REPHRAIN

Protecting citizens online

The Decline of Third-Party Cookies in the AdTech Sector: Of Data Protection Law and Regulation (I)

Asma Vranaki, University of Bristol

Francesca Farmer, University of Bristol

December 2022

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

The Decline of Third-Party Cookies in the AdTech Sector: Of Data Protection Law and Regulation (I)

Dr Asma Vranaki[*] and Dr Francesca Farmer[†]

1. Introduction

Nowadays, third-party cookies or similar technologies (TPC) routinely fuel modern digital advertising operations like data monitoring, data analytics, profiling, targeting and predictions. Simply, TPC are cookies or 'small, unique text files'[1] that are created by domains, other than the one visited by end-users, and dropped on their terminal equipment to record a broad range of 'personal data' including browsing behaviour, preferences, geo-location and real-time transactions. Personal data refers to any information that relates to an 'identified' or 'identifiable' person (or 'data subject').[2] Such personal data is then mined for advertising operations like profiling and drawing inferences. This report uses the term AdTech to refer to the diverse, opaque, highly fluid and complex actors, interdependencies, practices, techniques and processes that underpin today's advertising sector.[3] In Europe, the far-reaching impact of TPC operations on the individual's fundamental rights and freedoms, such as data protection and privacy, has long been recognised by key stakeholders, such as European data protection authorities (EU DPAs), policy actors and data protection law scholars.[4] EU DPAs are

[*] Senior Lecturer in Law, Law School, University of Bristol; Policy & Regulation Co-Lead of the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN); Principal Investigator. Email: asma.vranaki@bristol.ac.uk. For more on REPHRAIN, see <https://www.rephrain.ac.uk>.

[†] Post-doctoral researcher, Law School, University of Bristol (June 2021 to July 2022). All inquiries concerning this publication should be directed to the first author.

1 William T Harding, Anita J Reed and Robert L Gray, 'Cookies and Web bugs: What They Are and How They Work Together' (2001) 18(3) Information Systems Management 17.

2 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] OJ L119, 1 (hereinafter GDPR) Art 4(1) (definitions of personal data and data subject).

3 For definitions of the AdTech label, see Michael Veale and Frederick Borgesius, 'Adtech and Real-time Bidding under European Data Protection Law' (2022) 23(2) German Law Journal 226; Róisín Áine Costello, 'The Impacts of AdTech on Privacy Rights and the Rule of Law' (2020) Technology and Regulation 11, section 2; Damien Geradin and Dimitros Katsifis, '"Trust Me, I'm Fair": Analysing Google's Latest Practices in Ad Tech from the Perspective of EU Competition Law' (2020) 16(1) European Competition Journal 11, section II; Dylan Cooper, Taylan Yalcin, Cristina Nistor, Matthew Macrini and Ekin Pehlivan, 'Privacy Considerations For Online Advertising: A Stakeholder's Perspective to Programmatic' (2022) 7 Journal of Consumer Marketing.

4 See Eleni Kosta, 'Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies' (2013) 21 International Journal of Law and Information Technology 27; Rachel K Zimmerman, 'The Way the Cookies Crumble: Internet Privacy and Data Protection in the Twenty-first Century' (2000) 4 New York University Journal of Legislation & Public Policy 439; Damien Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster-Tracking the Crumbs of Online User Behavior' (2014) 5 Journal of Intellectual Property Information Technology & Electronic Commerce Law 194; Eleni Kosta, 'The Netherlands: The Dutch Regulation of Cookies (2014) 2 European Data Protection Law Review 97, 102; European Data Protection Board (EDPB), 'Statement 03/2021 on the ePrivacy Regulation' <https://edpb.europa.eu/system/files/2021-

independent supervisory authorities with a range of tasks, competences and powers including enforcing, overseeing and monitoring the application of the General Data Protection Regulation (GDPR) as well as resolving complaints.[5]

From a data protection law perspective, TPC-based processing operations can raise wide-ranging challenges like defective informational transparency,[6] unlawful TPC placement,[7] effectively navigating the complex legislative interplays (e.g. ePrivacy Directive and GDPR)[8] and unlawful processing of TPC data.[9] TPC processing also has broader ramifications for individuals, society and the economy: from 'surveillance capitalism'[10] to discrimination[11] to perpetuating and strengthening existing social inequalities[12] to commodifying people as consumers.[13]

03/edpb_statement_032021_eprivacy_regulation_en_0.pdf> accessed 24 November 2022; Proposal For a Regulation of the Parliament and of the Council (EU) Concerning the Respect for Private Life and the Protection Of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final (hereinafter ePrivacy Regulation).

5 See GDPR (n 2) Chapter 6; Asma Vranaki, 'Cloud Investigations by European Data Protection Authorities: An Empirical Account' in John A Rothchild (ed), *Research Handbook on Electronic Commerce Law* (Edward Elgar Publishing 2016a) 518; Asma Vranaki, 'Learning Lessons From Cloud Investigations in Europe: Bargaining Enforcement and Multiple Centers of Regulation in Data Protection' (2016b) 2 University of Illinois Journal of Law and Technology 245.

6 See Kosta, 'Peeking into the Cookie Jar' (n 4); Omer Tene and Jules Polenetsky, 'To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising' (2011) 13 Minnesota Journal of Law Science & Technology 281; Alessandro Mantelero, 'The Future of Consumer Data Protection in the EU Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30(6) Computer Law & Security Review 30(6) 643; Fred H Cate and Viktor Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (2013) 3(2) International Data Privacy Law 67; Solon Barocas and Helen Nissenbaum, 'Big Data's End Run Around Anonymity and Consent' in Julia Lane, Victoria Stodden, Stefan Bender and Helen Nissenbaum (eds), *Privacy, Big Data, and the Public Good* (Cambridge University Press 2014) 44.

7 See Section 4.2 below.

8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ 2002 L201, 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337, 11 (hereinafter ePrivacy Directive) and GDPR.

9 For example, the processing of TPC containing personal data in contravention of the applicable GDPR provisions.

10 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future At The New Frontier of Power* (2019 Profile Books).

11 Betsy Anne Williams, Catherine F Brooks and Yotan Shmargad, 'How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications' (2018) 8 Journal of Information Policy 78.

12 See Oscar H Gandy jr, 'Coming to Terms with the Panoptic Sort' (1996) Computers, Surveillance, and Privacy 132; John E Campbell and Matt Carlson, 'Panopticon. com: Online Surveillance and the Commodification of Privacy' (2002) 46(4) Journal of Broadcasting & Electronic Media 586.

13 See Asma Vranaki, *Regulating Social Networking Sites: Data Protection, Copyright, and Power* (Edward Elgar Publishing 2022) chapters 6 and 7; Meaghan Donahue, 'The "Times They are A-changing" – Can the Ad Tech Industry Surviv in a Privacy Conscious World?' (2021) 30(1) Catholic University Journal of

Against this backdrop, lately, web browsers with substantial market share in countries like Europe, such as Safari and Mozilla, have started blocking TPC.[14] Google Chrome, with a global market share of 64% of web users,[15] has once again recently revised its estimated timeframe for phasing out TPC, which has now been pushed back to the second half of 2024.[16] In anticipation of the upcoming TPC decline, prominent industry players, especially large multinationals like Apple Inc., Microsoft Corporation and Google LLC (Google), with the support of standardisation bodies like the World Wide Web Consortium,[17] are forging the path ahead in various ways. For example, they are developing and implementing new techniques, practices and processes that do not involve TPC data points, such as mining telco data[18] or using traditional forms of advertising like contextual campaigns in avant-garde ways, to transform and amplify their business intelligence operations (Strategies).[19] Several legal and non-legal reasons can account for TPC decline including the emergence of stricter and stronger data protection laws in countries like Europe and the United States; [20] the move towards responsible and trustworthy data stewardships prompted by such laws;[21] the commercial roll-out of web anti-tracking tools;[22] ongoing public concern about commercial data surveillance with its attendant 'bad optics'[23] and industry perceptions that the continued reliance on TPC is not 'sustainable… in the long term.'[24]

Law and Technology 197; Asma Vranaki, 'Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power' (2017) 43 Rutgers Computer & Technology Law Journal 168.

14 For example, Marissa Wood, 'Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining By Default' (*Dist://d,* 3 September 2019) <https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/> accessed 10 April 2022.

15 As of April 2022, Statcounter, 'Browser Marketshare Worldwide' (2022) <https://gs.statcounter.com/browser-market-share> accessed 10 April 2022.

16 Vinay Goel, 'An Updated Timeline For Privacy Sandbox Milestones' (*Google Chrome*, 24 June 2021) https://blog.google/products/chrome/update-testing-privacy-sandbox-web/ ; Chromium Blog, 'Building a More Private Web: A Path Towards Making Third Party Cookies Obsolete' (2020) <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html> accessed 5 August 2021.

17 For example, Interview with a representative of a non-EU DPA (2022) [hereinafter Interview 001]. See Section 3.2 below for more on the project's interviews.

18 For example, IAB Europe, 'A Guide to the Third Party Cookie Era' (*IAB,* February 2021) <https://iabeurope.eu/wp-content/uploads/2021/02/IAB-Europes-Updated-Guide-to-the-Post-Third-Party-Cooke-Era-February-2021-1.pdf> 36ff accessed 24 November 2022.

19 For example, Interview 001 (n 17) and Interview with the legal counsel of an AdTech company (2022) [hereinafter Interview 008]. See Section 3.2 below for more on the project's interviews.

20 See GDPR (n 2) (Europe); and California Consumer Privacy Act of 2018 AB-375, Title 1.81.5.

21 See Lee Bygrave, 'Data Protection By Design and By Default: Deciphering The EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105; Lina Jasmontaite, Irene Kamara, Gabriela Zanfir-Fortuna and S Leucci, Data Protection By Design And By Default: Framing Guiding Principles Into Legal Obligations in the GDPR' (2018) 4(2) European Data Protection Law Review.

22 IAB Europe (n 18) 15 ff.

23 For example, Interview with a PET Developer (2022) [hereinafter Interview 006] and Interview with a representative of an EU DPA (2022) [hereinafter Interview 009]. See Section 3.2 below for more on the project's interviews.

24 For example, Interview 009, *ibid*.

Considering this rapidly developing landscape, it is important (1) to fully understand the Strategies used by the AdTech sector and (2) to critically and comprehensively assess, from both legal and regulatory viewpoints, their implications for the level of protection afforded to the individual's data privacy rights. These are the two main objectives of the empirical project, on which this report draws, to address the normative, theoretical and empirical lacunas to date in the data protection law and regulation scholarship (see **Section 2**).[25] In the first instance, the project has produced the following two related reports:

a. This first report explores the range of data protection law issues raised by two Strategies, namely, first-party cookies and contextual advertising; and
b. A forthcoming second report will cover the implications of another emerging Strategy, namely, privacy-enhancing technologies from the lens of data protection law and regulation.[26]

This report advances **five** interconnected but distinct arguments. First, overall, contrary to current stakeholder assumptions, the upcoming TPC decline renders the 'regulatory space'[27] – in the sense of 'the range of regulatory issues subject to public decision'– from a data protection law lens, even more complex, unpredictable and fragmented than it was when TPC data fuelled AdTech operations. Specifically, the empirical findings underscore that many new Strategies like first-party cookies and contextual advertising involve an even broader range of complex, often intractable and extremely changeable actors, processes, techniques and interventions than those traditionally present in the TPC processing chain, which raise either brand-new or more convoluted data protection law issues that require careful, highly situated and evidence-based analyses. Second, the burgeoning use of first-party cookies to sustain personalisation, profiling, predictions and other AdTech activities, in anticipation of TPC decline, raises complex challenges, across plural, overlapping and distinct data protection law frameworks that must be accurately identified and fully addressed, on a case-by-case basis by all relevant actors including EU DPAs and AdTech players to effectively safeguard the individual's data privacy rights. Where appropriate, existing regulatory (including legislative) gaps, divergences and inconsistencies concerning key matters including the legality of cookie walls must be urgently and effectively addressed for a range of reasons including legal coherence and legal consistency. Third, and relatedly, it is imperative that some EU DPAs revisit their assumptions about and assessments of the impact of processing the personal data associated with first-party cookies on the level of protection afforded to data privacy rights. Such review should adopt evidence-based approaches that reflect current and projected (in the short and medium term at the very least) uses of first-party cookies in the industry. Fourth, it is crucial that current divergences between regulatory and policy actors about contextual advertising, including whether they use personal data and/or are forms of targeted advertisements, are effectively resolved using evidence-based approaches to promote regulatory coherence. Finally, in a similar fashion to first-party cookies, it cannot be assumed, without a contextual analysis, that particular contextual advertising campaigns do not interfere with the fundamental rights and freedoms of individuals. Such conclusions can only be reached following a

---

25 This project is funded by REPHRAIN (EPSRC Grant: EP/V011189/1).

26 Asma Vranaki and Francesca Farmer, 'The Decline of Third-Party Cookies in the AdTech Sector: Of Data Protection Law and Regulation (II)' (Forthcoming).

27 Leigh Hancher and Michael Moran, 'Organizing Regulatory Space: Capitalism, Culture and Economic Regulation' in Robert Baldwin, Colin Scott and Christopher Hood (eds), *A Reader on Regulation* (Oxford University Press 1989) 271, 277.

systematic and situated analysis that considers several factors including whether the captured content meets the personal data threshold.

These arguments are developed in the remaining four sections. The first section provides a high-level analysis of the data protection law and regulation literature on first-party cookies and contextual advertising to accentuate the current state of play and gaps – whether normative or empirical – in the scholarship, some of which are bridged by this report. The second section delves into the research methodology, methods and scope of the project that underpins this report. The third section zooms into the empirical findings concerning the new ways in which first-party cookies are being used in the AdTech sector, with TPC decline, before scrutinising the extensive data protection challenges – both legal and regulatory – raised by such fledgling practices. Finally, the report sheds innovative empirical light on the resurgence of contextual advertising in the AdTech sector before assessing their implications from the lens of data privacy regulation.

2. AdTech, Cookies and New Strategies: Of the Data Protection Law Literature

This section provides a high-level critical overview of the treatment of burgeoning TPC replacement Strategies like first-party cookies and contextual advertising in the European data protection law scholarship to underscore the existing gaps, whether normative or empirical, in the literature. In light of the existing gaps, whether normative of empirical, in the literature and the rapidly changing landscape at legal, technological and social levels, this section argues that it is imperative at this crucial juncture in the AdTech industry to evaluate anew to what extent such Strategies, as currently deployed on the ground, do interfere with the individual's data privacy rights.

A thorough exploration of the literature shows that to date the scholarship has engaged in depth, mostly from a doctrinal perspective, with the difficulties of lawfully placing or accessing TPC as well as processing TPC data in accordance with data protection laws.[28] Relatedly, many scholars have also analysed, again mostly from normative standpoints, the impact of diverse AdTech operations like real-time bidding;[29] ad targeting; [30] profiling[31] and data mining on the individual's fundamental rights and freedoms like data protection.[32] However, up to now, there has been a dearth of scholarly

[28] Clifford (n 4); Kosta 'Peeking into the Cookie Jar' (n 4); Ronald Leenes and Eleni Kosta, 'Taming the Cookie Monster with Dutch law–a Tale of Regulatory Failure' (2015) 31(3) Computer Law & Security Review 317; Omer and Polonetsky (n 6); Frederik Zuiderveen Borgesius, 'Behavioral Targeting, a European Legal Perspective (2013) 11(1) IEEE Security & Privacy 82; Mathew S Kirsch, 'Do-not-track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising' (2011) 18 Richmond Journal of Law & Technology 1; Klaus Wiedemann, 'The ECJ's Decision in "Planet49"(Case C-673/17): A Cookie Monster or Much Ado About Nothing?' (2020) 51(4) International Review of Intellectual Property and Competition Law 543; Agnieszka Jablonowska and Adrianna Michatowicz, 'Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies' (2020) 6 European Data Protection Law Review 137.

[29] See Veale and Borgesius (n 3).

[30] See Frederick Zuiderveen Borgesius, 'Personal Data Processing For Behavioural Targeting: Which Legal Basis?' (2015) 5(3) International Data Privacy Law 163; Georgia Skouma and Laura Léonard, 'On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Springer 2015).

[31] Sandra Wachter, 'Affinity Profiling and Discrimination By Association in Online Behavioral Advertising' (2020) 35 Berkeley Technology Law Journal 367.

[32] See Clifford (n 4); Veale and Borgesius (n 3).

commentary, either empirically or normatively, about the data privacy law implications of Strategies like first-party cookies (see **Section 4**) and contextual advertising (see **Section 5**). Work is now starting on evaluating the risks that some Strategies like differential privacy and fingerprinting pose to the individual's data privacy rights.[33]

The gaps in the literature concerning first-party cookies and contextual advertising are perhaps unsurprising given how these two Strategies have been used so far in the AdTech sector. For example, during the early days of the TPC era, first-party cookies were often set and accessed only by the visited domain with the collected data not shared with third parties. In such cases, legal compliance is often straightforward with, for example, the visited domain responsible for complying with the obligations for lawful placement and storage of first-party cookies and lawful processing of associated personal data. However, the context since the early days of TPC-fuelled AdTech operations has now significantly changed at a range of levels including operational and legal. As analysed in **Sections 4** and **5**, with the upcoming decline of TPC, first-party cookies and contextual and contextual advertising are being used in new ways in the AdTech sector and such new uses often raise complex data privacy law dilemmas. Relatedly, the AdTech landscape is in constant metamorphosis with the ongoing development of innovative practices, processes and techniques that aim to fine-tune operations like data capture, targeting, profiling and predictions. Likewise, the European legal landscape has also significantly shifted in recent years with the emergence of new laws, EU DPA guidance and decisions from the Court of Justice of the European Union (CJEU)[34] which often have important legal ramifications for many of the emerging Strategies.

Given such diverse and wide-ranging developments, it cannot be assumed that the renewed use of traditional Strategies like first-party cookies and contextual advertising is unproblematic. Rather, it is necessary to pause and reflect on whether the prevailing old-school views, be they in the literature or at regulatory level, stand up to scrutiny in today's highly fluid, experimental and innovation driven AdTech landscape. For instance, with the upcoming decline of TPC, in what ways are first-party cookies and contextual advertising now deployed on the ground for AdTech operations? What are their specific data flows? What particular data protection law challenges arise from the specific data flows involved in particular scenarios? What are the legal implications of the, often, new ways in which contextual advertising and first-party cookies operate nowadays? To what extent do First-Party Cookie Data points and contextual data points simply signal a move from particular data points, online identifiers and commercial surveillance practices to others that are still problematic from a data protection law standpoint?[35] These are crucial avenues of inquiries to shed a fuller light on the impact of Strategies like first-party cookies and contextual advertising on the individual's data privacy rights. Such investigations also bring to light the flawed assumptions and fundamental misunderstandings at play amongst those involved in the regulatory process, which threaten the effective safeguard of the individual's fundamental rights and freedoms like data protection and privacy.

Having surveyed the data protection law and regulation scholarship to evaluate its coverage, to date, of central aspects pertinent to this report including TPC, first-party cookies and contextual

33 Paarth Naithani, 'Practitioners' Corner: Regulating The Fingerprinting Monster Through EU Data Protection' (2021) 7(4) European Data Protection Law Review 184; Vranaki and Farmer (n 26).

34 See Sections 4 and 5 below.

35 Similar questions have also been raised by the project's respondents. For example, Interview 001 (n17); Interview 009 (n 23).

advertising and pinpointed the existing gaps (whether normative or empirical), next the project's methodology, methods and scope are considered.

3. Methods, Methodology and Scope

This section explores the project's research methodology, methods and scope.

3.1 Research Methodology

The project underpinning this report employs both socio-legal methods and doctrinal approaches to make sense, from empirical, legal and conceptual perspectives, of the impact of emerging Strategies in the AdTech sector on data privacy regulation. However, in this report, the doctrinal methodology is very much at the foreground to provide a critical analysis, from a normative standpoint, of the legal implications of first-party cookies and contextual advertising.[36] This legal analysis is essential to achieve one of the report's main objectives, namely, providing a critical and up-to-date analysis of the data protection laws governing first-party cookies and contextual advertising whilst engaging with important dimensions like gap analysis, regulatory inconsistency and regulatory incoherence. The socio-legal approach is very much in the background in this piece. Notwithstanding, it can often be detected in the report's empirical sections on, for example, the resurgence of Strategies like contextual advertising; the diverse and mutable practices, processes and techniques sustaining these Strategies; and the challenges of discharging and/or maintaining data protection compliance on the ground in particular empirical contexts.[37]

Despite the potential shortcomings of black-letter approaches including the exclusion of the broader set of interventions, actors and processes required on the ground for legal rules to be applied and enforced in practice, it is crucial that this methodology is at the foreground in this report, given the lack of sustained analysis, to date, in the literature of the data protection law implications of first-cookies and contextual advertising.[38] As recognised by other socio-legal scholars, where doctrinal analyses are nascent, a first essential step before engaging in rigorous interdisciplinary work[39] is to address such analytical gaps by evaluating, for instance, the meaning, clarity, coherence and defects of legal rules.[40] Here, to some extent, the authors avoid the limitations of a traditional 'black-letter

---

36 Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 8 Erasmus Law Review 130; Terry Hutchinson, 'Doctrinal Research: Researching the Jury' in *Research Methods in Law* (Routledge 2013) 15.

37 Naomi Creutzfeldt, Marc Mason and Kirsten McConnachie (eds), *Routledge Handbook of Socio-legal Theory and Methods* (Routledge 2019) Chapter 1.

38 *ibid*.

39 At this stage, the first author envisages using conceptual frames from socio-legal studies, regulation and science and technology studies to develop the future outputs that build on this report.

