.org/as-google-analytics-turns-10-we-ask-how-many-websites-use-it/>].

Naik, B. (2013), 'Tracking User Activities Using Web Bugs', *Infosec Institute*, [<https://resources.infosecinstitute.com/topic/tracking-user-activities-using-web-bugs/>].

Noyb (2021), 'noyb aims to end 'cookie banner terror' and issues more than 500 GDPR complaints', [<https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints>].

Olejnik, L. (2021), 'Initial privacy analysis of Google's Privacy Sandbox - Federated Learning of Cohorts leaking information about browsing in incognito mode', *Security, Privacy, and Tech Inquiries* [web blog], [<https://blog.lukaszolejnik.com/privacy-analysis-of-googles-privacy-sandbox-federated-learning-of-cohorts-leaking-information-about-browsing-in-incognito-mode/>].

Olejnik, L. (2021), 'Privacy of Google's Privacy Sandbox 2 - Federated Learning of Cohorts leaking user's visited websites?', *Security, Privacy, and Tech Inquiries* [web blog], [<https://blog.lukaszolejnik.com/privacy-of-google-privacy-sandbox-floc-leaking-visited-website-history/>].

OneTrust (2019), 'OneTrust Terms and Conditions – Cloud Deployment', [<https://www.onetrust.com/terms/OneTrustTermsConditionsUSCloudOneTrustStore.pdf>].

Oracle Data Management Platform Help Center, 'Oracle Data Marketplace', [<https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html>].

PricewaterhouseCoopers (2020), 'ISBA Programmatic Supply Chain Transparency Study', *ISBA*, [<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>].

Quantcast (2020), 'Quantcast Choice Terms of Service', [<https://www.quantcast.com/legal/quantcast-choice-terms-of-service/>].

Ryan, J. (2018), 'Critical data protection problems in the IAB's new OpenRTB 3.0 Spec', *Brave*, [<https://brave.com/iab-rtb-problems/>].

Ryan, J. (2020), 'The Commission's obligation to refuse an 'adequacy decision' to the United Kingdom due to inadequacy of enforcement of personal data protection in that jurisdiction', *Irish Council for Civil Liberties*, [<https://www.euractiv.com/wp-content/uploads/sites/2/2020/10/Letter-Brexit-Commission-data-ICO-12Oct2020.pdf>].

Schiff, A. (2020), 'Can LiveRamp Survive The Cookie Apocalypse?', *AdExchanger*, [<https://www.adexchanger.com/data-exchanges/can-liveramp-survive-the-cookie-apocalypse/>].

Schiff, A. (2021), 'Google Will Not Run FLoC Origin Tests In Europe Due To GDPR Concerns (At Least For Now)', *AdExchanger*, [<https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/>].

Simon, E. (2019), 'Prevent the Online Ad Industry from Misusing Your Data - Join the #StopSpyingOnUs Campaign', *Liberties*, [<https://www.liberties.eu/en/stories/stop-spying-on-us-fix-ad-tech-campaign/275>].

Ster (2020), 'A Future Without Advertising Cookies?', [https://www.ster.nl/media/h5ehvtx3/ster_a-future-without-advertising-cookies.pdf].

Stockley, M. (2015), 'Anatomy of a browser dilemma – how HSTS 'supercookies' make you choose between privacy or security', *Sophos*, [<https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/>].

Temkin, D. (2021), 'Charting a course towards a more privacy-first web', *Google Ads & Commerce Blog*, [<https://www.blog.google/products/ads-commerce/a-more-privacy-first-web/>].

The Privacy Collective (2020), ‘Dagvaarding’, [<https://www.rechtspraak.nl/SiteCollectionDocuments/RBAMS-dagvaarding-collectieve-vordering-Oracle-Nederland-BV-SFDC-Netherlands-BV-Oracle-Corporation-Oracle-America-Inc-Salesforce.pdf>].

Tiku, N. (2018), ‘What’s Not Included in Facebook’s “Download Your Data”’, *Wired*, [<https://www.wired.com/story/whats-not-included-in-facebooks-download-your-data/>].

Underwood, C. and Watson, C. (2021), ‘Birdwatching for Marketers: What Google’s FLoC & FLEDGE Mean for You’, *Search Discovery*, [<https://www.searchdiscovery.com/blog/floc-and-fledge-clarity-for-marketing/>].

Vivier, R. (2018), ‘Curious to understand how the programmatic advertising ecosystem (DSP, SSP, DMP) works in detail?’, *Digital Thought*, [<https://digitalthought.me/articles/digital-marketing/Programmatic-ad-bidding-cookie-sync.html>].

Vou, A. (2021), ‘Google and Facebook dominate behavioural advertising, even with the cookie crumbling’, *European Data Journalism Network*, [<https://www.europeandatajournalism.eu/eng/News/Data-news/Google-and-Facebook-dominate-behavioural-advertising-even-with-the-cookie-crumbling>].

W3Techs, ‘Usage Statistics and market share of Google Analytics for websites’, [<https://w3techs.com/technologies/details/ta-googleanalytics>].

Web Incubator CG, ‘floc’, *GitHub repository*, [<https://github.com/WICG/floc>].

Web Incubator CG, ‘turtledove’, *GitHub repository*, [<https://github.com/WICG/turtledove/blob/main/FLEDGE.md>].

Web Incubator CG, ‘privacy-preserving-ads – PARAKEET’, *GitHub repository*, [<https://github.com/WICG/privacy-preserving-ads/blob/main/Parakeet.md>].

Wong, J. (2018), ‘“It might work too well” the dark art of political advertising online’, *The Guardian*, [<https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy>].

Zvelo (2014), ‘Full Path URL Content Classification’, [<https://zvelo.com/content-classification-full-path-url-superiority/>].