40 Hutchinson, 'Doctrinal Research: Researching the Jury' (n 36). For more on the importance of interpretation in doctrinal methodologies, see Mark Van Hoecke, 'Legal Doctrine: Which Method(s) for What Kind of Discipline?' in Mark Van Hoecke (ed), *Methodologies of Legal Research* (Hart Publishing 2011).

law'[41] approach by rigorously and systematically developing the legal analysis through an in-depth engagement with the on-ground practices and processes that sustain these Strategies.[42]

Leaving aside methodological matters, next, the report indicates the project's main research methods.

3.2 Methods

The empirical project, underpinning this report, draws on two main data collection methods, namely, interviews and documentary analysis.

Following institutional and research centre ethical clearance approvals,[43] the authors qualitatively analysed several documents including:

a) Current[44] data protection laws at European and member state levels;
b) Relevant judicial decisions from the CJEU;[45]
c) Opinions, guidelines and official decisions from relevant European data privacy regulatory actors like the European Data Protection Board (EDPB), the now defunct Article 29 Working Party (A29WP) and EU DPAs.[46] The analyses of opinions, guidelines, decisions and other outputs from EU DPAs, such as the French and Belgian DPAs, are based on the first author's own translation of these documents. The analyses of the opinions and guidelines of other EU DPAs like the Italian, German and Spanish DPAs are based on either the translations provided on the relevant EU DPA's website and/or on translations provided by Google Translate;[47]

---

41 Hutchinson, 'Doctrinal research: researching the jury' (n 36) 12.

42 Creutzfeldt, Mason and McConnachie (n 37).

43 Email dated 11 October 2021 from the University of Bristol Law School Research Ethics Committee to the authors granting ethical approval (on file with the first author) and email dated 23 November from the REPHRAIN Ethics Board to the authors granting ethical approval (on file with the first author).

44 See GDPR (n 2); ePrivacy Directive (n 8); the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (SI No 336 of 2011); Data Protection Act 2018 (Number 7 of 2018) (Ireland).

45 See Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C:2019:801, [2019] ECR 00000 (hereinafter *Planet 49*); Case C-184/20 *Vyriausioji Tarnybinės Etikos Komisija v Fondas 'Nevyriausybinių Organizacijų Informacijos Ir Paramos Centras'* EU:C:2022:601,[2022] ECR 00000; Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779, [2016] ECR 00000; C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* EU:C:2019:629, [2019] ECR 00000.

46 The A29WP was an actor under the old 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) [1995] OJ L281/31 [hereinafter Data Protection Directive]. It was an advisory body composed of representatives of the EU DPAs, the European Data Protection Supervisor and the European Commission and often issued guidelines, opinions and recommendations for the implementation, application and interpretation of the Data Protection Directive. Now that the GDPR is in force, it has been replaced by the EDPB. For more on the EDPB, see GDPR Arts 68–76 (n 2).

47 See A29WP, 'Opinion 04/2012 on Cookie Consent Exemption' (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 8 July 2022; A29WP, 'Opinion 4/2007 on the

d) Where relevant, guidance from non-European data protection authorities; [48]
e) Relevant white papers and other policy documents from European institutions;[49]
f) Outputs from AdTech industry bodies like the European Interactive Advertising Bureau (IAB);[50] and
g) Outputs including press releases from key AdTech players.[51]

This evaluation helped the authors to (1) gain a deeper understanding of the rapidly shifting AdTech landscape at policy, regulatory, industry and legislative levels, (2) identify core stakeholder groups active in this arena for interview purposes and (3) devise suitable interview questions.

Following such investigations, the authors identified three core stakeholder groups that would provide thorough and novel insights into the emerging Strategies in the AdTech industry and their attendant data protection law pressure points, namely:

a. AdTech industry players operating in Europe (e.g. browsers, advertisers, industry associations and publishers);
b. EU DPAs, data protection authorities in other relevant jurisdictions and non-data protection regulators in relevant jurisdictions; and
c. Entities developing privacy-enhancing technologies with European operations (PET Developers).

Following the desk-based research, the authors identified over **twenty** potential respondents belonging to the three above-mentioned stakeholder groups. The authors then started recruiting

Concept of Personal Data' (2007) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> accessed 8 July 2022; A29WP, 'Opinion 2/2010 on Online Behavioural Advertising (WP 171)' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 24 November 2022; EDPB statement 03/2021 (n 4); Belgian DPA, 'Cookies et Autres Traceurs' (2020) <https://www.autoriteprotectiondonnees.be/cookies > accessed 8 July 2022; Commission Nationale de l'informatique et des Libertés (CNIL), 'Deliberation of the Restricted Committee n° SAN-2020-012 of 7 December 2020 concerning Google LLC and Google Ireland Limited' (2020) <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_restricted_committee_san-2020-012_of_7_december_2020_concerning_google_llc_and_google_ireland_limited.pdf> accessed 8 July 2022.

48 See ICO, 'Information Commissioner's Opinion: Data Protection and Privacy Expectations for Online Advertising Proposals' (2021) <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf> accessed 15 May 2022.

49 For example, European Commission, 'Privacy Enhancing Technologies (PETs)' (EC memo 07/159, 2 May 2007) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_07_159/MEMO_07_159_EN.pdf> accessed 24 November 2022; European Commission, 'Shaping Europe's Digital Future' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en> accessed 24 November 2022; EDPS, 'Shaping a Safer Digital Future: a New Strategy for a New Decade' (*EDPS,* 2022) <https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en> accessed 24 November 2022.

50 See IAB, 'The IAB Guide to Contextual Advertising' (*IAB,* 2021) >https://iabeurope.eu/wp-content/uploads/2021/07/IAB-Europe-Guide-to-Contextual-Advertising-July-2021.pdf> accessed 24 November 2022.

51 For example, Meta, 'Privacy-Enhancing Technologies and Building for the Future' (*Facebook,* 2021) <https://www.facebook.com/business/news/building-for-the-future> accessed 8 April 2022.

potential interviewees and interviewed a total of **15** respondents, split across each stakeholder group, between January and March 2022.[52] It should be noted that the interviews with AdTech industry players like browsers would often yield data relevant to PETs.[53] Overall, the empirical interviews aimed to provide the authors with first-hand and rich qualitative accounts of the diverse Strategies, either currently being developed or utilised in the AdTech sector, to re-invigorate practices like data capture, data mining, profiling, targeting and predictions in the absence of TPC. The interviews also intended to provide the authors with sufficient empirical data about the inner workings of each strategy so that they could develop a thorough and contextual analysis of the precise data privacy law challenges raised by particular Strategies. Throughout the interview design phase, the authors considered a range of matters including identifying the organisations, companies and institutions, within the three core stakeholder groups, that would most likely provide up-to-date, new, detailed and comprehensive insights into key areas relevant to the project to ensure that the sample size was valid, reliable and representative for the purposes of qualitative analysis.[54]

The qualitative interviews were conducted via Microsoft Teams, on a non-attributable basis. Thus, the identities of the respondents cannot be disclosed in this report and subsequent project outputs. Each interview lasted for around one hour, was recorded (where respondent consent was obtained) on a secure device for transcription purposes only and were transcribed verbatim by a University of Bristol approved transcriber to aid data analysis. All stages of data management, from capture to storage to deletion to security to transparency adhered to the requirements of UK data protection laws, which are the applicable frameworks as the authors are based in the UK. Where necessary, the interviewer would ask follow-up questions to gain more insights into some of the practical compliance dilemmas and how they are resolved. The authors used several data analysis techniques including explanation building to ensure rigorous and systematic data analysis.[55] They also used a range of diverse techniques like reading the transcripts in full on multiple occasions as well as identifying, comparing, contrasting and classifying information by using mind-maps to generate reliable findings.[56]

---

52 Interview 001 (n 17); Interview with a representative of an AdTech player (2022) [hereinafter Interview 002]; Interview with another AdTech industry player (2022) [hereinafter Interview 003]; Interview with a representative of another AdTech industry player (2022) [hereinafter Interview 004]; Interview with a representative of a non-data protection regulator (2022) [hereinafter Interview 005]; Interview 006 (n 23); Interview with another AdTech industry player (2022) [hereinafter Interview 007]; Interview 008 (n 19); Interview 009 (n 23); Interview with a representative of another EU DPA (2022) [hereinafter Interview 010]; Interview with a representative of another AdTech player (2022) [hereinafter Interview 011]; Interview with a representative of another AdTech player (2022) [hereinafter Interview 012]; Interview with a representative of another PET Developer (2022) [hereinafter Interview 013]; Interview with a representative of another AdTech industry player (2022) [hereinafter Interview 014] and Interview with a representative of another EU DPA (2022) [hereinafter Interview 015].

53 For example, Interview 008 (n 19).

54 Alan Bryman, *Social Research Methods* (Oxford University Press 2012) 416; Carol Warren, 'Qualitative Interviewing' in Jaber F Gubrium and James A Holstein (eds), *Handbook of Interview Research: Context and Method* (Sage 2002) 83, 99; Mira Crouch and Heather McKenzie, 'The Logic of Small Samples in Interview-Based Qualitative Research' (2016) 45(4) Soc Sci Info 483.

55 See Lisa Webley, 'Qualitative Approaches to Empirical Legal Research' in Peter Cane and Herbert M Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010).

56 See Carina Fearnley, 'Mind Mapping in Qualitative Data Analysis: Managing Interview Data in Interdisciplinary and Multi-Sited Research Projects' (2022) 9 Geography and Environment.

Following the exploration of the project's research methodology and methods, next, four points about the scope of the project are outlined.

3.3 Scope

To start, this project (and its accompanying outputs) engages with the regulatory (including legal) issues raised by the emerging Strategies in the AdTech industry from a European data protection law lens. Consequently, although Strategies like First-Party Cookie Data and contextual advertising raise competition law issues, like the emergence of 'walled gardens' in first-party cookie ecosystems,[57] these are outside this report's scope.

Second, some readers may wonder why this report does not engage with the development of interest-based or cohort-based advertising in the AdTech sector. The empirical data clearly shows that many stakeholders consider that such forms of advertising will play a crucial role in the sector in the future as TPC declines.[58] However, after careful reflection, the authors have decided to exclude interest-based advertising from the current deliverables of the project, for the time being, because of the demise of Google's Federated Learning of Cohorts (FLOC) in Europe, shortly after its initial trial, on data privacy law grounds.[59] In a nutshell, FLOC aimed to replace cookie-based advertising with interest-based advertisements.[60] Although Google has already announced FLOC's successor, namely, Topics, at the time of writing, the API for Topics has still not been finalised.[61] Thus, it is not yet possible to undertake a meaningful analysis of its compliance with European data protection laws. The authors will revisit interest-based advertising in future outputs either when the API for Topics is finalised and/or when another mature contender appears on the market.

Third, it would be impossible within the space constraints of this one report to engage in-depth with all the data protection law issues, especially under the GDPR, raised by the resurgence of first-party cookies and contextual advertising within the AdTech sector. Consequently, Sections 4 and 5 intend to provide a top-level analysis of the most pressing GDPR compliance challenges accentuated by the project findings to emphasise the extensive legal ramifications of the new Strategies and stimulate stakeholder discussions and developments in this arena.

Finally, although the report occasionally references the ePrivacy Regulation, [62] it is not within its ambit to explore its ramifications for the new Strategies covered in this report. This is by design to ensure that the analysis presented in this report reflects accurately the contributions of the project

---

57 For example, Interview 005 (n 52).

58 For example, Interview 001 (n 17); Interview 002 (n 52) ; Interview 005 (n 52); Interview 008 (n 19); Interview 010 (n 52); Interview 014 (n 52).

59 Vinay Goel, 'Get to know the new Topics API for Privacy Sandbox' (*Chrome*, 2022) <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/> accessed 20 May 2022.

60 Frederic Lardinois, 'Goodle Kills Off FloC, Replaces it with topics' (*Techcrunch+,* 25 January 2022) <https://techcrunch.com/2022/01/25/google-kills-off-floc-replaces-it-with-topics/> accessed 24 November 2022.

61 Github, 'The Topics API: Draft Proposal' (*GitHub*) <https://github.com/patcg-individual-drafts/topics> accessed 24 November 2022; Reuben Scrueurs, 'Take a Deep Breath and Consider the Benefits of Google's Topics API' (*AdExchanger,* 2022) < https://www.adexchanger.com/ad-exchange-news/take-a-deep-breath-and-consider-the-benefits-of-googles-topics-api/> accessed 24 November 2022.

62 See ePrivacy Regulation (n 4).

respondents. It is perhaps unsurprising that none of the interviewees mentioned the upcoming ePrivacy Regulation during the interviews given that the trilogue process is still under way at the time of writing.

Having explored the scope, methodology and methods of the project, the report now explores in-depth two of the main Strategies that emerge from the project findings, namely, first-party cookies and contextual advertising.

4. First-Party Cookies: Of Plural Data Protection Laws, Flawed Assumptions and Pressure Points

The empirical findings underscore that first-party cookies, and their associated personal data (First-Party Cookie Data) are being used afresh by AdTech players to fuel operations like data tracking, data mining, profiling, targeting and ad measurement. First-party cookies are set by the website (or host domain) visited by the end-user.[63] The section starts by examining the empirical data before outlining the complex, fragmented and plural laws that govern lawful cookie storage and access as well as lawful processing of cookie data including First-Party Cookie Data. Then, it applies this legal analysis to evaluate the data protection law implications of first-party cookies. Overall, two main contentions are advanced. First, the burgeoning use of **first-party cookies** to sustain personalisation, profiling, predictions and other AdTech activities, in anticipation of TPC decline, raise **complex challenges** across plural, overlapping and distinct data protection law frameworks that must be **accurately identified and addressed**, on a **case-by-case basis**, by all relevant actors including EU DPAs and AdTech players to safeguard the individual's **fundamental rights and freedoms**. Second and relatedly, it is imperative that **EU DPAs** revisit their **assumptions** about and **assessments** of the impact of **First-Party Cookie Data** processing on the level of protection afforded to the **individual's data privacy rights**. Such review should adopt **evidence-based approaches** that reflect current and projected uses of First-Party Cookie Data in the AdTech ecosystem with attendant repercussions on **enforcement priorities**, where appropriate.

4.1 The Rise of First-Party Cookies in AdTech

Before proceeding to the legal analysis, it is important to flesh out the project's findings on the growing roles of first-party cookies in the AdTech chain.

First-party cookies are evidently not new additions to the AdTech ecosystem. Although they were initially conceived in 1994 to facilitate web use by determining whether end-users are first-time or repeat website visitors,[64] nowadays, first-party cookies are used for several purposes including first-party data tracking, fraud detection and law enforcement.[65] The project's findings signal a clear transformation in the use of First-Party Cookie Data in the AdTech sector, in anticipation of TPC

63 eg ENISA, 'Privacy Considerations of *online behavioural tracking*' (*ENISA*, 2012) <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking/> 3 accessed 24 November 2022; Nuruallah Demir, Daniel Theis, Tobias Urban and Norbert Pholmann, 'Towards Understanding First Party Cookie Tracking in the Field' (2022) ARXIV <https://www.researchgate.net/profile/Tobias-Urban-3/publication/358046747> accessed 24 November 2022; Clifford (n 4) 195.

64 See Jay P Kesan and Rajiv C Shah, 'Deconstructing Code' (2003) 6 Yale Journal of Law & Technology 277, 299.

65 See Tene and Polenetsky (n 6) 305.

deprecation, with a wide range of real-time and historical personal data held by publishers (or website operators) – be it people's reading, transactional, viewing or interactional patterns – being introduced in the broader AdTech chain for, for example, onward sharing with an extensive and ever-growing range of AdTech players to monitor, profile, target and draw inferences about those visiting the publisher's website.[66] For instance, as explained in **Section 5**, First-Party Cookie Data can be merged with other data sources like contextual signals to further refine ad-targeting strategies to maximise conversion rates or, in other words, influence people to act on the advertisement in question[67] As another example, publishers can merge First-Party Cookie Data points with other data they hold about end-users to build more extensive and comprehensive consumption profiles that can be mined for several purposes like predicting people's medium or longer term needs. Consequently, this marks an important shift in the sector with First-Party Cookie Data being used in new ways to bolster manifold advertising practices, processes and techniques like contextual advertising, targeting and profiling.

The increasing roles that first-party cookies play in the AdTech sector is perhaps unsurprising. It provides the industry with sophisticated audience segmentation metrics, enables them to serve people with even more personalised content and promotions, boosts audience engagement and conversion metrics and seemingly places publishers at the heart of responsible and lawful data stewardship.[68] Surprisingly, given the new roles of First-Party Cookie Data within the AdTech ecosystem, many respondents, including EU DPAs, have indicated that they are not as concerned about the impact of first-party cookies on the individual's data protection and privacy rights.[69] Some assert that the line of data stewardship is clear, with first parties being the only ones to set and access first-party cookies and process First-Party Cookie Data .[70] Others contend that the processing of First-Party Cookie Data minimally impacts on data privacy rights due to lack of third-party data sharing.[71] However, as analysed in **Section 4.3.1** below, such assumptions are fundamentally flawed as, depending on the nature, scope, purposes and context of processing, the new ways in which First-Party Cookie Data fuel end-user profiling, targeting and monitoring can interfere with the individual's data privacy rights. Relatedly, some EU DPAs like the French DPA have flagged that this new strategy may impact on data privacy rights.[72]

Before tackling these points further, it is important to outline the legal rules on the lawful placement of and access to cookies and similar technologies, including first-party cookies, on end-user terminal equipment and the lawful processing of cookie data including First-Party Cookie Data.

4.2 Lawful Cookie Storage, Access and Data Processing: A Primer on European Data Protection Laws

66 For example, Interview 003 (n 52); Interview 005 (n 52); Interview 006 (n 23); Interview 010 (n 52); Interview 011 (n 52); Interview 012 (n 52); Interview 015 (n 52); IAB (n 50) 10.

67 *ibid* IAB.

68 Interview 005 (n 52); Interview 006 (n 23); Interview 010 (n 52).

69 Interview 001 (n 17); Interview 009 (n 23); Interview 015 (n 52).

70 See Commission Nationale de l'informatique et des Libertés (CNIL), 'Alternatives to Third-party Cookies: What Consequences Regarding Consent?' (2021) <https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent > accessed 8 July 2022.

71 Interview 001 (n 17); Interview 009 (n 23); Interview 015 (n 52).

72 CNIL (n 70).

This section provides a high-level analysis of the main European data protection law provisions that govern (1) cookie storage and access and (2) processing of cookie data containing personal data. For analytic ease, the general European legal position is considered without exploration of the national laws, at member state level, that, for instance, implement European legislative instruments like the ePrivacy Directive or legislate in GDPR derogation areas.[73]

As long recognised in the European data privacy law and regulation scholarship, the European cookie legislative landscape is complex, fragmented and overlapping with two legal instruments, namely, the ePrivacy Directive,[74] as nationally implemented by European member states, and the GDPR applicable.[75] The lawful placement of cookies and similar technologies on end-user equipment, such as mobile devices and personal computers, is governed by Art 5(3) of the ePrivacy Directive,[76] whilst the processing of cookie data, where the material and territorial scope of the GDPR are met, is governed by the latter.[77] It is important, at this juncture, to understand the relationship between the two legal instruments. The ePrivacy Directive is a *lex specialis* whose provisions 'particularise and complement' the GDPR, a *lex generalis*.[78] Consequently, the ePrivacy Directive and GDPR co-exist with one another with the ePrivacy Directive taking precedence, as a *lex specialis*, in cases where it provides specific rules governing particular processing operations. In other cases, where it does not provide specific rules, then the GDPR, as *lex generalis,* applies if the processing operations fall within its ambit.[79]

Let us consider the **cookie storage** and **access** legal regime further. To start with, unless exempted, the storage of information like cookies on end-users' terminal equipment or access to such information is only permissible if two cumulative conditions are met, namely, providing end-users with 'clear and comprehensive information' about matters like the processing purposes and eliciting valid end-user consent to such information storage and/or access irrespective of whether personal data is processed or not.[80] Both conditions must satisfy the relevant GDPR requirements and other applicable

---

73 For example, in jurisdictions like Ireland, the ePrivacy Directive has been nationally implemented by the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (SI No 336 of 2011). Ireland has also enacted the Data Protection Act 2018 (n 44) to, in part, legislate in GDPR derogation areas.

74 See ePrivacy Directive (n 8); Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul de Hert (eds), *Data Protection in a Profiled World* (Springer 2010); Jos Dumortier, 'Evaluation and Review of the ePrivacy Directive' (2016) 2 European Data Protection Law Review 247.

75 See GDPR (n 2); Vranaki, 'Social networking site regulation' (n 13) 169; Orla Lynskey, 'Track[ing] Changes: an Examination of EU Regulation of Online Behavioral Advertising Through a Data Protection Lens' (2011) 36(6) European Law Review 874, 876.

76 See also Poullet (n 74) and Dumortier (n 74).

77 GDPR Arts 2 (material scope), 3 (territorial scope), 12 (transparency modalities), 7 (conditions for consent) and 4(11) (definition of consent) (n 2).

78 ePrivacy Directive Art 1(2) (n 8).

79 See EDPB, 'Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (*EDPB,* 2019) section 4 <https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 24 November 2022; GDPR (n 2) Recital 173.

80 ePrivacy Directive Art 5(3). The two exemptions are the communications and 'strictly necessary' exemptions. For more see A29WP, Opinion 04/2012 (n 47).

national data protection laws.[81] Thus, information, such as, the identity of the controller (or the entity that solely or jointly decides the processing 'purposes' and 'means'),[82] the processing purposes, the data recipients, third-country data transfers and the exercise of data subject rights including subject access requests, must be provided to end-users.[83] Such information has to meet all the GDPR **transparency** requirements including concision, intelligibility, accessibility and clarity[84] with, where suitable, layered approaches including standardised icons and 'other means'[85] deployed to provide end-users with an 'easily visible, intelligible'[86] and accessible outline of the processing operations. When it comes to consent, it must be obtained to store information like cookies on their terminal equipment or gain access to such stored information **before** cookies or similar technologies are placed on end-user equipment.[87] **Valid consent** must meet the four, often intertwined, GDPR mandated ingredients, namely, being 'freely given', specificity, 'informed' and being an 'unambiguous indication' of the end-user's agreement to the processing.[88] It must also adhere to all the legally-mandated conditions including revocation; simple and accessible consent request and no tie-ins between the consent document and other documents.[89] Recent judicial developments have confirmed that, *inter alia*, valid consent, for purposes of Art 5(3) of the ePrivacy Directive, cannot be evinced through pre-checked boxes that end-users must deselect to withhold their consent.[90]

Whilst the ePrivacy Directive governs the lawful storage of cookies and similar technologies, the **processing** of **cookie data** is governed by the GDPR where threshold concepts like material scope, territoriality and personal data are met. For information to amount to personal data, it must satisfy four core cumulative ingredients, namely, 'any information'; 'relating to'; 'identified and identifiable' and 'natural person'.[91] Specifically, the GDPR provides that identifiers, such as online identifiers, can render an individual identifiable.[92] This is crucial in determining whether, considering the processing scope, nature, purpose and context, cookie data amounts to personal data. For instance, where cookie data can be linked to a name, email address or unique identifier that singles out individuals to track

81 For instance, in European member states like Ireland, consent and transparency must comply with the relevant GDPR and Irish Data Protection Act 2018 (n 44) provisions.

82 GDPR Art 4(7) (n 2).

83 GDPR Art 13 (n 2).

84 GDPR Art 12(1) (n 2).

85 GDPR Art 12(1) (n 2).

86 GDPR Art 12 (7) (n 2).

87 For example, EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (*EDPB,* 2020) 90 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.> accessed 24 November 2022.

88 GDPR Art 4(11) (n 2).

89 GDPR Art 7(2) (form of consent request and lack of tie-in); 7(3) (revocation) and 7(4) (freely given) (n 2).

90 *Planet49* (n 45).

91 For a high-level analysis of the CJEU jurisprudence and European data protection law stance on personal data, see Lee Bygrave and Luca Tosoni, 'Article 4(1), Personal Data' in Christopher Kuner, Lee Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2020) 103; see also A29WP, 'Opinion 04/2007 on the concept of personal data' (2007) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf > accessed 24 November 2022.

92 GDPR Art 4(1) (n 2).

browsing behaviour[93] it will amount to personal data. The broader question of identifiability is not addressed in the main legal text of the GDPR but rather in its recitals, which although instructive are not binding. Specifically, recital 26 provides, *inter alia*, that the determination of whether a person is identifiable requires considering all the means 'likely reasonably' to be used by the controller or another person to identify the person. Recital 30 also emphasises that online identifiers like device and cookie identifiers can be linked to a natural person to, for instance, authenticate and profile them, and can, consequently, amount to personal data.[94]

Having outlined the law, the report now turns to the legal implications of storing and accessing first-party cookies for AdTech operations.

4.3 First-Party Cookies: European Data Privacy Regulation Challenges

This section analyses **four** overarching legal and regulatory dilemmas raised by the expansive deployment of first-party cookies in the AdTech chain. Where relevant, guidance from a range of regulatory actors in the data protection law sphere in Europe and CJEU judicial decisions, are considered to advance the analysis. Recommendations are also presented to address the regulatory (including legal) gaps and weaknesses identified.

4.3.1 First-Party Cookie and Data Privacy Rights: Of Fundamental Misconceptions and Assumptions

To start, the project's findings emphasise a **lack of regulatory concern** and **enforcement appetite**, amongst respondents, about the invigorated roles of first-party cookies within the AdTech chain. [95] This corresponds to the current guidance issued by some EU DPAs like the Irish DPA who do not consider first-party analytic cookies as an enforcement priority.[96] The Irish DPA assumes that first-party analytic cookies are only deployed for aggregated statistical purposes with adequate information provided to end-users about the cookie processing activities and an accessible and easy-to-use opt-out mechanism. This section critically explores the potential reasons for such stance and evaluates whether it is justified.

Several factors can explain the project's findings and broader perspective adopted by some EU DPAs. For instance, in the past, the now defunct A29WP has provided instructive but non-binding guidance that first-party analytics cookies used only for first-party aggregated statistical purposes are unlikely to raise impact on end-user data privacy rights as long as they meet the transparency requirements.[97] This opinion forms the basis of the current Irish DPA guidance on first-party cookies. However, it is unreasonable to rely on this dated, 10-year-old guidance confined only to the use of first-party cookies for first-party aggregated statistical purposes, to write a blank 'compliance cheque' for all first-party cookie processing. As highlighted before, the legislative landscape, since the

93 See A29WP, Opinion 02/2010 (n 47).

94 GDPR Recital 30 (n 2).

95 See A29WP, Opinion 04/2012 (n 47) 7–8. Regulators in other jurisdictions like the UK strongly disagree with the European consensus; see ICO (n 48) section 4.

96 Data Protection Commission of Ireland, 'Guidance Note: Cookies and Other Tracking Technologies' (April 2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> 8 accessed 24 November 2022.

97 See A29WP history (n 46) and EDPB; GDPR Arts 68–76 (n 2).

guidance, has drastically evolved. There are now new and stricter legal rules on personal data processing, many of which impact on placing and accessing first-party cookies and processing First-Party Cookie Data. Likewise, nowadays, as explored earlier, first-party cookies play a more predominant role than anticipated in the guidance in sustaining several AdTech practices like extensive data monitoring, mining, targeting and profiling which depending on the processing context, which can interfere to varying levels with the individual's data protection and privacy rights.[98] Their usage in the AdTech ecosystem is likely to continue to grow as AdTech actors are encouraged by key industry players like the IAB to capitalise fully on first-party data to sustain their activities.[99]

What else can potentially explain this regulatory position? As underlined by some data privacy regulators, the terms first-party and third-party often have distinct definitions in spheres like web standards, marketing data categorisation and law (e.g. data protection and contract law).[100] For instance, the first-party/third-party dichotomy is used in web standards to differentiate between the visited website's content and services and those loaded by other parties. In marketing, first-party data refers to data that organisations obtain directly from individuals as they interact with and use their offerings.[101] Third-party data refers to, typically, consolidated datasets across several sources, which are licensed to third parties for purposes like marketing.[102] These distinct definitions may also partly explain the over-simplifications, misunderstandings or false assumptions about first-party cookies including assumed clear lines of responsible data stewardship and accountability; absence of large-scale multi-actor data sharing and monitoring; and low-level data privacy risks.[103] However, in line with well-established and sound data protection law principles, it cannot be assumed without a case-by-case analysis, considering the nature, scope, means and purposes of processing, that the use of specific first-party cookies for AdTech operations like personalisation and targeting pose minimal or no data privacy risks to individuals. [104] Thus, it is **imperative** that **EU DPAs** clarify the legal position in this regard based on **reliable and systematic evidence** of **first-party cookies'** growing roles in the sector.

Having explored why some EU DPAs may not deem first-party cookies as priority enforcement and oversight areas and gauged whether such perspectives are justified, next, the report considers to what extent the lawful storage of and access to first-party cookie for these new AdTech purposes is uncomplicated.

4.3.2 First-Party Cookie Storage and Access for AdTech: Of Lawfulness

This section contends that in practice, depending on the processing context, it can be an **arduous** task to satisfy the legal conditions for the **lawful storage** of and **access** to **first-party cookies** for AdTech

98 DPAs in jurisdictions like the UK share similar views; see ICO opinion (n 48).

99 IAB, 'IAB guide to in-app advertising' (*IAB,* 2022) <https://iabeurope.eu/wp-content/uploads/2022/02/IAB-Europe-Guide-to-In-app-advertising.pptx.pdf> accessed 24 November 2022.

100 *ibid*.

101 Data and Marketing Association, 'DMA Advice: Using Third Party Data Under the GDPR' (*DMA,* 2018) 4<https://dma.org.uk/uploads/misc/third-party-data-guide-1.0.pdf> accessed 8 July 2022.

102 *Ibid*, 6.

103 For example, Interview 010 (n 52).

104 Some non-EU DPAs like the UK DPA have adopted this position; see ICO (n 48) 37ff.

operations including personalisation, data capture, data mining and targeting. This argument is developed in three stages. First, general aspects like lines of responsibility and cookie lifespans are explored. Second, the report explores in-depth the difficulties in practice of discharging informational transparency in this changed landscape. Finally, the report analyses to what extent it is easy or not to elucidate valid consent in such situations.

4.3.2.1 First-Party Cookies: Of Responsibility Lines and Cookie Duration

To start, as explored in **Section 4.2**, unless exempted, first-party cookies can only be lawfully dropped on end-user terminals (and accessed) for AdTech purposes if two conditions, namely, transparency and valid consent, are met. Before considering these ingredients further, it is important to examine two crucial preliminary points. First, the refreshed applications of first-party cookies, with TPC decline, means that data flows are becoming far more convoluted, unpredictable and changeable. For example, publishers continually combine diverse and incredibly rich First-Party Cookie Data points like geo-location, biographical data, demographic data and real-time online activities with data points they hold about end-users for AdTech activities like audience segmentation, targeting and conversion measurements. They can also share such data with an ever-expanding range of third parties for AdTech activities. In this fluid landscape, which entities are best placed to discharge both obligations? Traditionally, publishers would be **responsible** for delivering effective informational transparency and obtaining end-user consent for cookie storage and access. However, is this still a foregone conclusion? Or are there circumstances where publishers are not the right or only parties that should be responsible for discharging the transparency and consent obligations? For instance, where third parties process particular First-Party Cookie Data points for operations like data matching and targeting to what extent can publishers discharge informational transparency for such third-party processing, obtain granular consent for each third-party operation and manage important aspects like consent revocation and the exercise of data subject rights? This primordial question is unaddressed in the ePrivacy Directive. So far, few EU DPAs have offered guidance on this salient compliance question. For instance, building on the GDPR controllership test, the French DPA advises that, depending on the processing context, third parties that determine, either solely or jointly, the means and purposes of processing are either sole or joint controllers, respectively.[105] In cases of joint controllership, publishers and third parties must clearly define their obligations for the processing including the extent to which they are responsible for discharging compliance with the ePrivacy Directive conditions.[106] Thus, going forward, **it is crucial that all EU DPAs provide clear and consistent regulatory guidance on this fundamental question.**

Second, since the CJEU's *Planet 49* decision, it is established jurisprudence that the **cookie retention period** must be indicated in cookie policies.[107] However, this raises an important question, namely, what is the appropriate retention period for first-party cookies? So far, regulatory guidance

105 GDPR Art 26(1) (n 2); Commission nationale de l'informatique et des libertés (CNIL), 'Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) et abrogeant la délibération n° 2019-093 du 4 juillet 2019' <https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf> accessed 24 November 2022 [36] [37] and [39]. For more information on the translation of the sources analysed, see Section 3.2 (c) (hereinafter Translation).

106 *ibid*.

107 *Planet 49* (n 45) [81].

on this question is often either absent, sparse or not harmonised. For example, the conference of German data protection supervisory authorities advises that a short cookie lifespan is more likely to meet the requirements of the test balancing the interests of controller, third parties and data subjects[108] but stops short of specifying a suitable cookie retention period.[109] The Spanish DPA advises that the cookie duration period should be proportionate to the pursued processing but again does not recommend what would amount to a reasonable cookie duration period.[110] Notwithstanding, the Spanish DPA recommends, as good practice, that cookie consent should be renewed after 24 months, thus suggesting, at first brush, that in some cases, taking into account factors like proportionality and processing aims, two years might be a reasonable cookie life span.[111] The French DPA adopts a different tack: it advises that the lifespan of analytic cookies, that are exempted under its guidance from the ePrivacy Directive provisions, should not exceed 13 months with the collected data from such cookies retained for a maximum of 25 months.[112] To aid the **robust safeguard** of **data privacy rights** and **facilitate compliance,** it is critical that **EU DPAs issue clear, comprehensive** and **consistent guidance** on either the **valid retention period** or the **applicable test** to evaluate an **appropriate cookie duration period.** Such guidance should correspond within previous **European regulatory (including judicial) positions** on this subject matter.

Moving away from responsibility lines and cookie lifespans, next, the report considers the challenges of discharging informational transparency in this new landscape.

4.3.2.2 First-Party Cookies and Informational Transparency

As indicated earlier, the new uses of First-Party Cookie Data often lead to an intricate and fluid processing chain inhabited by diverse entities. Thus, as with TPC, in such cases, it can be difficult to provide end-users with **easy-to-understand, granular, complete** and **accessible information** about all legally prescribed matters including the precise data points processed for one or more AdTech operation; every specific processing purpose like anonymisation, third-country transfers, third-party sharing, data amalgamation, targeting, ad measurement, predictions and profiling; and cookie duration.[113] As recognised by the literature, several behavioural, linguistic, literacy and economic

108 GDPR Art 6(1)(f) (n 2).

109 For example, see Datenschutzkonferenz, 'Orientierungshilfe der Aufsichtsbehörden für Anbieter: innen von Telemedien ab dem 1' (2021) < https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf> accessed 8 July 2022 (the German conference of supervisory authorities' published guidance on internet tracking); 'FAQ zu Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps' <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/FAQ-zu-Cookies-und-Tracking.pdf (the FAQ on cookies and tracking)> accessed 24 November 2022; see Translation (n 105).

110 See Agencia Espanola Proteccioin Datos, 'Guide on Use of Cookies' (January 2021) >https://www.aepd.es/es/documento/guia-cookies-en.pdf> accessed 24 November 2022section 2.1.3 ff; see Translation (n 105).

111 *ibid* section 3.2.8; translation (n 105).

112 See CNIL (n 70) [50]; Translation (n 105).

113 *Planet49*, para 81 (n 45). This raises a crucial question, namely, the reasonable cookie retention period taking into account factors like the processing context and the impact of processing on the data privacy rights of individuals which, as explored earlier, to date has been answered in disparate ways by EU DPAs.

factors like end-user apathy, cognitive overload, 'consent fatigue,'[114] low comprehension levels, the financial costs of reading lengthy policies and the much maligned 'myth'[115] of the so-called 'privacy paradox'[116] can impair the delivery of effective informational transparency.[117] The modalities of cookie notification including pop-ups and banners can also, depending on their lay-out, design and visual prominence, impact on their visibility to end-users.[118] These can all certainly result in partial or failed transparency and should not be readily discounted.

Relatedly, end-users may not always be furnished with **full**, **complete, intelligible**, **accurate and granular information** about the first-party cookies' specific AdTech processing operations. This can arise in several scenarios. Occasionally, people may not be fully informed that the processing activities include amalgamating First-Party Cookie Data with other real-time and historical end-user data points from several sources including third parties, other first-party data and digital exhaust to systematically build rich and dynamic end-user profiles for commercial analytics and marketing purposes. Importantly, end-users may not know or understand that global entities like Meta Platforms Inc and Google, operating across plural and often interconnected devices, applications, platforms and services, often share and cluster disparate and plural real-time, past and predicted end-user data points across all their operations for AdTech purposes like personalising content and delivering hyper-targeted promotions. Even if they are provided with sufficiently precise information about the mechanics and practices of intra-group data sharing, for previously outlined reasons, they may not fully understand who has access to their data and why. Since the *Planet 49* ruling, it is also established jurisprudence that end-users must be informed whether cookies are accessed or not by third parties.[119] Thus, where third parties like advertisers, data management platforms and data brokers have access to First-Party Cookie Data for one or more AdTech operations, this should be clearly and

---

114 For more on the so-called consent fatigue, see Alexis Ward, 'The Oldest Trick in the Facebook: Would the General Data Protection Regulation have stopped the Cambridge Analytica Scandal?' (2022) 25 Trinity College Law Review 221; Maximilian Grafenstein, Julie Heumüller, Elias Belgacem, Timo Jakobi and Patrick Smiesko, 'Effective Regulation Through Design – Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection By Design Approach' (SSRN 19 October 2021) <https://ssrn.com/abstract=3945471> accessed 24 November 2022; Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: following in US Footsteps?' (2017) 26(2) Information & Communications Technology Law 146, 171; Eleni Kosta, 'The Netherlands: The Dutch regulation of cookies' (n 4) 102.

115 See Daniel Solove, 'The Myth of the Privacy Paradox' (2021) 89 (1) George Washington Law Review 1.

116 See Solove *ibid*; Sarah Spiekermann, Jens Grossklags and Bettina Berendt, 'E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior' (EC '01: proceedings of the 3rd ACM conference on electronic commerce 2001) 38, 45; Nina Gerber, Paul Gerber and Melanie Volkamer, 'Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior' (2018) 77 Computers & Security 226.

117 For example, Vranaki *Regulating Social Networking Sites: Data Protection, Copyright, and Power* chapters 6 and 7 (n 13); Alecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 Journal of Law and Policy for the Information Society 543; Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442; Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509.

118 For example, Michael Kretschmer, Jan Pennekamp and Klaus Wehrle, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the web' (2021) 15(4) ACM Transactions on the Web 1.

119 *Planet 49*, para 81 (n 45); see Wiedemann (n 28) for a discussion on the ambit of the informational transparency obligation when it comes to third-party data sharing.

explicitly communicated to end-users in cookie policies. In other cases, several first-party cookies can have the same name although they undertake distinct operations like targeting and audience measurement. Here, unless this is clearly spelt out, end-users may not always fully understand the how and why of processing.[120] So far, the CJEU has not explicitly ruled on the ambit of the informational transparency obligation (and thus relatedly on informed consent) in respect of the different types of cookies (whether first party or otherwise) present online. However, the Advocate General's opinion in the *Planet 49* case, instructive to but not binding on the court, lends weight to the aforementioned point as it suggests that organisations must provide end-users with clear, intelligible, non-ambiguous and exhaustive information so that they understand the functioning of the cookies deployed on particular websites.[121] Whether the CJEU rules on this specific question in the future and/or decides to follow the position set out in the Advocate General's opinion in *Planet 49* remain to be seen. In all these scenarios, it can be difficult to discharge fully the informational transparency obligations. [122]

Having explored the difficulties of discharging **effective transparency**, next, the report scrutinises the challenges of obtaining valid consent for lawful first-party cookie storage and access in this cutting-edge environment.

4.3.2.3 Elucidating Valid Consent for First-Party Cookie Placement and Access

As a reminder, **valid consent** must be 'freely given',[123] 'specific',[124] 'informed',[125] 'unambiguous',[126] as easy to revoke as given,[127] not bundled with other matters like the terms of use,[128] demonstrable[129] and sought before cookies are dropped.[130] In the modernised AdTech landscape, what are the main obstacles to obtaining valid consent? This section explores this question through close engagement with recent relevant judicial and regulatory developments, which can often be problematic both for AdTech players and individuals as data subjects. Entities encounter yet again the well-known quagmire of complying with manifold and often divergent regulatory guidance whilst individuals, depending on

120 For example, Interview 010 (n 52).

121 *Planet49*, para 115 (n 45).

122 For example, Datenschutzkonferenz (n 109); Garante Per La Protezione Dei Dati Personali, 'Guidelines on the Use of Cookies and Other Tracking Tools' (Official Journal of the Italian Republic 163, 9 July 2021); Agencia Espanola Proteccion Datos (n 110); A29WP, 'Guidelines on Consent under Regulation 2016/679' (2017) <https://ec.europa.eu/newsroom/article29/redirection/document/51030 > accessed 8 July 2022; Belgian DPA (n 47); Translation (n 105).

123 GDPR Art 4(11) (n 2).

124 *ibid*.

125 *ibid*.

126 *ibid*.

127 See GDPR Art 7(3) (revocation) (n 2); Belgian DPA (n 47); CNIL, 'Deliberation of the restricted committee' (n 47); A29WP (n 122) 21ff f; see Translation n (105).

128 GDPR Art 7(4) (bundled consent) (n 2); A29WP (n 122) 5ff.

129 GDPR Art 7(1) (demonstrable consent) (n 2).

130 For example, CNIL, 'Deliberation of the restricted committee' [68] (n 47); Translation (n 105).

the applicable guidance, may have more or less control over how and why their personal data is processed with attendant impact on their self-determination, autonomy and dignity.[131]

The difficulties are now evaluated in detail by considering **five** central aspects of **valid consent**, namely, being freely given, being informed, specificity, unambiguity and cookie consent modalities as these are particularly challenging. Starting with **freely given** consent, it is well-trodden legal ground, that for consent to be freely given, individuals must have real choice in granting consent (or not) to the placement of first-party cookies for particular AdTech operations.[132] In other words, website use and access should not be conditional on end-users granting consent to such processing.[133] European member states like Ireland have clear guidance that consent mechanisms like pop-up, banner, message bar or header bar, should be designed so that end-users are not nudged towards providing rather than withholding consent.[134] In Germany, the conference of German data protection supervisory authorities has adopted a similar position.[135]

Turning to **informed** consent, due to the close links between transparency and informed consent, where end-users are furnished with incomplete, inaccurate, general, poorly visible or unintelligible information about all the legally mandated matters including all the specific AdTech processing purposes, the data recipients, their data subject rights and the identity of the controllers, this, alongside the other factors behind low or partial transparency, will impact on whether the consent obtained is truly informed or not.[136] Relatedly, **specific** consent means that consent must be granular. In other words, it must be sought for each pursued AdTech processing operation with end-users free to accept or reject particular processing operations.[137] Some EU DPAs, like the French DPA provide often non-binding and non-exhaustive additional cookie recommendations to their regulatees like setting out each processing purpose in a concise and 'highlighted' title accompanied by a brief description of the purpose with potentially drop-down buttons used to provide additional information about each purpose. [138]

For consent to be **unambiguous**, clear and affirmative end-user action is required.[139] Thus, continued use of websites or apps;[140] opt-out mechanisms like pre-set slides and browser settings

---

131 For more on the links between self-determination, autonomy, dignity and EU data protection laws, see Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 45.

132 For example, EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 [90] (n 87).

133 EDPB *ibid*; Belgian DPA (n 47); Translation (n 105).

134 For example, Data Protection Commission of Ireland, 'Fundamentals for Child-oriented Approach to Data Protection' (December 2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/> 99 accessed 24 November 2022.

135 Datenschutzkonferenz (n 109); see Translation (n 105).

136 CNIL, 'Délibération n° 2020-091' (n 105) [12], [22], [23]; EDPB, 'Guidelines 05/2020' (n 87) [64], [66], 67]; Belgian DPA (n 47); Translation (n 105).

137 For example, Data Protection Commission of Ireland (n 134) 9; CNIL, 'Délibération n° 2020-091' (n 105); Datenschutzkonferenz (n 109); Translation (n 105).

138 CNIL, 'Délibération n° 2020-091' (n 105) [13]; See Translation (n 105).

139 See EDPB Consent Guidelines [75], [82]; CNIL, 'Délibération n° 2020-091' (n 105) [9], [22]; Translation (n 105).

140 CNIL, 'Délibération n° 2020-091' (n 105) [27]; Translation (n 105).

accepting cookies by default do not meet the unambiguity requirement.[141] Whilst the CJEU jurisprudence has ruled that pre-ticked boxes are not valid forms of consent, there is still some regulatory divergences and gaps about the level of action required for consent to be unambiguous. EU DPAs like the Belgian and French contend that mere web scrolling does not satisfy the unambiguity requirement.[142] However, others like the Italian DPA adopt a nuanced approach and contend that scrolling cannot be completely ruled out as a valid consent mechanism in cases where it is merely one component of a consent mechanism.[143]

What are the suitable ways of **obtaining consent**? Through cookie banners? Through 'cookie walls'? Through consent management platforms? The answers to these questions often remain a moving target due to several factors including regulatory (including legislative) divergences and gaps. Let us consider the last two questions to illustrate this point. In May 2020, the EDPB issued clear guidance indicating that **cookie walls** (or scenarios where end-users must consent to cookie storage and/or access in order to access particular services or functionalities) do not meet the requirement of freely given consent.[144] Whilst, by and large, the EDPB position has been adopted by many EU DPAs like the Spanish and Dutch DPAs,[145] some EU DPAs like the French DPA, have adopted a slightly more nuanced approach on this matter. Thus, the French DPA advises that cookies walls are unlikely to meet the consent threshold under the GDPR but cautions that such assessments must be made on a case-by-case basis.[146] Going forward, this fragmented approach at EU DPA level is likely to be exacerbated by upcoming legislative developments. To start, the European Council's agreed version of the **ePrivacy Regulation** (Council's ePrivacy Regulation) does not contain any explicit provision on cookie walls. Rather, it tackles the legality (or otherwise) of cookie walls in one of its recitals whose wording is ambiguous, at odds with the EDPB position and non-binding. In a nutshell, recital 20aaaa provides, *inter alia*, that cookie walls do not deprive end-users of a 'genuine choice' if they can exercise choice between services in the sense of being able to accept either an offer that includes consenting to cookie storage and/or access or an 'equivalent offer' not based on such conditions.[147] The Council's ePrivacy Regulation does not clarify how an assessment of **equivalence** should be made in this context. Recital 20aaaa also specifies that the existence of a clear imbalance between end-users and service providers in such contexts has a bearing on whether end-users have a real choice or not. In the interests of **legal**

141 Datenschutzkonferenz (n 109); Translation (n 105).

142 For example, Belgian DPA (n 47); CNIL, 'Délibération n° 2020-091' (n 105) [27]; Translation (n 105).

143 Garante Per La Protezione Dei Dati Personali (n 122) section 6; Translation (n 105).

144 EDPB, 'Guidelines 05/2020' (n 87) [39].

145 For example, Agencia Espanola Proteccion Datos (n 110) paragraph 3.2.10; Dutch DPA, 'Websites Must Remain Accessible When Tracking Cookies Are Refused' (*Autoriteit Persoonsgegevens*, 7 March 2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies> accessed 24 November 2022; Translation (n 105).

146 CNIL, 'Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL' (2022) <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ> question 30; see Translation (n 105).

147 Proposal for a Regulation of the Parliament and of the Council (EU) concerning the Respect for Private Life and The Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2021] 6087/21(hereinafter Council's ePrivacy Regulation).

coherence and consistency, it is imperative that the **ePrivacy Regulation formally** and **explicitly** clarifies in its **operative provisions** whether (or to what extent) **cookies walls** are **permissible** or not.[148]

What about elucidating valid consent through industry-issued **consent and transparency frameworks**? This is a rapidly evolving area following the Belgian DPA's investigation of the Interactive Advertising Bureau Europe Transparency and Consent Framework (TCF), a leading consent and transparency framework across Europe, in 2022. The Belgian DPA found, *inter alia,* that the TCF breached several GDPR provisions including transparency, lawful processing basis, security and integrity and data protection impact assessment and consequently imposed a €250,000 fine.[149] At the time of writing, this matter is still ongoing with, for example, Belgian Market Court having issued an interim ruling following the IAB's appeal against the Belgian DPA's initial findings and its referral of a number of preliminary questions to the CJEU.[150]

Based on the foregoing, due to a range of factors including regulatory gaps, lags and inconsistencies, it can currently be tricky to elucidate valid consent for the lawful first-party cookie placement and access for AdTech operations. Given the **transborder data flows** in the **AdTech sector**, it is **imperative** that **EU DPAs** adopt **common principles** on **valid cookie consent**, with particular attention paid to first-party cookie processing, to promote the **adoption** and **application** of law **consistently** across Europe to **robustly safeguard** the **individual's data privacy rights**. In the interests of **legal coherence and consistency**, it is also crucial that the **ePrivacy Regulation** formally and explicitly clarifies whether **cookies walls** are permissible or not under the law.[151] As highlighted earlier, the Council's ePrivacy Regulation does not currently contain any specific binding provisions on cookie walls bar the wording expressed in Recital 20(aaaa) which is unclear, open to interpretation and also not binding.[152]

The report now leaves aside the regulatory (including legal) implications of lawful first-party cookie placement and access and tackles the challenges of processing First-Party Cookie Data in line with the GDPR.

4.3.3 First Party Cookie Data, AdTech and GDPR

The following legal analysis assumes that the processing of First-Party Cookie Data falls within the GDPR's material and territorial scope.[153] Evidently, entities processing First-Party Cookie Data must undertake this scoping analysis to determine whether and if so, to what extent, they must comply

148 This echoes the EPBD's recommendation on this point (n 4) 3.

149 DOS-2019-01377 *Decision on the merits 21/2022 of 2 February 2022* (Belgian Data Protection Authority 2022) <https://www.loyensloeff.com/globalassets/02.-publications-pdf/02.-external/2022/beslissing_21-2022_en.pdf> accessed 24 November 2022.

150 Court of Appeal of Brussels, Market Court, Decision on the merits 21/2022 of 2 February 2022, *IAB Europe v Data Protection Authority* 2022/AR/292 (2022*)* <https://www.iccl.ie/wp-content/uploads/2022/09/English-Judgement-Markets-Court-07-09-2022_Redacted.pdf> accessed 24 November 2022 ; Society for Computers & Law, 'Belgian Market Court refers Preliminary Questions to the CJEU in IAB Europe Cookie Case' (*SCL,* 8 September 2022) <https://www.scl.org/articles/12685-belgian-market-court-refers-preliminary-questions-to-the-cjeu-in-iab-europe-cookie-case> accessed 24 November 2022.

151 This echoes the EPBD's recommendation on this point (n 4) 3.

152 See Council's ePrivacy Regulation, recital 20aaaa (n 147).

153 GDPR Arts 2 (material scope) and 3 (territorial scope) (n 2).

with the GDPR. As per the report's scope (**Section 3.3**), this section zooms into **eight**, rather than all, dilemmas to provide a bird-eye's view of the wide-ranging compliance challenges raised by First-Party Cookie Data processing to stimulate much-needed stakeholder discussion on this topic. However, this does not mean that other aspects, such as third-country data transfers and exercise of particular data subject rights like access and erasure, are not equally as problematic.

First, the earlier Section **4.3.2.1** analyses on responsibility lines and transparency are also relevant here. Thus, before processing any First-Party Cookie Data , all entities handling such data for one or more specific AdTech purposes must be clear about their precise **responsibility lines** for such processing either as sole controllers, joint controllers or processors (or entities that undertake processing activities 'on behalf' of controllers).[154] Such data stewardship allocation is a cornerstone of **accountability,** which does not only require controllers to ensure legal compliance, but also demonstrate such compliance on request.[155] Such apportionment of responsibility must consider which party has 'effective control'[156] over the processing 'means' and 'purposes' throughout the lifecycle of processing.[157] Depending on the processing context, controllership may be shared between one or more entities,[158] with such organisations often having variable rather than 'equal' [159] levels and degrees of responsibility to determine the 'why' and 'how' of processing. The status of entities, as controllers or processors, may also change over the lifecycle of data processing as their precise involvement in processing evolves. In such cases, it is crucial that the compliance obligations of such entities are cyclically recalibrated as their status under the law changes. Crucially, where controllers use processors to undertake particular operations like data mining, they must only recruit processors that, for example, offer 'sufficient' and 'appropriate' 'technical and organisational measures' guarantees.[160] Such processors must also abide by several obligations, often contained in binding contracts with controllers,[161] including obtaining prior controller approval before engaging other processors,[162] processing First-Party Cookie Data only in line with the 'documented' controller 'instructions',[163] complying with the security obligations[164] and supporting the controllers in responding to requests by data subjects to exercise their rights.[165] Regarding **transparency**, the earlier (**Sections 4.2 and 4.3.2**) scrutiny of information transparency is equally pertinent here. For example, controllers must furnish individuals with accessible, simple and comprehensive information about such processing including the specific First-Party Cookie Data points processed for AdTech activities,

154 See GDPR Arts 4(8) (processor definition), 5 (data protection principles), 6 (lawful processing), 24 (controller responsibility), 28 (processor obligations and 32 (security) (n 2).

155 GDPR Arts 5(2)(accountability) and 24 (controller responsibility) (n 2).

156 See A29WP '01/2010' (n 156).

157 GDPR Art 4(7) (controller definition) (n 2).

158 For example, GDPR Art 26 (n 2); *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* para 67, (n 45).

159 For example, A29WP 01/2010 (n 156).

160 GDPR Art 28(1) (processor obligations) (n 2).

161 GDPR Art 28(3)(processor obligations) (n 2).

162 GDPR Art 28(2)(processor obligations) (n 2).

163 GDPR Art 28(3)(a) (n 2).

164 GDPR Art 28(3)(c) (n 2).

165 GDPR Art 28(3)(e) (n 2).

the precise AdTech processing operations undertaken, the data recipients, third-country transfers and their data subject rights. Likewise, where organisations use the TCF for informational transparency purposes, the ongoing battle between EU DPAs like the Belgian DPA and the IAB (see **Section 4.3.2**) remains relevant.

Second, where controllers collect First-Party Cookie Data for particular AdTech operations like monitoring, predictions, targeting and profiling, they must ensure that such data is collected for **explicit, clear** and **specific purposes** and not processed for 'further', 'incompatible' purposes, unless legally permissible.[166] Importantly, they must clearly identify the specific first-party cookies that collect the individuals' personal data for one or more AdTech purpose. The exact purposes like ad targeting, audience segmentation and profiling must be granularly identified. They must also ensure that any further First-Party Cookie Data processing is not incompatible with their originally specified purposes.[167] '[F]urther processing for purposes like archiving and statistics are considered compatible in prescribed circumstances'.[168]

Third, controllers do not have blanket permission to process First-Party Cookie Data for one or more AdTech purposes. They must comply with the **data minimisation principle** and only collect First-Party Cookie Data that is 'adequate', 'relevant' and 'limited to what is necessary' for the AdTech purpose(s) pursued. Specifically, they must evaluate whether their current and proposed data analytics roadmap, throughout its lifecycle (from planning to capture to cleaning to standardising to analysis to interpretation to reporting)[169] adheres to data minimisation with, for example, an assessment of whether the pursued AdTech processing cannot be reasonably be achieved without one or more First-Party Cookie Data points.[170]

Fourth, controllers must 'bake in' appropriate '**technical and organisational**' measures, like pseudonymisation and data minimisation, to uphold all GDPR provisions including the data protection principles.[171] Controllers must consider a list of exhaustive factors including the implementation cost, the state of the art, the processing purposes and the risk the processing activities are likely to pose to the individual's fundamental rights and freedoms, to determine the suitable measures to be deployed in specific processing scenarios. They must also implement appropriate 'technical and organisational measures' to ensure that, **by default**, only the personal data strictly necessary for one or more specific AdTech purposes, whether in terms of amount, processing extent and storage period, is processed.[172] The '**by design**' and 'by **default**' requirements apply not only at the time of processing, but also before

166 See GDPR Art 5(1)(b) (n 2); A29WP, Opinion 03/2013 (n 166).

167 See GDPR Art 6(4)(a)–(e) for the list of factors to consider when determining if further processing is compatible with the original purpose (n 2).

168 GDPR Art 89(1) (n 2).

169 For more on the stages in the lifecycle of data analytics projects, see David Nettleton, *Commercial Data Mining: Processing, Analysis and Modeling for Predictive Analytics Projects* (Elsevier 2014); Thomas Runkler, *Data Analytics* (Springer 2012) 1.

170 For example, GDPR Art 5(1)(e) (n 2); Cécile de Terwangne, 'Article 5 Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 317ff.

171 See GDPR Art 25(1) (n 2).

172 See GDPR Art 25(2) (n 2).

processing. Consequently, these mandatory assessments must be cyclically repeated when, for example, new data points join the controller's AdTech ecosystem. [173]

Fifth, controllers must identify one or more suitable bases to **legitimise** the processing of First-Party Cookie Data for one or more AdTech purposes.[174] Depending on the nature, scope, means, and purposes of First-Party Cookie Data processing, occasionally controllers may need to rely on more than one lawful basis to legalise particular operations. Consent, obtained by first-party cookie setters, for the lawful first-party cookie storage and access cannot be used to legalise the processing of First-Party Cookie Data for purposes like data monitoring and predictive analytics. Relatedly, where '**special data categorie**s' like race, ethnicity, trade union membership, health, genetic data and biometric data are processed under the '**explicit**' **consent** exemption, such exemption must be supported by a suitable Art 6 legitimating ground.[175] Explicit consent is a higher standard of consent than the one provided by Art 6(1)(a) with individuals required to provide an 'express' consent statement like a signed consent statement, completed digital form or a scanned document containing their signature. [176] Where explicit consent is elucidated via the TCF, as with transparency, controllers must remain up to date with the relevant European regulatory developments and take suitable remedial measures where appropriate.

Sixth, where First-Party Cookie Data processing meets the Art 35(1) ingredients, controllers must conduct a **data protection impact assessment** (DPIA) before the processing to evaluate the likelihood and severity of risk that the proposed operations may pose to the individual's fundamental rights and freedoms. In particular, multinational organisations operating across several platforms, applications, websites, products and services that conduct 'systematic and extensive' personal data evaluation, based on automated processing like profiling that is used to reach decisions about end-users with either 'legal effects' or of equivalent significance, must conduct DPIAs.[177]

Seventh, controllers and processors handling First-Party Cookie Data must implement appropriate technical and organisational measures for **security** purposes. They must consider legally prescribed factors, such as the state of the art; the implementation cost; the processing scope, nature, purpose and context and the likelihood and severity of data privacy harms to the individuals; to determine the range of suitable risk-based measures and practices like encryption; pseudonymisation; ongoing system or service confidentiality, integrity, availability and resilience, as well as timely post-incident data availability and access restoration.[178] The Section **4.3.4** analysis is also apropos here.

Finally, entities using First-Party Cookie Data points for one or more specific AdTech operations must ensure, in line with their broader assessments of responsibility lines, that such processing is

---

173 For an insightful analysis of the 'by default' and 'by design' provisions, see Lee Bygrave 'Article 25 Data Protection By Design and By Default' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

174 GDPR Art 6(1)(a)-(f) (n 2).

175 This is the current position as per the latest guidance. See EDPB, 'Guidelines 03/2019 Processing personal data through video' (*EDPB,* 2019) 14 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.> accessed 24 November 2022.

176 See EDPB 'Guidelines 05/2020) 20–21 (n 87).

177 GDPR Art 35(3)(a) (n 2).

178 See GDPR Arts 32(1)(a) – (c), 32 (2), 32 (3) and 32(4) (n 2).

rolled out in practice in ways that support the exercise and timely operationalisation of all applicable **data subject rights** including access, erasure, objection, automated decision-making and profiling.[179] For instance, end-users must have effective ways to control and manage, as far as legally permissible, who has access to their First-Party Cookie Data, and why, throughout the data analysis lifecycle.

Based on this analysis, it is clear that the **lawful processing** of **First-Party Cookie Data** is not always uncomplicated. Next, the report considers how these legal challenges are further exacerbated or take on a different shade given the pervasive and ubiquitous deployment of Canonical Name Record or Alias (CNAME) cloaking in the AdTech ecosystem to evade third-party anti-tracking in-browser settings, extensions and plug-ins.[180]

4.3.4 CNAME: Of Cloaks and Daggers

This section considers how CNAME third-party cookie cloaking practices, to the extent that they are not curtailed, interfere with the **ePrivacy Directive** and **GDPR** obligations and, thus, further complicate the legal landscape.

Before proceeding further, it is important to understand the CNAME technique. CNAME refers to the technique of mapping one domain to another in the domain name system (DNS) record. In the context of third-party tracking and analytics, the presence of third-party data tracking and analytics actors within the first-party data chain is concealed, as a CNAME DNS database record indicates that third-party tracking and analytics entities are sub-domains or aliases of the root first-party domain name. Recent research has demonstrated that websites including the so-called top 300,000, in sectors like banking and retail routinely deploy CNAME techniques to hide the presence of third-party tracking and analytics in the first-party cookie ecosystem.[181] Some industry players like browsers are responding to such trends by, for example, releasing updates to cap the expiry of cloaked third-party cookie HTTP responses to a week.[182]

Depending on the processing context (including the cookie policy's wording), the use of CNAME cookie cloaking can infringe the **two** ePrivacy Directive **conditions** for **lawful cookie placement and access**. The **transparency** condition is not met where end-users are not provided with full, clear, accurate and simple information about all the legally mandated matters including the fact that the cookie, presented as a first-party cookie, is in fact not a first-party cookie but rather is stored and accessed by one or more third parties for AdTech purposes like data amalgamation, data mining and

---

179 See GDPR Arts 15 (access), 17 (erasure), 21 (objection) and 22 (automated decision-making and profiling) (n 2).

180 For example, Interview 008 (n 19); Interview 010 (n 52); Ha Dao, Johan Mazel and Kensuke Fukuda, 'Characterizing CNAME Cloaking Based Tracking on the Web' (IEEE/IFIP Network Traffic Measurement and Analysis Conference 2020); Ha Dao, Johan Mazel and Kensuke Fukuda, 'CNAME Cloaking-Based Tracking On the Web: Characterization, Detection, and Protection' (2021) 18(3) IEEE Transactions on Network and Service Management 3873; Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich Wambach and Mika Ayenson, 'Behavioral Advertising: The Offer You Can't Refuse' (2012) 6 Harvard Law & Policy Review 273.

181 See Yuta Takata, Daiki Ito, Hiroshi Kumagai and Masaki Kamizono, 'Risk Analysis of Cookie Sharing By Link Decoration and CNAME Cloaking' (2021) 29 Journal of Information Processing 649; Dao, Mazel and Fukuda, 'CNAME cloaking-based tracking on the web' *ibid*.

182 John Wilander, 'CNAME Cloaking and Bounce Tracking Defense' (*WebKit,* 2020) <https://webkit.org/blog/11338/cname-cloaking-and-bounce-tracking-defense/ > accessed 8 July 2022.

audience segmentation. This issue is compounded by the intricacy of the CNAME chain, which is often long and includes several CNAMES, such as first-party sub-domain, cloud storage and tracker.[183] Likewise, the use of CNAME techniques in the first-party cookie chain may impact on the lawful placement and access of first cookies where all ingredients required for **valid consent** (see **Section 4.2**) are not obtained. For instance, where end-users are provided with inadequate, inaccurate, incomplete or unclear information regarding the storage of and access to third-party cookies, which are operating under the guise of first-party cookies, they will not be in a position to provide informed and specific consent to such cookie storage and access.

With respect to the GDPR, where it applies,[184] third-party cloaked data capture, tracking and analytics practices can breach both its letter and spirit. The following exploration of its implications for **four** central GDPR aspects, namely, fairness, accountability, security and the data subjects' rights, brings to the fore a crucial question: to what extent are CNAME cookie cloaking practices legal under the GDPR? It should be noted that to-date only the French DPA has provided some rudimentary guidance on this question by suggesting, *inter alia*, that the use of the CNAME cookie cloaking technique does not in principle breach the GDPR but may, depending on how it is operationalised and implemented on the ground, raise concerns under, for example, the transparency and security principles.[185] However, as explored next, in practice, the use of CNAME techniques often raise far more complex data protection law issues than currently recognised by EU DPAs like the French DPA.

Kicking off with the **first data protection principle**, where the CNAME cookie cloaking technique is not clearly, fully and suitably explained in privacy policies (or other relevant documents), transparency and lawfulness considerations aside, this breaches the GDPR **fairness** principle as individuals are actively being misinformed about the presence of third-party trackers and analytics within the first-party cookie chain and are labouring under the misapprehension that all First-Party Cookie Data are only processed by the first-party setter.[186] In such cases, core aspects of fairness including not processing personal data by 'deception'[187] or 'in secret'[188] are clearly in question depending on how particular CNAME techniques are operationalised and implemented in practice.

Second, the use of CNAME techniques raises complex **accountability** questions between the range of entities involved in the so-called first-party cookie chain including the first-party cookie setter and the myriad of cloaked third-party data analytics and tracking actors.[189] As explained earlier, it is imperative that lines of **responsible data stewardship** are clearly, accurately and granularly defined

183 Tatsuya Mori, Takeru Inoue, Akihiro Shimoda, Kazumichi Sato, Shigeaki Harada, Keisuke Ishibashi and Shigeki Goto, 'Statistical Estimation of the Names of HTTPS Servers With Domain Name Graphs' (2016) 94 Computer Communications 104; Dao, Mazel and Fukuda, 'CNAME cloaking-based tracking on the web' (n 180).

184 See GDPR Arts 2 (material scope) and 3 (territorial scope) (n 2).

185 CNIL, FAQ (n 146) Question 29.

186 See GDPR Art 5(1)(a) (lawful, fair and transparent processing) (n 2).

187 Terwangne (n 170) 314.

188 See European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, and European Data Protection Supervisor (eds), *Handbook on European Data Protection Law* (Publications Office of the European Union 2018) 118 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > accessed 24 November 2022.

189 GDPR Art 5(2) (accountability) (n 2).

at the time of processing to ensure that each entity knows its legal status throughout the processing lifecycle (e.g. controller, processor or joint controller), all compliance obligations are clearly and correctly allocated to the right party depending on its legal status throughout the processing lifecycle, and all other GDPR provisions on matters like the controller/processor relationship and the processor's obligations are respected.[190] Such evaluation must determine which actors truly determine the 'how' and 'why' of processing irrespective of the apparent shrouds that hide their real roles within the processing chain.[191] This also introduces another layer of complexity when it comes to enforcement as **EU DPAs** require appropriate **expertise** and **access** to relevant **information** including contextual, real-time and accurate data flow maps to verify and/or correctly assess the legal status of the myriad of **camouflaged entities** contained in the chain during enforcement.[192]

Third, the use of CNAME techniques raises complex and not yet fully understood **security** challenges. For instance, depending on their configurations, session cookies that authenticate end-users to the visited website and are only known by these two parties, can be leaked to all cloaked sub-domains where websites set the 'domain' attribute of such cookies to all website domains and sub-domains.[193] In such cases, the personal data of end-users contained in session cookies are disclosed to cloaked third-party actors in breach of, for instance, confidentiality.[194] Depending on whether the cookie 'secure' attribute is set in this scenario, another concerning security issue may arise. Thus, where websites do not set the secure attribute for session cookies and such cookies are shared with the cloaked third-parties using plain text HTTP, the session cookies and personal data they contain can be intercepted by a network attacker.[195] Previous research has shown that this issue is most likely to arise when people use outdated browsers that may not block tracker requests over unsecure connections.[196] Evidently, depending on the context, data leaks to third parties can also be problematic under other GDPR provisions like lawful processing and other data protection principles. Finally, third-party CNAME cookie cloaking practices interfere with the **rights** of **data subjects**, to exercise control over and reach autonomous decisions in line with their agentic capabilities about,

190 See GDPR Arts 4(7) (controller definition); 4(8) (processor definition); 24–26(controller obligations and joint controller); 28 and 29 (processor obligations and processing under controller's authority) (n 2).

191 *ibid*, controller definition.

192 See Asma Vranaki, 'Data Governance in the Cloud: Of Scarce Regulatory Resources and Tactical Delegated Enforcement' [2021] Public Law 125 for more on the importance of resources (including expertise and information) to effective enforcement.

193 See Kosta 'Peeking into the cookie jar' (n 4) session cookies; Assel Aliyeva, and Manuel Egele, 'Oversharing Is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies' (Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security) 123 (cookie configuration).

194 Aliyeva and Egele, *ibid*; Dao, Mazel and Fukuda, 'CNAME cloaking-based tracking on the web' (n 180); Takata, Ito, Kumagai and Kamizono (n 181) 649.

195 Aliyeva and Egele (n 193); Suphannee Sivakorn, Iasonas Polakis and Angelos D Keromytis, 'The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information' (Proceedings of the 2016 IEEE Symposium on Security and Privacy) 724.

196 Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen and Tom Van Goethem, 'The Cname of the Game: Large-Scale Analysis of DNS-based Tracking Evasion' (2020) 3 Proceedings on Privacy Enhancing Technologies 394.

their personal data.[197] The net effect, by bypassing people's choices to filter or block third-party trackers through, for example, in-browser settings or features, plug-ins and extensions,[198] is that the CNAME cookie cloaking practice interferes with both the GDPR's fundamental objectives and provisions.[199]

In sum, the third-party CNAME cookie cloaking practices raise serious questions under both legislations. **This is an area where harmonised and detailed EU DPA guidance is urgently required on several aspects including the scope of its legality (if any)**. Leaving aside the data privacy law implications of first-party cookies, next, the report deals with another popular strategy in ascendance in the sector, with TPC decline, namely, contextual advertising.

5. A Return to Contextual Advertising

The project's findings demonstrate that contextual advertising is resurging in the AdTech sector amidst the TPC decline, with many stakeholders, like some EU DPAs, often considering contextual advertising as a form of advertising that interferes minimally with the individual's data privacy rights. To what extent is this assumption well-founded? Through an analysis of the actual practices, processes and techniques deployed in contextual campaigns delivered on websites and social media platforms, this section contends that it cannot be assumed, **without a case-by-case analysis**, that **contextual advertising** does not impinge on the **individual's data privacy rights**. Here, the section often zooms into the mechanics of contextual campaigns on two environments, namely websites and social media, that provide extensive, varied, real-time, detailed and routine in-session content that can be mined for contextual campaigns. It also analyses the legal implications of particular data analytics practices and techniques, like sentiment analysis on social media, deployed in such environments for contextual advertising purposes. It also argues that there are **fundamental divergences** between the **actors** involved in the different stages of the regulatory process (e.g. rule setting, rule interpretation and enforcement) about whether **contextual advertising** amounts to **targeted advertising** and utilises **personal data**.[200] It is imperative that such **disparities** are satisfactorily resolved, through **evidence-based approaches** to contextual advertising, to reach **accurate determinations**, at all levels, about their impact on the level of protection afforded to the individual's fundamental rights and freedoms.

---

197 See Omar Tene and Jules Polonetsky, 'Big Data For All: Privacy and User Control in the Age of Analytics' (2012) 11 Northwestern Journal of Technology & Intellectual Property xxvii.

198 Browsers like Firefox and Brave and Tor provide individuals with dedicated features like Enhanced Tracking Protection and Shields, respectively, to prevent third-party tracking; see Firefox browser <https://www.mozilla.org/en-US/ exp/firefox/> accessed 24 November 2022; Brave browser < https://brave.com/> accessed 24 November 2022; <https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/ > accessed 24 November 2022; <https://brave.com/shields/> accessed 24 November 2022. Browser extensions like Ghostery support privacy-protecting browsing by, for instance, blocking third-party trackers; see <https://www.ghostery.com> accessed 24 November 2022.

199 See GDPR Arts 1(2) and 1(3) (n 2).

200 See Bridget Hutter, *Compliance: Regulation and Environment* (Oxford University Press 1997) 12; Julia Black, 'The Role of Risk in Regulatory Processes' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford 2010) for more on regulatory processes.

5.1 Contextual Advertising: Of Plural Actors, Practices and Processes

Before addressing these points, it is important to explore the empirical findings further and consider important aspects like emerging contextual personalisation and targeting practices to set the scene for the upcoming **Sections 5.2** and **5.3** analyses.

The project's findings show that the old practice[201] of contextual advertising, originally deployed in traditional media like newspapers and nowadays regularly used in search advertising,[202] is re-emerging in the AdTech sector as a highly promising and lucrative strategy to construct and reach, with great precision, tailored audiences who are most likely to be interested in and/or act on a promotion without deploying personalisation practices like profiling.[203] Contextual advertising refers to the delivery of advertisements that correspond to the content of webpages visited by individuals.[204] In practice, intricate and diverse processes, techniques and practices like natural language processing, computer vision, clustering, topic tagging and semantic analysis are applied to analyse in real-time key dimensions of the visited webpage including its content (e.g. topics covered); any embedded images, audio and videos; its emotional tone, its linguistic configuration and geographic information.[205] Based on such analyses, advertisements that closely match the webpage's content, rather than the visitor's personal data, are served to end-users.[206] New, emerging and yet to come artificial intelligence advancements are likely to further fine tune all dimensions of contextual analysis including ad targeting, programmatic auctions, content analysis, mindset analysis and ad performance

201 For example, Ian Brown, 'Data Protection: the New Technical and Political Environment' (2010) 20(6) Computers & Law.

202 See European Commission, 'Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union' (June 2018) <https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf> 31 accessed 24 November 2022.

203 For example, Interview 010 (n 52); Interview 011 (n 52); Interview 012 (n 52); Interview 003 (n 52); Interview 009 (n 23); IAB (n 50).

204 For example, Alexander Bleier, 'On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3980001> accessed 29 May 2022; Bartosz Wojdynski and Hyejin Bang, 'Distraction Effects of Contextual Advertising on Online News Processing: An Eye-Tracking Study'(2016) 35(8) Behaviour and Information Technology 654.

205 See Hamed Jelodar, Yongli Wang, Chi Yuan, Xia Feng, Xiahui Jiang, Yanchao Li and Liang Zhao, 'Latent Dirichlet Allocation (LDA) and Topic Modeling: Models, Applications, A Survey' (2019) 78(11) Multimedia Tools and Applications 15169 (topic identification); Asima Yadav and Dinesh Kumar Vishwakarma, 'Sentiment Analysis Using Deep Learning Architectures: A Review' (2020) 53(6) Artificial Intelligence Review 4335 (sentiment analysis); Emil Häglund and Johanna Björklund, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis (2022) arXiv preprint arXiv:2205.00911 (AI practices and techniques deployed in contextual analysis); Bleier (n 204); IAB (n 50) 3ff; Emmanuel Netter, '"Free" Online Service in Exchange For Targeted Advertising : The Business Model With Feet of Clay' (*HAL Open Science,* 2021) <https://hal.archives-ouvertes.fr/hal-03329824/document> accessed 24 November 2022.

206 See Aureilo Lopez-Tarruella, *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge* (Springer 2012) chapter 1; Asuncion Esteve, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA' (2017) 7(1) International Data Privacy Law 36.

measurement.[207] The contextual advertising chain is also convoluted and consists of a diverse range of rapidly changing actors like publishers, advertisers, targeted individuals, data management organisations (including multiple data analytics companies), advertising networks, advertising exchanges and supply-side/demand-side platforms.[208] Crucially, unlike other forms of advertising, contextual campaigns, in theory at least, do not profile end-users over a prolonged period of time. However, people are still being targeted based on their real-time information, which may extend to personal data, to be served with advertisements that match their current consumption needs, opinions, beliefs and so on.[209]

The findings about the renaissance of contextual advertising are also corroborated by European industry trends[210] and official statistics[211] with some estimating that, by 2026, globally, contextual advertising will be worth $335.1 billion.[212] Several reasons can account for this revival including the upcoming TPC decline;[213] the emergence of stricter laws on data tracking, profiling, targeting and automated decision-making;[214] the enactment of recent new European laws like the Digital Services Act that ban ad-targeting on the basis of special data categories and prohibit circulating targeted advertisements to minors;[215]ongoing artificial intelligence developments; and industry research

---

207 Omid Rafieian and Yoganarasimhan Hema, 'Targeting and Privacy in Mobile Advertising' (2020) 2(40) Marketing Science 193 (ad targeting); Bleier (n 204).

208 European Parliament JURI committee, 'Regulating Targeted and Behavioural Advertising in Digital Services' (September 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf> 24 accessed 24 November 2022.

209 For example, Interview 010 (n 52) and Interview 011 (n 52).

210 See The Drum Studios, 'Contextual Advertising: The New Frontier' (*GumGum,* 2021) <https://insights.gumgum.com/hubfs/Contextual-Advertising-the-new-frontier-final-guide.pdf> (AdTech player) accessed 24 November 2022; IAB (n 50) (European industry body); ICCL (n 150) (Ireland-based advocacy group).

211 Eurostat, 'Internet Advertising of Businesses - Statistics on Usage of Ads' (*Eurostat*, December 20108)<https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads#Ads_that_reach_the_right_audience_with_relevant_and_meaningful_content>. accessed 24 November 2022.

212 For example, Strategyr, 'Contextual Advertising: World Market Report' (*Strategyr,* 2022) <https://www.strategyr.com/market-report-contextual-advertising-forecasts-global-industry-analysts-inc.asp.> accessed 24 November 2022.

213 For example, Interview 010 (n 52); Interview 011 (n 52); Häglund and Björklund (n 205); IAB, 'Ipsos: State of Data' (*IAB,* March 2021) <https://www.iab.com/wp-content/uploads/2021/03/IAB_Ipsos_State_Of_Data_2021-03.pdf> 12 (projected 24% increase in contextual advertising expenditure) accessed 24 November 2022.

214 Bleier (n 204).

215 See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, 1 (hereinafter DSA), Art 26(3) (prohibition of advertising based on the profiling of special data categories) and 28(2) (prohibition of profiling-based advertising for minors). The DSA came into force on 16 November 2022; see European Commission, 'The Digital Services Act: Ensuring a Safe and Accountable Online Environment' (2022) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.> accessed 24 November 2022.

purporting to show that people are more likely to engage with contextual advertisements.[216] From a marketing perspective, contextual advertising campaigns are particularly helpful, in this rapidly changing landscape, to help advertisers reach people who have strong preferences for their offerings, with a high degree of accuracy, based on their real-time content consumption.[217]

Notwithstanding the reawakening of contextual advertising, as examined next, from a data protection law and regulation perspective, it is not always a straightforward form of advertising.

5.2 Contextual Advertising: The Personalisation Pot of Gold?

This section underlines important areas of **inconsistencies** between **actors** involved in different stages of the **regulatory process** including rule setting, rule interpretation, enforcement and oversight when it comes to contextual advertising. If such fragmentation persists, it will impact on **effective data privacy regulation** on the ground.

To start, a study commissioned by the Committee of Legal Affairs that provides legal input to the European Parliament, Europe's co-legislator, on several areas including the European legislative packages indicates that contextual advertising is a form of **targeted advertising** given that the end-users are targeted with advertisements that match the content of the visited webpages and/or their search keywords.[218] Consequently, contextual advertising joins the family of other forms of advertising like online behavioural advertising (OBA) and segmented advertising that, at the heart of their operations, are tailored to individuals based on distinct situational factors like webpage content, personal preferences, online behaviour, characteristics, location data and other information.[219] Depending on the advertising type (e.g. segmented versus OBA), different personal data categories are targeted for ad delivery.

However, this stance is not replicated by other actors who play important roles in other phases of the regulatory process, such as enforcement and rule interpretation. For example, many EU DPAs, Europe's foremost 'data privacy guardians', [220] currently posit that **contextual advertising**, that is not fuelled by personal data but only by on-screen content, is outside the scope of data protection law. [221]

---

216 For example, Double Verify, 'Global Consumer Insights' (*Double Verify,* September 2020) <https://doubleverify.com/wp-content/uploads/2020/09/DV_Four_Fundamental_Shifts_In_Media_and_Advertising_During_2020.pdf.> accessed 24 November 2022. It should be noted that the organisations commissioning such research are often developing and commercialising contextual advertising ecosystems. In such cases, there is a clear potential for conflict of interests and the research findings alongside their methodologies must be carefully evaluated to ascertain their validity, rigour and representativeness.

217 For example, Jin-A Choi and Lim Kiho, 'Identifying Machine Learning Techniques For Classification of Target Advertising' (2020) 6(3) ICT Express 175; Wojdynski and Hyejin (n 204); Kaifu Zhang and Zsolt Katona, 'Contextual Advertising' (2012) 31(6) Marketing Science 980.

218 See European Parliament JURI committee (n 208) 12; European Commission (n 202) 31.

218 Opinion 2/2010 (n 47) 5.

219 Segmented advertising refers to the practice of grouping people as audiences based on particular metrics like behaviour, geographic location and demographic data; see Alessandra Buratto, Luca Grosset and Bruno Viscolani, 'Advertising a New Product in a Segmented Market' (2006) 175(2) European Journal of Operational Research 1262.

220 GDPR Art 57 (EU DPA tasks) (n 2).

221 See Data Protection Commission of Ireland (n 134) 4.

Other European data protection regulatory actors like the now defunct A29WP have also indicated that contextual advertising is less problematic than OBA due to its use of 'snapshots' of, for instance, what website visitors view, search for or interact with rather than OBA's more extensive data capture, targeting and profiling practices.[222] Is the assumption that contextual advertising does not use personal data correct? Section 5.3. considers this question further. Relatedly, do contextual advertising practices really have negligible impact on the individual's data privacy rights? Current contextual advertising practices suggest otherwise. [223] For instance, although contextual advertising does not rely on end-user profiling it still involves the **systematic** and **routine recording** and **tracking** of varied end-user information like visited webpage, clicked content, website visit duration and hover rates. As recognised in the data protection literature and explored in **Section 5.3**, such information, depending on the context, can amount to personal data. Moreover, based on extensive surveillance, end-users are also **targeted** with contextual advertising campaigns that match, for example, their real-time search terms, click-through rates, webpage interactions and metadata. As artificial intelligence capabilities continue to evolve, over time, it is likely that the varied practices sustaining contextual advertising like personalisation, targeting and ad auctioning will become even more sophisticated with an increasing amount of personal data being analysed in novel and more granular ways. Thus, as further elaborated in Section 5.3, it cannot be assumed, **without a case-by-case analysis**, considering the nature, scope, context and purpose of processing, that **contextual advertising** campaigns are either outside of the scope of the **legislative framework** (the Irish DPA stance) or an easier or less **privacy intrusive** compliance choice (the old A29WP position).

Such fundamental paradoxes amongst actors operating within the regulatory sphere show that **profound misunderstandings** currently prevail about the types of practices and processes that sustain contextual advertising and their attendant impact on the level of protection afforded to the individual's fundamental rights and freedoms. Thus, if contextual advertising is to re-establish itself as a lucrative and highly effective mode of advertising, which also respects the individual's data privacy rights, it is **imperative** that such **multi-stakeholder discrepancies** are ironed out by adopting **evidence-based** and **highly situated approaches** to **contextual advertising**.

5.3 Personal Data: Of Contextual Information, Emotions and Opinions

To what extent does the information used to fuel contextual advertising practices like targeting, in-session content analysis, ad engagement metrics and conversion rates amount to personal data? This is a core question that has emerged so far. This section addresses this question in detail at a normative level by exploring (1) how such determinations are generally approached at a normative level, (2) the impact of current and projected advancements in artificial intelligence capabilities on such evaluations and (3) the legal status of information like emotions and opinions that frequently fuel contextual advertising on social media.

First, building on Section 5.2, it cannot be assumed that information processed for contextual advertising like in-session content, search queries, tags, click-through rates and interactive behaviour does not amount to **personal data**. This conclusion can only be reached following a **case-by-case analysis**, considering the processing nature, scope, purpose and context, to evaluate if the information

222 A29WP, 'Opinion 2/2010' (n 47) 5. This position is echoed in other jurisdictions like the UK with the UK DPA indicating that companies may find that it is easier to comply with the data protection law principles like data minimisation by using contextual advertising rather than forms of advertising involving end-user profiling; ICO (n 48) 45.

223 *ibid*.

meets the **four** core cumulative ingredients for **personal data**, namely, 'any information'; 'relating to'; 'identified and identifiable' and 'natural person'.[224] Current European judicial, legislative and regulatory approaches towards the concept of personal data are expansive and highly flexible with the relationship between an individual and a particular data point and the attendant identifiability level (direct or indirect) central factors in determining if the personal data threshold is reached.[225] Given the salience of these two factors in this regard, they are now considered further. Based on influential but non-binding regulatory guidance, information can **relate** to an individual in several ways: it is about the individual; it is not about the individual but is used or likely to be used to assess and nudge, for instance, the individual's conduct or deal with the individual in a specific manner, or the information is likely have an effect on the individual's rights and interests.[226] Thus, depending on further contextual specificities, click-through rates, geographical location, hover rates and other in-session information, either on their own or in conjunction with other data points like First-Party Cookie Data, can reach the **personal data threshold** when they are, for instance, about specific end-users, are used assess them as consumers (e.g. ad conversion metrics) or nudge them to click on ads.[227] When it comes to the second determinant of personal data, namely, **identifiability**, as highlighted by the scholarship and EU DPA outputs, this evaluation can be troublesome for a range of reasons including the non-binding status of the anonymisation test in the GDPR, the divergent guidance from EU DPAs on the permissible re-identification risk and the ever-shifting status of information along the identifiability spectrum based on objective factors like the re-identification cost, the time required for re-identification, technological developments and the current state of the art.[228] Notwithstanding, depending on the processing context, the key markers of identifiability may be met when, for instance, the end-user's personal data is singled out, data points associated with a specific person or group of persons are combined or inferences are drawn about end-users based on fragmented and diverse data points.[229] Here, organisations must **cyclically assess** whether the information processed for contextual advertising campaigns have reached the **personal data threshold** as, for example, new data points are added to the processing, new operations are rolled out and so on.

Second and relatedly, short-term and projected longer-term (so far) **progress** in **artificial intelligence** especially in data collection, analytics and targeting capabilities is likely to complicate the landscape further with additional and more granular data points, open to capture during browsing sessions, that provide the often opaque and changeable advertising ecosystem with novel and deeper insights into people's current lifestyle choices, health concerns, family building plans and so on. Thus, it is crucial that all **stakeholders** including industry and EU DPAs, evaluate, on a **case-by-case basis**,

224 See A29WP Opinion 4/2007 (n 91); Bygrave and Tosoni (n 91) 103.

225 See GDPR recital 26 and Art 4(1) (n 2); A29WP Opinion 4/2007 (n 91); Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 European Journal of Law and Technology 1; Bygrave and Tosoni (n 91) 103.

226 See A29WP Opinion 4/2007 (n 91) 10–11.

227 See see Della Corte and A29WP opinion on personal data (n 225).

228 *ibid*.

229 These criteria were proposed by the now defunct A29WP, '05/2014 Opinion on Anonymisation Techniques' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. accessed 24 November 2022. They have since between adopted by many EU DPAs in their anonymisation guidance. See Data Protection Commission Ireland, 'Guidance on Anonymisation and Pseudonymisation' (June 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf> 6–7 accessed 24 November 2022.

whether the deployment of specific innovative data capture, measurement, targeting and analysis techniques, which have reached market maturity, in particular contextual advertising campaigns, transform **raw information** in such ways that the **personal data threshold** is reached.[230]

Third, contextual advertisements delivered over social network sites, blogs and other types of **social media platforms** can be particularly problematic from a data protection law standpoint as they may lead to the pervasive and quotidian surveillance of people's shifting and real-time emotions, opinions and other online activities. Such rich information about people's current concerns, needs and activities can then be analysed using **innovative** and **emerging processes** and **techniques** like natural language processing, affective computing and machine tagging to, for example, identify, make inferences about and react to someone's opinions, attitudes and emotions towards a particular topic, brand, political figure, product and so on.[231] Here, a vast array of real-time and highly dynamic user-generated content like people's posts, photos, likes, retweets, shares, platform interactions (e.g. who they follow and direct message) and bookmarks are **minutely recorded**, **evaluated and mined** to provide **highly unique**, **time sensitive** and **detailed** insights into people's **current** emotions, opinions and so on.[232] Such knowledge can be acted upon in several ways. It can be used, on its own, to make real-time assessments of and inferences about the end-user's current opinions, preferences and feelings to select a contextual advertising campaign that corresponds to their present mindset. It can be amalgamated with other data points like first-party data, digital exhaust data[233] and self-reported[234] data to bolster more sophisticated end-user segmentation and appraisal to target end-users with promotions that are **tailored** to their actual needs at the time of ad delivery to increase the probability of **end-user engagement** and **conversion**.[235] It can also potentially feed into **predictive models** to estimate someone's medium and long-term preferences in order to target them with the

230 As noted by other scholars, linear and technological deterministic accounts of projected developments in the broad field of artificial intelligence are unhelpful given the tangled, contested, heterogeneous and unstable construction of specific technologies or techniques as 'technological artefacts.' See Raphael Gellert, 'Personal Data's Ever-Expanding Scope in Smart Environments and Possible Path(S) For Regulating Emerging Digital Technologies' (2021) International Data Privacy Law 1. For more on technological artefacts as 'hybrids' see Vranaki *Regulating Social Networking Sites* chapter 3 (n 13).

231 Affective computing refers to '…computing that relates to, arises from, or deliberately influences emotions.'; see Rosaline Picard, *Affective Computing* (MIT Press 2000) 5; Machine tagging involves the classification and parsing of text using machine learning classifiers like Support Vector Machine. See Minara P Anto, Anthony Mejo, KM Muhsina, Johny Nivy, James Vinay and Wilson Aswathy, 'Product Rating Using Sentiment Analysis' (2016 International Conference on Electrical, Electronics, and Optimization Techniques) 3458. For more on sentiment or opinion analysis, see Xing Fang and Justin Zhan, 'Sentiment Analysis Using Product Review Data' (2015) 2(1) Journal of Big Data 1; Ayushi Mitra, 'Sentiment Analysis Using Machine Learning Approaches (Lexicon based on movie review dataset' (2020) 2(03) Journal of Ubiquitous Computing and Communication Technologies 145.

232 See K Patel, D Mehta, C Mistry el al, 'Facial Sentiment Analysis Using AI Techniques: State-Of-The-Art, Taxonomies, and Challenges' (2020) 8 IEEE Access 90495; Ali Yadollahi, Ameneh Gholipour Shahraki and Osmar R Zaiane, 'Current State of Text Sentiment Analysis from Opinion to Emotion Mining' (2018) 50(2) ACM Computing Surveys 1 (on the links between sentiment analysis, emotion mining and opinion mining).

233 For example, IP address, device type, identifiers like platform identifier and browser type.

234 For example, email addresses, phone numbers and full names.

235 Bleier (n 204).

most relevant contextual advertising campaign at the right time in the future and/or be used as datasets to train machine learning algorithms.[236]

To what extent can **opinions** and **emotions**, to take two key aspects identified and assessed by such types of sentiment analysis on social media, amount to personal data? Due to space constraints, a thorough examination of this question is the task for another day. Generally, the answer depends on the processing context. The CJEU has long recognised that subjective information like opinions can amount to personal data if the required ingredients are met.[237] For example, the personal data threshold is crossed if the processing of personal data reveals **opinions** about an identified or identifiable person, or if it aims to evaluate how such individual views or feels about a particular matter. Moreover, where the processing of personal data reveals, for example, an end-user's political opinions or other forms of special data, the special data category threshold can also be crossed. [238] Crucially, to date the CJEU has adopted an expansive interpretation of the special data categories in its decisions to ensure that the objectives of the law, namely, providing a high level of protection to the individual's fundamental rights and freedoms are achieved.[239] Recent CJEU decisions continue to travel in this direction with, for example, the recent ruling that the processing of personal data that indirectly discloses special data categories, such as someone's sexual orientation, constitutes processing of special data categories.[240]

What about **emotions**? Can they meet the personal data threshold? Again, this is context dependent. There is a dearth of legislative, judicial and regulatory activity on this specific question so far. Although the GDPR's broad definition of personal data does not explicitly list emotions as a type of personal data, this is not a barrier for emotion data to amount to personal data in the right scenario. Based on existing, although non-binding, regulatory guidance, emotions, as with opinions, can in specific circumstances amount to personal data when they are, for instance, about specific identified or identifiable individuals or are used to evaluate, treat or influence people in particular ways in order to serve them the most relevant contextual advertisement.[241] As with opinions, certain emotions can fall under the special data category when they are used to shed light on or draw inferences about, for instance, someone's political leanings, religious beliefs and ethnicity. On a related note, in one of its recitals (instructive but not binding), the proposed ePrivacy Regulation recognises that emotions, in general, are 'highly sensitive' types of information.[242] This raises an important question about the

---

236 For example, Mitra (n 231) (on sentiment analysis and predictive modelling).

237 For example, Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994, [2017]. For an interesting analysis of the status of opinion *de facto* as personal data, see Dara Hallinan and Frederick Zuiderveen Borgesius, 'Opinions Can Be Incorrect (In Our Opinion)! On Data Protection Law's Accuracy Principle' (2020) 10(1) International Data Privacy Law 1.

238 See GDPR Art 9(1) (n 2).

239 For example, Case C-101/01, *Criminal proceedings against Bodil Lindqvist* EU:C:2003:596, [2003] OJ C118, paras 50 and 51. For a good overview of the CJEU and relevant jurisprudence on this see Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 365, 372–373.

240 Case C-184/20 *OT v Vyriausioji Tarnybinės Etikos Komisija* EU:C: 2022:601, [2022], paras 123 and 128.

241 For a cursory examination of this topic, see Eduard Fosch Villaronga, '"I Love You" Said The Robot: Boundaries of the Use of Emotions in Human-Robot Interactions' in Hande Ayanoğlu and Emília Duarte (eds), *Emotional Design in Human-Robot Interaction* (Springer 2019) 93.

242 See the ePrivacy regulation, recital 2 (n 4) and Council's ePrivacy Regulation, recital 2 (n 147).

status of emotion under data protection law. Does emotion, satisfying all the Art 4(1) ingredients, amount to personal data or a special data category?[243] In the future, this question must be addressed at appropriate levels, such as legislative, judicial and regulatory, to ensure **legal coherence** and **consistency**, which are crucial for several reasons including having laws that are **clear**, **make sense**, **work well** with one another (especially when they overlap in scope, application and goals), are **predictable**, are **uniformly interpre**ted (where applicable) and achieve their **intended objectives** (including protecting rights robustly as well as providing effective remedies and modes of redress when rights are breached).[244]

Having analysed when information processed for contextual campaigns meet one of the GDPR's central threshold concepts, namely, personal data, and highlighted areas of legal incoherence and inconsistency in the European data protection law regime, next the report scrutinises the legal ramifications of other GDPR provisions for contextual campaigns.

5.4 Contextual Advertising and the GDPR

Where the material and territorial scopes of the GDPR are met for specific contextual operations like matching people to advertisements and evaluating people's current preferences, opinions, emotions and needs, such processing must comply with the GDPR. In line with the report's scope (see **Section 3.3**), this section unpacks **six compliance challenges** raised by contextual advertising to highlight their far-reaching data protection law implications and galvanise stakeholder activities. For avoidance of doubt, depending on their specific operations and designs, contextual campaigns can also be problematic under other GDPR provisions like the fair, lawful and transparent processing principle; legitimate processing ground; special data categories processing, the data subjects' rights and data protection by design and default.[245] It should also be noted that even when personal data is not processed in contextual campaigns, such information remain subject to the provisions of European laws governing the processing of non-personal data.[246]

First, where personal data is collected for one or more contextual advertising purposes, such purposes must be **legitimate** (e.g. in accordance with existing laws including data protection laws), **explicit** and set out in **sufficient detail** so that individuals understand how and why their personal data are being processed for such purposes. Relatedly, such data must not be 'further' processed for

---

243 See Andrew McStay, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7(1) Big Data & Society 2053951720904386 for an interesting take on emotions and biometrics.

244 See Elina Paunio, 'Beyond Predictability–Reflections on Legal Certainty and the Discourse Theory of Law in the EU Legal Order' (2009) 10(11) German Law Journal 1469 (predictability and EU law); Jack M Balkin, 'Understanding Legal Understanding: The Legal Subject and the Problem of Legal Coherence' (1993) Yale Law Journal 105 (for a wider perspective, than usually present in traditional legal theory, on legal coherence); Neil MacCormick, 'The Requirement of 'coherence': Principles and Analogies' in Neil MacCormick (ed), *Legal Reasoning and Legal Theory* (OUP 1978) (for a traditional take in legal theory on coherence).

245 See Thilo Gottschalk and Francesca Pichierri, 'About Migration Flows and Sentiment Analysis on Twitter Data: Building the Bridge Between Technical and Legal Approaches to Data Protection' (LREC 2022 Joint Workshop Language Resources and Evaluation Conference 20–25 June 2022) 27, 40; GDPR Art 9(2) (n 20).

246 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Non-Personal Data Regulation) [2018] O J L 303, 59. OJ L 303, 28.11.2018, p. 59–68.

'incompatible' purposes unless such processing falls within the ambit of Art 89(1).[247] Specifically, if contextual advertising is to minimally interfere with the individual's fundamental rights and freedoms, it is essential for **EU DPAs** to offer organisations appropriate advice about the range of **contextual advertising purposes** that are permissible under the **purpose limitation principle**. Crucially, it is important that personal data collected for contextual advertising purposes are **not merged** with other data points like First-Party Cookie Data that organisations hold about individuals to prevent **extensive cross-platform profiling**, **ad targeting** and **data analytics** over a longer period than the browsing session.

Second, personal data processed for one or more contextual advertising purposes must be '**adequate**', '**relevant**' and '**limited**' to what is needed to achieve such purposes with personal data only processed where the pursued purposes cannot be **reasonably fulfilled** in other ways.[248] Adherence with the **data minimisation principle** requires a qualitative and quantitative evaluation of the precise number of data points, about an individual, required as a *minimum* to achieve the pursued processing purpose.[249] It also entails assessing the impact of the processing on the individual's fundamental rights and freedoms with data not processed where it disproportionally impacts on such rights.[250] There are close interplays between the data minimisation and storage limitation principles with, as explained later, the requirement to set the data retention period at 'a strict minimum'[251] to achieve the processing goal. Compliance with the data minimisation principle and related GDPR provisions can be particularly problematic for companies that operate across a range of often imbricated markets like search engines, social media, cloud computing, the Internet of Things and artificially intelligent assistants, as they have access to voluminous, high velocity, varied, real-time, historical and veracious datasets, which can be relationally analysed for contextual advertising purposes like predictions and targeting.[252] Crucially, such entities combine in-session browsing data points, collected for contextual advertising, with other plural data points they hold about individuals like First-Party Cookie Data to, for example, further extend the tentacles of modern surveillant assemblages to expand 'digital dossiers,'[253] routinely and automatically categorise individuals as belonging to particular consumption groups[254] and turn people into 'searchable databases'[255] for several AdTech operations.[256] Such ample, routine and continuous data combination clearly raises serious compliance questions under the data minimisation principle.

---

247 For more on assessing 'incompatible' further processing, see GDPR Art 6(4) (n 2).

248 GDPR Art 5(1)(c) (n 2).

249 see Terwangne (n 170) 317.

250 *ibid*.

251 See GDPR Art 5(1)(e) (n 2) and *ibid*.

252 For more on the characteristics of 'Big Data' databases, see Rob Kitchin, 'Big Data, New Epistemologies and Paradigm Shifts' (2014) 1(1) Big Data & Society 1.

253 Daniel Solove, *The Digital Person: Technology and Privacy In The Information Age* (vol 1) (New York University Press 2004) 1.

254 See Campbell and Carlson (n 12); Vranaki *Regulating Social Networking Sites: Data Protection, Copyright, and Power* Chapter 7 section 7.6 (n 13).

255 See David Lyon, 'Surveillance as Social Sorting,' in David Lyon (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003) 14.

256 For more on the surveillant assemblage, see Vranaki *Regulating Social Networking Sites: Data Protection, Copyright, and Power* Chapter 7, Section 7.4 (n 13).

Third, personal data processed for contextual advertising operations must be '**accurate**' and 'where necessary, kept **up to date**' with controllers under the obligation to take 'reasonable' steps to erase or rectify **inaccurate personal data** 'without delay'. This obligation must be discharged whilst considering the processing purposes pursued.[257] Compliance with this principle may be problematic in the context of emerging techniques used in contextual advertising like sentiment analysis which, given their early maturity levels, can potentially lead to inaccurate inferences.[258] Likewise, the personal data gathered may become inaccurate over time, post collection, as people's preferences, characteristics, emotions, opinions and other personal data change.[259] Here, when organisations undertake sentiment analysis based on social media, they can, as a starting point, use the tools offered by social media platforms like Twitter's Batch Compliance to verify the accuracy of the information over time.[260]

Fourth, personal data processed for contextual advertising must adhere to the **storage limitation principle** so that data is not 'kept for longer than necessary' to achieve the intended purpose. As mentioned earlier, companies offering varied and often overlapping digital offerings like social network sites, blogs, cloud-based storage facilities, instant messaging services, voice-over-IP services and wearables have the clear potential of merging contextual personal data points with other personal data they hold about individuals over the lifecycle of their data analytics operations. Where such data amalgamation occurs, it may significantly impact on the individual's data privacy rights because, for example, real-time in-session data are retained beyond the browsing session and are added to databases of historical and biographical (to name a few) data about the person for AdTech operations like audience construction, granular targeting and real-time data monitoring. Here, further **EU DPA guidance** on the **permissible retention period** for **contextual data points** is required. It is **recommended** that contextual data points are **permanently deleted** at the end of the **browsing session** to prevent such **data amalgamation**, which can feed into other advertising practices like profiling, predictions, targeting and segmentation based on large-scale cross-platform data surveillance.[261]

Fifth, the contextual advertising ecosystem is **complex** and **dynamic** with multiple actors, processes, techniques and practices involved to achieve objectives like targeting the right person with the right promotion. For example, a diverse, often opaque (to data subjects at least) and highly changeable range of actors like the targeted person, advertisers, publishers, data management organisations (including data analytics companies), advertising networks, advertising exchanges platforms and supply-side/demand-side platforms[262] are typically involved in contextual advertising. Thus, it is imperative that the lines of **data protection responsibilities** and **accountability** are clearly

257 GDRP Art 5(1)(d) (n 2).

258 See Kigon Lyu and Hyeoncheo Kim, 'Sentiment Analysis Using Word Polarity of Social Media' (2016) 89(3) Wireless Personal Communications 941; Douglas Rice and Christopher Zorn, 'Corpus-based Dictionaries For Sentiment Analysis of Specialized Vocabularies' (2021) 9(1) Political Science Research and Methods 20; Justin Grimmer, Margaret Roberts and Brandon Stewart, *Text As Data: A New Framework For Machine Learning and the Social Sciences* (Princeton University Press 2022) chapters 22-24 (on inferences).

259 For more on people's shifting preferences, behaviours and personal data, see Vranaki *Regulating Social Networking Sites: Data Protection, Copyright, and Power* chapter 6 (n 13).

260 Gottschalk and Pichierri (n 145).

261 European Commission (n 202) 31.

262 European Parliament JURI committee (n 208) 24.

articulated and recorded, before processing happens, so that the actors involved in the contextual advertising chain are clear about their identities (e.g. sole controller, joint controller and processor) and corresponding obligations under data protection laws. This **assessment** must be conducted on a **case-by-case basis** considering the processing nature, scope, purpose and context with careful evaluation of the **precise data flows** involved in the chain and the **forms of such data** (e.g. personal data, special data category, non-personal data, anonymised data and pseudonymised data) as they circulate from one actor to another. Crucially, as with First-Party Cookie Data, the legal status (and thus compliance obligations) of a particular actor can change throughout the data analytics lifecycle depending on its precise role in each stage of processing.

Finally, controllers must undertake a **DPIA** where their contextual advertising activities pose, in all likelihood, 'high risk' to the fundamental rights and freedoms of individuals especially where new technologies and techniques like natural language processing and sentiment analysis are utilised. Although the GDPR does not define the notion of high risk, it provides a non-exhaustive list of scenarios where the high-risk threshold is likely to be reached including the large-scale special data categories processing.[263] Elsewhere, the now-defunct A29WP has provided additional guidance (as always instructive but non-binding) on the additional criteria to be considered when making a high risk assessment including large-scale processing (e.g. volume, duration and geographical coverage of processing), combining data points in ways that are not within the reasonable expectation of the data subjects and using new technologies or techniques, considering the current state of the art, that provide innovative data capture and analytics processes with so-far unknown legal or societal consequences.[264] Overall, depending on the precise operations of particular contextual advertising campaigns and the onward flow of contextual data points to broader AdTech databases, a DPIA may be mandatory.

In sum, it is evident that the processing of personal data for contextual advertising campaigns raises profound, complicated and challenging data protection law compliance challenges that should be systematically identified and addressed, on a case-by-case basis, taking into account a broad range of factors including the impact of processing of the individual's data privacy rights.

6. Conclusion

This report has explored, at empirical and regulatory (including normative) levels, the impact of TPC decline on the AdTech sector. In particular, it has presented novel and detailed empirical findings on two Strategies, namely first-party cookies and contextual advertising, which are currently deployed in the AdTech industry to sustain and bolster contemporary AdTech practices like data capture, predictions, ad targeting, personalisation and data mining in the absence of TPC. It has also presented new lines of analyses, not currently present in the data protection law and regulation literature, on the impact of these new Strategies on the level of protection afforded to the individual's fundamental rights and freedoms. **Five** main contentions have been advanced. To start, from a regulatory lens, the phasing out of TPC has important implications for the AdTech's data protection regulatory space, which is gradually becoming even more intricate, changeable and intractable than was the case when TPC was at the heart of many AdTech activities. Consequently, a more diverse and convoluted range

263 GDPR Arts 35 (1) (high-risk) and 35(3)(a)-(c) (when is a DPIA required?) (n 2).

264 European Commission, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (13 October 2017) <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711> 9–10 accessed 24 November 2022.

of actors, processes, techniques and practices than those present in TPC-fuelled operations are increasingly involved on the ground in the AdTech processing chain with far-reaching implications for data privacy regulation (including the level of protection afforded to people's fundamental rights and freedoms in practice). This marked change in the regulatory space necessitates thorough, exacting and highly contingent exploration. Second, the growing roles of first-party cookies and their attendant personal data in the AdTech processing chain can be highly problematic from a data protection law perceptive due to several reasons including the tangled, intricate and manifold range of legal issues raised under plural legal frameworks; the current lack of comprehensive and contextual assessment of the impact of, for example, the processing of First-Party Cookie Data points on the individual's data privacy rights and the current regulatory (including legal) disparities and discontinuities which impact on the level of protection afforded to the individual's data privacy rights on the ground. Third, central regulatory actors in the European data protection law regime like EU DPAs must scrutinise afresh their understandings of how first-party cookies are now deployed in practice in the AdTech chain and relatedly review their assessments of how such new uses interfere with the individual's fundamental rights and freedoms like data protection and privacy. Fourth, turning to another strategy, namely contextual advertising, this report has contended that it is imperative that current divergences, concerning contextual campaigns, between the actors involved in different stages of data privacy regulation are ironed out for the sake of regulatory coherence. Finally, just like first-party cookies, contextual advertising often raises highly difficult and highly situated data protection law ramifications that should be identified and addressed by carefully evaluating the precise contours, dimensions and affordances of the specific AdTech chain within which such campaigns find themselves. Much work remains to be done in this space to comprehensively capture the expanding range of Strategies, including first-party cookies and contextual advertising, which are silently but inexorably joining the AdTech chain, evaluate their impact on the data privacy regulatory space and scrutinise, based on up-to-date and reliable evidence of how these Strategies operate on the ground, their implications for data protection law and regulation.

Bibliography

Primary sources

European Union Cases

Case C-101/01, *Criminal proceedings against Bodil Lindqvist* EU:C:2003:596, [2003]

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C: 2016:779, [2016] ECR 00000

Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C: 2017:994, [2017]

Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C: 2019:801, [2019] ECR 00000

Case C-25/17 *Jehovah Todistajat* EU:C: 2018:551, [2018]

Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* EU:C: 2019:629, [2019] ECR 00000

Case C-184/20 *Vyriausioji Tarnybinės Etikos Komisija v Fondas 'Nevyriausybinių Organizacijų Informacijos Ir Paramos Centras' OT v Vyriausioji Tarnybinės Etikos Komisija* EU:C: 2022:601, [2022] ECR 00000

National Cases

Court of Appeal of Brussels, Market Court, Decision on the merits 21/2022 of 2 February 2022, *IAB Europe v Data Protection Authority* 2022/AR/292 (2022)

Decisions from EU DPAs

DOS-2019-01377, *Decision on the merits 21/2022 of 2 February 2022* (Belgian Data Protection Authority 2022)

Legislation

European Union

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ 2002 L201, 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337, 11

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] OJ L119, 1

Proposal For a Regulation of the Parliament and of the Council (EU) Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Non-Personal Data Regulation) [2018] O J L 303, 59

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, 1

Proposal for a Regulation of the Parliament and of the Council (EU) concerning the Respect for Private Life and The Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2021] 6087/21

Legislation from Other Jurisdictions

California Consumer Privacy Act of 2018 AB-375, Title 1.81.5

Data Protection Act 2018 (Number 7 of 2018) (Ireland)

European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI No 336 of 2011) (Ireland)

Secondary Sources

Books

Bryman A, *Social Research Methods* (Oxford University Press 2012)

Creutzfeldt N, Mason M and McConnachie K (eds), *Routledge Handbook of Socio-legal Theory and Methods* (Routledge 2019)

European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, and European Data Protection Supervisor (eds), *Handbook on European Data Protection Law* (Publications Office of the European Union 2018)

Grimmer J, Roberts M and Stewart B, *Text As Data: A New Framework For Machine Learning and the Social Sciences* (Princeton University Press 2022)

Hutter B, *Compliance: Regulation and Environment* (Oxford University Press 1997)

Kuner C, Bygrave L, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Latour B, *Science in Action* (Open University Press 1987)

Lopez-Tarruella A, *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge* (Springer 2012)

Nettleton D, *Commercial Data Mining: Processing, Analysis and Modeling For Predictive Analytics Projects* (Elsevier 2014)

Picard R, *Affective Computing* (MIT Press 2000)

Rrunkler T, *Data Analytics* (Springer 2012)

Solove D, *The Digital Person: Technology and Privacy in the Information Age* (vol 1) (New York University Press 2004) 1

Spiekermann S, *Ethical IT Innovation: A Value-Based System Design Approach* (Taylor & Francis 2016)

Vranaki Asma, *Regulating Social Networking Sites: Data Protection, Copyright, and Power* (Edward Elgar Publishing forthcoming)

Wiener N, *The Human Use of Human Beings: Cybernetics and Society* (Doubleday Anchor 1954)

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

Book Chapters

Barocas S and Nissenbaum H, 'Big Data's End Run Around Anonymity and consent' in Lane J, Stodden V, Bender S and Nissenbaum H (eds), *Privacy, Big Data, and the Public Good* (Cambridge University Press 2014)

Black J, 'The Role of Risk in Regulatory Processes' in Baldwin R, Cave M and Lodge M (eds), *The Oxford Handbook of Regulation* (Oxford 2010)

Bygrave L and Tosoni L, 'Article 4(1), Personal Data' in Kuner C, Bygrave L, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2020)

Bygrave L, 'Article 25 Data Protection By Design and By Default' in Kuner C, Bygrave L, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Domingo-Ferrer J and Blanco-Justicia A, 'Privacy-preserving Technologies' in Christen M (ed), *The Ethics of Cybersecurity* (The International Library of Ethics, Law and Technology 2020)

Edwards L, 'Data Protection and e-Privacy: from Spam And Cookies to Big Data, Machine Learning and Profiling' in Edwards L (ed), *Law, Policy and the Internet* (Hart 2018)

Fogg BJ, 'Introduction' in Fogg BJ (ed), *Interactive Technologies, Persuasive Technology* (Morgan Kaufmann 2003)

Friedman B, Kane PH Jnr and Borning A, 'Value Sensitive Design and Information Systems' in Himmar KE and Tavani HT (eds), *The Handbook of Information and Computer Ethics* (Wiley 2008)

Georgieva L and Kuner C, 'Article 9 Processing of Special Categories of Personal Data' in Kuner C, Bygrave L, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Hancher L and Moran M, 'Organizing Regulatory Space: Capitalism, Culture and Economic Regulation' in Baldwin R, Scott C and Hood C (eds), *A Reader on Regulation* (Oxford University Press 1989)

Hutchinson H, 'Doctrinal Research: Researching the Jury' in *Research Methods in Law* (Routledge 2013)

Lyon D, 'Surveillance as Social Sorting' in Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003)

MacCormick N, 'The Requirement of 'Coherence': Principles and Analogies' in MacCormick N (ed), *Legal Reasoning and Legal Theory* (OUP 1978)

McStay A, 'Micro-moments, Liquidity, Intimacy and Automation: Developments in Programmatic Ad-tech' in Siegert G, Rimscha MB and Grubenmann S (eds), *Commercial Communication in the Digital Age – information or disinformation?* (De Gruyter Saur 2017)

Nouwt S, 'The Role of Data Protection Authorities' in Y Poullet, P de Hert and C de Terwangne (eds), *Reinventing Data Protection?* (Springer 2009)

Poullet Y, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Gutwirth S, Poullet Y and de Hert P (eds), *Data Protection in a Profiled World* (Springer 2010)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009)

Skouma G and Léonard L, 'On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection' in Gutwirth S, Leenes R and de Hert P (eds), *Reforming European Data Protection Law* (Springer 2015)

Stalla-Bourdillon S and Rossi A, 'Aggregation, Synthesisation and Anonymisation A Call For A Risk-Based Assessment of Anonymisation Approaches' in Hallinan D, Leenes R and de Hert P, *Data Protection and Privacy: Data Protection and Artificial Intelligence* (CPDP Vol 13, Hart Publishing 2021)

Terwangne C, 'Article 5 Principles Relating to Processing of Personal Data' in Kuner C, Bygrave L, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Tham S, Rodgers S and Thorson E, 'Trends and Opportunities for Digital Advertising Research: a Content Analysis of Advertising Age, 2000–2015' in Rodgers S and Thorson E (eds), *Digital Advertising Theory and Research* (Routledge 2017)

Tzoulia E, 'Targeted Advertising in the Digital Era: Modern Challenges to Consumer Privacy and Economic Freedom: The Responses of the EU Legal Order' in Synodinou T-E, Jougleux P, Markou C and Prastitou-Merdi T (eds), *EU Internet Law in the Digital Single Market* (2021 Springer)

Villaronga Eduard Fosch, '"I Love You" Said The Robot: Boundaries of the Use of Emotions in Human-Robot Interactions' in Ayanoğlu Hande and Duarte Emília (eds), *Emotional Design in Human-Robot Interaction* (Springer 2019)

Vranaki A, 'Cloud Investigations by European Data Protection Authorities: an Empirical Account' in Rothchild JA (ed), *Research Handbook on Electronic Commerce Law* (Edward Elgar Publishing 2016a)

Warren C, 'Qualitative Interviewing' in Gubrium JF and Holstein JA (eds), *Handbook of Interview Research: Context and Method* (Sage 2002)

Webley L, 'Qualitative Approaches to Empirical Legal Research' in Cane P and Kritzer HM (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010)

Journal Articles

Abbas A, Hidayet A, Selcuk UA and Conti M, 'A Survey on Homomorphic Encryption Schemes: Theory and Implementation' (2018) 51(4) ACM Computing Surveys article 79

Acquisti A and Gross R, ‘Imagined Communities: Awareness, Information Sharing, and Privacy on Facebook’ (2006) Privacy Enhancing Technologies Workshop

Acquisti A, Brandimarte L and Loewenstein G, ‘Privacy and Human Behavior in the Age of Information’ (2015) 347(6221) Science 509

Acquisti A, Taylor C and Wagman L, ‘The Economics of Privacy’ (2016) 54(2) Journal of Economic Literature 442

Alessi M, Alessio C, Enza G, Matera M, Pino S and Storelli D, ‘A Decentralized Personal Data Store Based on Ethereum: Towards GDPR Compliance’ (2019) 5(2) Journal of Communications Software and Systems

Balkin JM, ‘Understanding Legal Understanding: The Legal Subject and the Problem of Legal Coherence’ (1993) Yale Law Journal 105

Bashir A and Wilson C, ‘Diffusion of User Tracking Data in the Online Advertising Ecosystem’ (2018) 4 Proceedings on Privacy Enhancing Technologies 85

Bleier A, ‘On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web’ (2022) SSRN eLibrary <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3980001> accessed 29 May 2022

Boerman SC, Kruikemeier S and Borgesius FJZ, ‘Online Behavioral Advertising: A Literature Review and Research Agenda’ (2017) 46(3) Journal of Advertising 363

Borgesius FZ, ‘Behavioral Targeting, A European Legal Perspective (2013) 11(1) IEEE Security & Privacy 82

Borgesius FZ, ‘Personal Data Processing For Behavioural Targeting: Which Legal Basis?’ (2015) 5(3) International Data Privacy Law 163

Borking J and Raab C, ‘Laws, PETs and Other Technologies For Privacy Protection‘ (2001) 1(1) Journal of Information, Law & Technology

Bortz A, Barth A and Czeskis A, ‘Origin Cookies: Session Integrity For Web Applications’ (2011) Web 2.0 Security and Privacy (W2SP)

Brown I, ‘Data Protection: The New Technical and Political Environment’ (2010) 20(6) Computers & Law

Buratto A, Grosset L and Viscolani B, ‘Advertising a New Product in a Segmented Market’ (2006) 175(2) European Journal of Operational Research 1262

Bygrave L, ‘Data Protection By Design and By Default : Deciphering The EU’s Legislative Requirements’ (2017) 4(2) Oslo Law Review 105

Campbell J, Goldfarb A and Tucker C, ‘Privacy Regulation and Market Structure’ (2015) 24(1) Journal of Economics & Management Strategy 47

Campbell JE and Carlson M, ‘Panopticon. com: Online Surveillance and the Commodification of Privacy’ (2002) 46(4) Journal of Broadcasting & Electronic Media 586

Cate FH and Mayer-Schönberger V, ‘Notice and Consent in a World of Big Data’ (2013) 3(2) International Data Privacy Law 67

Chen J, Edwards L, Urquhart L and McAuley D, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) International Data Privacy Law

Choi JA and Kiho L, 'Identifying Machine Learning Techniques For Classification of Target Advertising' (2020) 6(3) ICT Express 175

Clifford D, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the Crumbs of Online User Behavior' (2014) 5 Journal of Intellectual Property Information Technology & Electronic Commerce Law 194

Cooper DA, Yalcin T, Nistor C, Macrini M and Pehlivan E, 'Privacy Considerations For Online Advertising: A Stakeholder's Perspective to Programmatic' (2022) 7 Journal of Consumer Marketing

Coppens B and Zendra O, 'Privacy: Whether You're Aware of it or Not, it Does Matter!' (2021) HiPEAC Vision 1

Costello RÁ, 'The Impacts of AdTech on Privacy Rights and the Rule of Law' (2020 April) Technology and Regulation 11

Crouch M and McKenzie H, 'The Logic of Small Samples in Interview-Based Qualitative Research' (2016) 45(4) Social Science Info 483

Dalla Corte L, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 European Journal of Law and Technology 1

Dao H, Mazel J and Fukuda K, 'CNAME Cloaking-based Tracking on the Web: Characterization, Detection and Protection' (2021) 18(3) IEEE Transactions on Network and Service Management 3873

Demir N, Theis D, Urban T and Pholmann N, 'Towards Understanding First Party Cookie Tracking in the Field' (2022) ARXIV

Donahue M, 'Times the Times They Are A Changin' - Can the Ad Tech Industry Survive In A Privacy Conscious World?' (2021) 30(1) Catholic University Journal of Law and Technology Article 7

Dumortier J, 'Evaluation and Review of the ePrivacy Directive' (2016) 2 European Data Protection Law Review 247

Dwork C and Roth A, 'The Algorithmic Foundations of Differential Privacy' (2013) 9(3-4) Foundations and Trends in Theoretical Computer Science 211

Esteve A, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA' (2017) 7(1) International Data Privacy Law 36–47

Fang X and Zhan J, 'Sentiment Analysis Using Product Review Data' (2015) 2(1) Journal of Big Data 1

Fearnley C, 'Mind Mapping in Qualitative Data Analysis: Managing Interview Data in Interdisciplinary and Multi-sited Research Projects' (2022) 9 Geography and Environment

Finck M, 'The Limits of the GDPR in the Personalisation Context' (2021) Max Planck Institute for Innovation and Competition Research Paper N21-11

Gal M and Oshrit A, 'The Unintended Competitive Effects of the GDPR' (2020) Journal of Competition Law and Economics

Gandy Jr OH, 'Coming to Terms with the Panoptic Sort' (1996) Computers, Surveillance, and Privacy 132

Gellert R, 'Personal Data's Ever-Expanding Scope in Smart Environments and Possible Path(S) For Regulating Emerging Digital Technologies' (2021) International Data Privacy Law 1

Geradin D and Katsifis D, '"Trust me, I'm fair": Analysing Google's Latest Practices in Ad Tech From the Perspective of EU Competition Law' (2020) 16(1) European Competition Journal 11 section II

Geradin D, Karanikioti T and Katsifis D, 'GDPR Myopia: how a Well-Intended Regulation Ended Up Favouring Large Online Platforms - The Case of Ad Tech' (2021) 17(1) European Competition Journal 47

Gerber N, Gerber P and Volkamer M, 'Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior' (2018) 77 Computers & Security 226

Goldfarb A, 'What is Different About Online Advertising? Review of Industrial Organization' (2014) 44(2) Special Issue: Symposium on The Economics of Internet Advertising 115

Grafenstein M, Heumüller J, Belgacem E, Jakobi T and Smiesko P, 'Effective Regulation Through Design – Aligning The Eprivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection By Design Approach' (19 October 2021) SSRN eLibrary <https://ssrn.com/abstract=3945471> accessed 24 November 2022

Guida S, 'Third-party Cookies and Alternatives: What Consequences in Terms of Consent?' (2021) 2 European Journal of Privacy Law & Technologies

Häglund E and Björklund J, 'AI-Driven Contextual Advertising: A Technology Report and Implication Analysis (2022) arXiv preprint arXiv:2205.00911

Hallinan D and Borgesius FZ, 'Opinions Can Be Incorrect (In Our Opinion)! On Data Protection Law's Accuracy Principle' (2020) 10(1) International Data Privacy Law 1

Harding WT, Reed AJ and Gray RL, 'Cookies and Web bugs: What They Are and How They Work Together' (2001) 18(3) Information Systems Management 17

Hoofnagle CJ, Soltani A, Good N, Wambach D and Ayenson M, 'Behavioral Advertising: The Offer You Can't Refuse' (2012) 6 Harvard Law & Policy Review 273

Hutchinson T, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 8 Erasmus Law Review 130

Jablonowska A and Michatowicz A, 'Planet49: Pre-Ticked Checkboxes are not Sufficient to Convey User's Consent to the Storage of Cookies' (2020) 6 European Data Protection Law Review 137

Janssen H and Singh J, 'Personal Information Management Systems' (2022) 11(2) Internet Policy Review

Jasmontaite L, Kamara I, Zanfir-Fortuna G and Leucci S, 'Data Protection By Design And By Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4(2) European Data Protection Law Review

Jelodar H, Wang Y, Yuan C, Feng X, Jiang X, Li Y and Zhao L, 'Latent Dirichlet allocation (LDA) and Topic Modeling: Models, Applications, A Survey' (2019) 78(11) Multimedia Tools and Applications 15169

Jia J, Zhe JG and Wagman L, 'The Short-run Effects of GDPR on Technology Venture Investment' (NBER Working Paper No w25248 2019)

Jindal K and Aron R, 'A Systematic Study of Sentiment Analysis for Social Media Data' (2021) Computer Science: Materials Today

Kaushik G and Rishabh P, 'Collection of Data Through Cookies and Smart Devices–a case study' (2018) 4(5) International Journal of Advance Research, Ideas and Innovations in Technology 458

Kesan JP and Shah RC, 'Deconstructing Code' (2003) 6 Yale Journal Law & Technology 277

Kirsch M, 'Do-not-track: Revising the EU's Data Protection Framework to Require Meaningful Consent For Behavioral Advertising (2011) 18 Richmond Journal of Law & Technology 1

Kitchin R and McArdle G, 'What Makes Big Data, Big Data? Exploring the Ontological Characteristics of 26 Datasets' (2016) 3(1) Big Data & Society

Kitchin R, 'Big Data, New Epistemologies and Paradigm Shifts' (2014) 1(1) Big Data & Society 1

Kokott J and Sobotta C, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3(4) International Data Privacy Law 222

Kosta E, 'Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies' (2013) 21 International Journal of Law and Information Technology 27

Kosta E, 'The Netherlands: The Dutch Regulation of Cookies' (2016) 2 European Data Protection Law Review 97

Kretschmer M, Pennekamp J and Wehrle K, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web' (2021) 15(4) ACM Trans art 20

Latham O, Hervé and Bizet R, 'Antitrust Concerns in Ad-Tech: Formalizing the Combined Effect of Multiple Conducts and Behaviours' (2021) 17(2) European Competition Journal 353

Latvala L, Horn J and Bruno B, 'Thriving in the Age of Privacy Regulation: A First-party Data Strategy' (2022) 7(3) Applied Marketing Analytics 211

Leenes R and Kosta E, 'Taming the Cookie Monster with Dutch law–a Tale of Regulatory Failure' (2015) 31(3) Computer Law & Security Review 317

Lynskey O, 'Track[ing] Changes: an Examination of EU Regulation of Online Behavioral Advertising Through a Data Protection Lens' (2011) 36(6) European Law Review 874

Lyu K and Kim H, 'Sentiment Analysis Using Word Polarity of Social Media' (2016) 89(3) Wireless Personal Communications 941

Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information & Communications Technology Law 146, 171

Mantelero A, 'The Future of Consumer Data Protection in the EU Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30(6) Computer Law & Security Review 643

Mason WH and Wolfinger NH, 'Cohort Analysis' (2001) California Center for Population Research UCLA On-Line Working Paper Series

McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4(1) Journal of Law and Policy for the Information Society 543

McStay A, 'Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy' (2020) 7(1) Big Data & Society 2053951720904386

Mellet K and Beauvisage T, 'Cookie Monsters. Anatomy of a Digital Market Infrastructure' (2019) Consumption, Markets and Culture

Mitra A, 'Sentiment Analysis Using Machine Learning Approaches (Lexicon Based On Movie Review Dataset' (2020) 2(03) Journal of Ubiquitous Computing and Communication Technologies 145

Mori T, Inoue T, Shimoda A, Sato K, Harada S, Ishibashi K and Goto S, 'Statistical Estimation of the Names of HTTPS Servers With Domain Name Graphs' (2016) 94 Computer Communications 104

Naithani P, 'Practitioners' Corner: Regulating the Fingerprinting Monster Through EU Data Protection' (2021) 7(4) European Data Protection Law Review 184

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701

Pastor A, Cuevas R, Cuevas Á and Azcorra A, 'Establishing Trust in Online Advertising With Signed Transactions' (2020) IEEE Access

Patel K, Mehta D, Mistry C, Gupta R, Tanwar S, Patel NK and Alazab M, 'Facial Sentiment Analysis Using AI Techniques: State-Of-The-Art, Taxonomies, and Challenges' (2020) 8 IEEE Access 90495

Paunio E, 'Beyond Predictability–Reflections On Legal Certainty and the Discourse Theory of Law in the EU Legal Order' (2009) 10(11) German Law Journal 1469

Rafieian O and Hema Y, 'Targeting and Privacy in Mobile Advertising' (2020) 2(40) Marketing Science 193

Rice D and Zorn C, 'Corpus-based Dictionaries for Sentiment Analysis of Specialized Vocabularies' (2021) 9(1) Political Science Research and Methods 20

Scott-Morton FM, Crawford GS, Crémer J, Dinielli D, Fletcher A, Heidhues P, Schnitzer M and Seim Ka, 'Equitable Interoperability: The 'Super Tool' of Digital Platform Governance' (Digital Regulation Project - Policy Discussion Paper 2021)

Shanmugarasa Y, Hye-Young P, Kanhere SS and Zhu L, 'Towards Automated Data Sharing in Personal Data Stores' (2022) 20(1) IEE Security & Privacy

Shoban BS, 'Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data' (2017) 6(21) International Journal of Advanced Research in Computer and Communication Engineering

Solove D, 'The Myth of the Privacy Paradox' (2021) 89(1) George Washington Law Review 1

Strycharza J, Smita E, Helberger N and Noort G, 'No to Cookies: Empowering Impact of Technical and Legal Knowledge On Rejecting Tracking Cookies' (2021) 120 Computers in Human Behavior

Takata Y, Ito D, Kumagai H and Kamizono M, 'Risk Analysis of Cookie Sharing By Link Decoration and CNAME Cloaking' (2021) 29 Journal of Information Processing 649

Tene O and Polenetsky J, 'To Track Or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising' (2011) 13 Minnesota Journal Law Science & Technology 281

Tene O and Polonetsky J, 'Big Data For All: Privacy and User Control in the Age of analytics' (2012) 11 Northwestern Journal of Technology & Intellectual Property xxvii

Veale M and Borgesius FZ, 'Adtech and Real-Time Bidding Under European Data Protection Law' (2022) German Law Journal 23(2) 226

Vranaki A and Farmer F, 'Third-party cookies, Data Analytics and Targeted Advertisements: Of Data Protection Law and Regulation (II)' Forthcoming

Vranaki A, 'Data Governance in the Cloud: Of Scarce Regulatory Resources and Tactical Delegated Enforcement' [2021] Public Law 125

Vranaki A, 'Learning Lessons From Cloud Investigations in Europe: Bargaining Enforcement and Multiple Centers of Regulation In Data Protection' (2016b) 2 University of Illinois Journal of Law and Technology 245

Vranaki A, 'Social Networking Site Regulation: Facebook, Online Behavioral Advertising, Power and Data Protection Laws' (2017) 43(2) Rutgers Computer & Technology Law Journal 169

Wachter S, 'Affinity Profiling and Discrimination By Association in Online Behavioral Advertising' (2020) 35 Berkeley Technology Law Journal 367

Waldman AE, 'Data Protection By Design? A Critique of Article 25 of the GDPR' (2021) 53 Cornell International Law Journal

Ward W, 'The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?' (2022) 25 Trinity College Law Review 221

Wiedemann K, 'The ECJ's Decision in "Planet49"(Case C-673/17): A Cookie Monster or Much Ado About Nothing?' (2020) 51(4) International Review of Intellectual Property and Competition Law 543

Williams BA, Brooks CF and Shmargad Y, 'How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications' (2018) 8 Journal of Information Policy 78

Wojdynski B and Bang H, 'Distraction Effects Of Contextual Advertising on Online News Processing: An Eye-Tracking Study' (2016) 35(8) Behaviour and Information Technology 654

Yadav A and Vishwakarma DK, 'Sentiment Analysis Using Deep Learning Architectures: A Review' (2020) 53(6) Artificial Intelligence Review 4335

Yadollahi A, Shahraki AG and Zaiane OR, 'Current State of Text Sentiment Analysis from Opinion to Emotion Mining' (2018) 50(2) ACM Computing Surveys 1

Yana D, G Acar, L Olejnik, W Joosen and T Van Goethem, 'The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion' (2021) 3 Proceedings on Privacy Enhancing Technologies 394

Ylijoki O and Porras J, 'Perspectives to Definition of Big Data: A Mapping Study and Discussion' (2016) 4(1) Journal of Innovation Management

Zhang K and Katona Z, 'Contextual Advertising' (2012) 31(6) Marketing Science 980

Zimmerman RK, 'The Way The Cookies Crumble: Internet Privacy And Data Protection In The Twenty-first Century' (2000) 4 New York University Journal of Legislation & Public Policy 439

Conference Papers and Proceedings

Assel A and Egele M, 'Oversharing is Not Caring: How CNAME Cloaking Can Expose Your Session Cookies' (Proceedings of the ACM Asia Conference on Computer and Communications Security 2021)

Barocas S and Nissenbaum H, 'On Notice: The Trouble With Notice and Consent' (Proceedings of the engaging data forum: The first international forum on the application and management of personal electronic information 2009)

Cheng H, Jianbing N, Rongxing L, and Shen Xuemin S, 'Online Advertising With Verifiable Fairness' (IEEE International Conference on Communications 2019)

Coopamootoo Kovila PL, 'Usage Patterns of Privacy-Enhancing Technologies' (CCS '20, 9–13 November 2020, Virtual Event, USA) <https://dl.acm.org/doi/pdf/10.1145/3372297.3423347 > accessed 23 April 2022

Cummings R and Desai D, 'The Role of Differential Privacy in GDPR Compliance' (Position paper, FATREC'18, October 2018, Vancouver, Canada) < https://cpn-us-w2.wpmucdn.com/sites.gatech.edu/dist/c/679/files/2018/09/GDPR_DiffPrivacy.pdf> accessed 4 July 2022

Dao H, Mazel J and Fukuda K, 'Characterizing CNAME Cloaking Based Tracking on the Web' (IEEE/IFIP Network Traffic Measurement and Analysis Conference 2020)

Gottschalk T and Pichierri F, 'About Migration Flows and Sentiment Analysis on Twitter Data: Building the Bridge Between Technical and Legal Approaches to Data Protection' (LREC Joint Workshop Language Resources and Evaluation Conference 20–25 June 2022)

Imane I, Santos C, Al Kassar F, Bielova N and Calzavara S, 'On Compliance of Cookie Purposes With the Purpose Specification Principle' (International Workshop on Privacy Engineering, Genova, Italy 1–8 April 2020)

Minara PA, Mejo A, Muhsina KM, Nivy J, Vinay J and Aswathy W, 'Product Rating Using Sentiment Analysis' (International Conference on Electrical, Electronics, and Optimization Techniques 2016) 3458

Sanchez-Rola I, Dell'Amico M, Kotzias P, Balzarotti D, Bilge L, Vervier P-A and Santos I, 'Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control' (14th ACM Asia Conference on Computer and Communications Security 2019) 340

Sivakorn S, Polakis I and Keromytis A, 'The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information' (Proceedings of the IEEE Symposium on Security and Privacy 2016) 724–742 <https://doi.org/ 10.1109/SP.2016.49.> accessed 24 November 2022

Spiekermann S, Grossklags J and Berendt B, 'E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior' (Proceedings of the 3rd ACM conference on electronic commerce 2001) 38

Tongwei R, Wittman A, De Carli L and Davidson D, 'An Analysis of First-party Cookie Exfiltration Due to CNAME Redirections' (Workshop on Measurements, Attacks, and Defenses for the Web–

MADWeb 2021) <https://web.cs.wpi.edu/~ldecarli/docs/papers/madweb21-cloaking.pdf> accessed 29 May 2022

Zhang H, Guerrero C, Wheatley D and Seok LY, 'Privacy Issues and User Attitudes Towards Targeted Advertising: A Focus Group Study' (Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting 2010) <https://journals.sagepub.com/doi/pdf/10.1177/154193121005401913> accessed 23 May 2022

Websites

Bing L, 'The Science of Detecting Fake Reviews' (*Content24,* 18 May 2012) <http://content26.com/blog/bing-liu-the-science-of-detecting-fake-reviews/> accessed 24 November 2022

Burgess M, 'Google's Plan to Eradicate Cookies is Crumbling' (*Wired*, 2021) <https://www.wired.co.uk/article/google-floc-trial> accessed 28 April 2022

Cypher B, 'Google's FLoC Is a Terrible Idea' (*EFF*, 2021) <https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea> accessed 23 April 2022

EOLOGY, 'Everything Will Be New in 2022: Google Stops FLOC – from now on Topics will be interesting' (*Eology,* 2022) < https://www.eology.net/news/google-topics> accessed 23 April 2022

Frederic L, 'Goodle kills off FloC, replaces it with Topics' (*Techcrunch+,* 25 January 2022) <https://techcrunch.com/2022/01/25/google-kills-off-floc-replaces-it-with-topics> accessed 24 November 2022

Garfield B, 'Digital Society: Regulating Privacy and Content Online' (*Solent University*, 2020) <https://pure.solent.ac.uk/ws/files/17068932/DigitalSocietyReport.pdf> accessed 23 April 2022

Ghosh D, 'How GDPR Will Transform Digital Marketing' (*Harvard Business Review*, 21 May 2018) <https://scholar.harvard.edu/files/dipayan/files/how_gdpr_will_transform_digital_marketing.pdf> accessed 23 April 2022

Glomb T, 'Say Goodbye to Cookies' (*Harvard Business Review*, 8 April 2021) <https://hbr.org/2021/04/say-goodbye-to-cookies> accessed 9 August 2021

IAPP, 'The Way the Third-party Cookie Crumbles: Part 2 – Shifting Industry Practices and alternatives to third-party Cookies' (*IAPP,* 2021) <https://iapp.org/news/a/the-way-the-third-party-cookie-crumbles-part-2-shifting-industry-practices-and-alternatives-to-third-party-cookies/ > accessed 23 April 2022

ISO, 'ISO/IEC 27701:2019 Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines' (*ISO,* 2022) <https://www.iso.org/standard/71670.html> accessed 23 April 2023

Jernigan C and Mistree B, 'Gaydar: Facebook Friendships Expose Sexual Orientation' (*First Monday*, 2009) 14 <https://firstmonday.org/article/view/2611/2302> accessed 23 May 2022

Kihn M, 'Did Google Just Kill Independent Attribution' (*AdExchanger*, 2018) <https://www.adexchanger.com/analytics/did-google-just-kill-independent-attribution/ > accessed 24 May 2022

Lapowsky I, 'Concern Trolls and Power Grabs: Inside Big Tech's Angry, Geeky, Often Petty War For Your Privacy' (*Protocol*, 2021) < https://www.protocol.com/policy/w3c-privacy-war> accessed 6 July 2022

Marvin G, 'The New Contextual Ad Targeting Works, Study Says' (*Search engineland,* 2020) <https://searchengineland.com/the-new-contextual-ad-targeting-works-study-says-331574 > accessed 8 July 2022

McKee M, 'Brand Bias: 70% of Consumers Look For Known Retailers When Doing Product Searches' (*Search engine land,*2013) <https://searchengineland.com/brand-bias-70-of-consumers-look-for-known-retailers-when-doing-product-searches-179570> accessed 26 May 2022

Netter N, '"Free" Online Service in Exchange for Targeted Advertising : The Business Model With Feet of Clay' (*HAL Open Science,* 2021) <https://hal.archives-ouvertes.fr/hal-03329824/document> accessed 24 November 2022

REPHRAIN, 'Home' (2022) <https://www.rephrain.ac.uk/ > accessed 15 May 2022

Schiff A, 'Google will not run FLoC Origin Tests in Europe due to GDPR Concerns (At Least For Now)' (*AdExchanger*, 2021) < https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/> accessed 4 July 2022

Scrueurs R, 'Take a Deep Breath and Consider the Benefits Of Google's Topics API' (*AdExchanger*, 2022) < https://www.adexchanger.com/ad-exchange-news/take-a-deep-breath-and-consider-the-benefits-of-googles-topics-api/> accessed 24 November 2022

Society for Computers & Law, 'Belgian Market Court refers Preliminary Questions to the CJEU in IAB Europe Cookie Case' (*SCL*, 8 September 2022) <https://www.scl.org/articles/12685-belgian-market-court-refers-preliminary-questions-to-the-cjeu-in-iab-europe-cookie-case> accessed 24 November 2022

Vinay G, 'Get to Know the new Topics API for Privacy Sandbox' (*Chrome*, 2022) <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/> accessed 24 November 2022

WARC, 'Why AI Means the Return of Contextual Targeting' (*WARC*, 18 February 2020) <https://www.warc.com/newsandopinion/news/why-ai-means-the-return-of-contextualtargeting/43241> accessed 28 May 2022

Wilander J, 'CNAME Cloaking and Bounce Tracking Defense' (*WebKi*t, 2020) <https://webkit.org/blog/11338/cname-cloaking-and-bounce-tracking-defense/ > accessed 8 July 2022

Will K and White L, 'Belgian DPA fines IAB Europe over its Consent Framework's GDPR Violations' (*Norton Rose Fulbright Data Protection Report,* February 2022) <https://www.dataprotectionreport.com/2022/02/belgian-dpa-fines-iab-europe-over-its-consent-frameworks-gdpr-violations/> accessed 24 May 2022

Wood M, 'Today's Firefox blocks Third-party Tracking Cookies and Cryptomining By Default' (*Mozilla Blog*, 2019) <https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/> accessed 15 April 2022

Official Reports, Guidance and Opinions

Agencia Espanola Proteccion Datos, 'A Guide on the Use of Cookies' (2019) <https://www.aepd.es/sites/default/files/2020-09/guia-cookies-en.pdf > accessed 8 July 2022

Article 29 Working Party (A29WP), 'Opinion 9/2014 on the Application of Directive 2002/58/EC to device fingerprinting (WP 224)' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf> accessed 10 June 2022

A29WP, 'Opinion 2/2010 on Online Behavioural Advertising (WP 171)' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf > accessed 11 July 2022

A29WP, 'Guidelines on Consent Under Regulation 2016/679' (2017) <https://ec.europa.eu/newsroom/article29/redirection/document/51030 > accessed 8 July 2022

A29WP, 'Opinion 005/2014 on Anonymisation Techniques 216' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 11 July 2022

Belgian DPA, 'Cookies et Autres Traceurs' (2020) <https://www.autoriteprotectiondonnees.be/cookies > accessed 8 July 2022

Centre for Data Ethics and Innovation (CDEI), 'Online targeting: Final Report and Recommendations' (2020) <https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations> accessed 10 May 2022

CDEI, 'Opportunities for PETs' (2021) <https://cdeiuk.github.io/pets-adoption-guide/opportunities> accessed 24 May 2022

CDEI, 'PETs Adoption Repository' (2021) <https://cdeiuk.github.io/pets-adoption-guide/repository> accessed 24 May 2022

Competition and Markets Authority (CMA), 'Online Platforms and Digital Advertising: Market Study Final Report' (2022) <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_LT_TEXT.pdf> accessed 24 May 2022

CMA, 'Appendix X: Assessment of Pro-Competition Interventions to Enable Consumer Choice Over Personalised Advertising, 2020 Online Platforms and Digital Advertising Report' (2021) <https://assets.publishing.service.gov.uk/media/5fe36a658fa8f56af0ac66f2/Appendix_X__-__assessment_of_pro-competition_interventions_to_enable_consumeMAr_choice_over_personalised_advertising_1.7.20.pdf> accessed 24 May 2022

CMA, 'Online Platforms and Digital Advertising Market Study - Appendix G: the role of tracking in digital advertising' (2021) <https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf> accessed 23 May 2022

CMA, 'Appendix L: Potential Approaches to Improving Personal Data Mobility, Online Platforms and Digital Advertising Market Study' (2021) <https://assets.publishing.service.gov.uk/media/5df9efa2ed915d093f742872/Appendix_L_Potential_approaches_to_improving_personal_data_mobility_FINAL.pdf> accessed 23 May 2022

Commission Nationale de l'Informatique et des Libertés (CNIL), 'Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL' (2022) <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ> accessed 24 November 2022

CNIL, 'Cookies: the CNIL fines Google a Total of 150 million euros and Facebook 60 million euros for Non-compliance with French Legislation' (2022) <https://www.cnil.fr/en/cookies-cnil-fines-google-otal-150-million-euros-and-facebook-60-million-euros-non-compliance> accessed 24 May 2022

CNIL, 'Alternatives to Third-Party Cookies: What Consequences Regarding Consent?' (2021) <https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent> accessed 24 May 2022

CNIL, 'Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 24 May 2022

CNIL, 'ISO 27701, an International Standard Addressing Personal Data Protection' (2020) <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection> accessed 24 May 2022

CNIL, 'Deliberation of the Restricted Committee no SAN-2020-012 of 7 December 2020 concerning Google LLC and Google Ireland Limited' (2020) <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_restricted_committee_san-2020-012_of_7_december_2020_concerning_google_llc_and_google_ireland_limited.pdf> accessed 8 July 2022

CNIL, 'Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) et abrogeant la délibération n° 2019-093 du 4 juillet 2019' <https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf> accessed 24 November 2022

Data Protection Commission Ireland, 'Data Protection Commission Statutory Inquiry into Quantcast International Limited' (2019) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-quantcast> accessed 25 May 2022

Data Protection Commission Ireland, 'Guidance Note Cookies and Other Tracking Technologies' (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> accessed 25 May 2022

Datenschutzkonferenz, 'Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1' (2021) < https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf> accessed 8 July 2022

Department for Culture Media and Sport, 'National Data Strategy' (2020) <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy> accessed 26 May 2022

Dutch DPA, 'Websites Must Remain Accessible When Tracking Cookies Are Refused' (Autoriteit Persoonsgegevens, 7 March 2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies> accessed 24 November 2022

European Union Agency for Cybersecurity, 'Privacy and Data Protection By Design – From Policy to Engineering' (2014) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport accessed 25 May 2022

European Commission, 'Commission Proposes High Level Of Privacy Rules For All Electronic Communications and Updates Data Protection Rules For EU Institutions' (2017) <https://ec.europa.eu/commission/presscorner/detail/en/ip_17_16> accessed 19 May 2022

European Commission, 'Digital Single Market – Stronger Privacy Rules For Electronic Communications' (2017) <https://ec.europa.eu/commission/presscorner/detail/en/memo_17_17> accessed 19 May 2022

European Commission, 'What Does Data Protect 'By Design' and 'By Default Mean'?' (2022) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en> accessed 29 May 2022

European Data Protection Board, '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' (2019) <https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 29 May 2022

European Data Protection Supervisor, 'Personal Information Management Systems' (2022) <https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en> accessed 29 May 2022

European Data Protection Supervisor, '10 Misunderstandings Related to Anonymisation' (2021) <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf> accessed 23 June 2022

Garante Per La Protezione Dei Dati Personali, 'Guidelines on the Use of Cookies and Other Tracking Tools' (Official Journal of the Italian Republic 163, 9 July 2021)

Information Commissioners Office (ICO), 'Information Commissioner's Opinion: Data Protection and Privacy Expectations For Online Advertising Proposals' (2021) <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf> accessed 30 May 2022

ICO, 'Update Report Into Adtech and Real Time Bidding' (2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf> accessed 20 May 2022

ICO, 'Guidance on the Use of Cookies and Similar Technologies' (2019) <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf> accessed 21 May 2022

ICO, 'Legitimate Interests' (2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 23 May 2022

ICO, 'Data Protection and Privacy Expectations For Online Advertising Proposals' (2021) <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf> accessed 23 May 2022

ICO, 'Contact Report' (2019) <https://ico.org.uk/media/about-the-ico/disclosure-log/4019410/3-attachment-ic-66641-x3v8-pt5-mins-of-meetings-with-iab-aug-19-jan-20-r.pdf> accessed 29 May 2022

ICO, 'Chapter 2: How Do We Ensure Anonymisation is Effective?' (2021) <https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf> accessed 29 May 2022

ICO, 'Data Protection By Design and Default' (2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> accessed 20 May 2022

Worledge M and Bamford M, 'AdTech Market Research Report' (*ICO*, 2019) <https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf> accessed 23 April 2022

Zerdick T, 'Pseudonymous Data: Processing Personal Data While Mitigating Risks' (*EDPS*, 2021) <https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en > accessed 4 July 2022

Industry Reports

Apple, 'Privacy' (2022) <https://www.apple.com/uk/privacy/features/ > accessed 4 July 2022

Brindra C, 'Building a Privacy-First Future For Web Advertising' (Google 2021) <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/> accessed 20 May 2022

Chromium Blog, 'Building a More Private Web: A Path Towards Making Third Party Cookies Obsolete' (2020) <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html> accessed 15 April 2022

Cluep, 'Music Streaming Service' (2022) <https://cluep.com/cases/entertainment> accessed 11 July 2022

Data and Marketing Association, 'DMA Advice: Using Third Party Data Under the GDPR' (2018) <https://dma.org.uk/uploads/misc/third-party-data-guide-1.0.pdf> accessed 8 July 2022

Dutton S, 'What is FLoC?' (*Google*, 2022) <https://web.dev/floc/#floc-algorithm> accessed 23 May 2022

Eurostat, 'Internet Advertising of Businesses - Statistics on Usage of Ads' (*Eurostat*, December 20108) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads#Ads_that_reach_the_right_audience_with_relevant_and_meaningful_content> accessed 24 November 2022

Google, 'Additional Steps to Safeguard User Privacy' (*Google*, 2019) <https://www.blog.google/products/admanager/additional-steps-safeguard-user-privacy/> accessed 25 May 2022

Google, 'Building a Privacy-First Future For Web Advertising' (*Google*, 2021) <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/> accessed 27 May 2022

Google, 'Get to Know the new Topics API for Privacy Sandbox' (*Google*, 2022) <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/> accessed 29 May 2022

Google, 'The Privacy Sandbox: Topics' (*Google*, 2022) <https://privacysandbox.com/proposals/topics> accessed 29 May 2022

Interactive Advertising Bureau (IAB) Europe, 'State of Data' (*IAB,* 2021) <https://www.iab.com/wp-content/uploads/2021/03/IAB_Ipsos_State_Of_Data_2021-03.pdf> accessed 29 May 2022

IAB UK, 'IAB UK Sets Out Actions to Address ICO's Real-time Bidding Concerns' (*IAB,* 2020) <https://www.iabuk.com/news-article/iab-uk-sets-out-actions-address-icos-real-time-bidding-concerns> accessed 29 May 2022

IAB, 'Transparency and Consent Framework' (*IAB,* 2022) <https://iabeurope.eu/transparency-consent-framework/> accessed 29 May 2022

IAB UK, 'Understanding Cohorts' (*IAB,* 2021) < https://www.iabuk.com/user-identity/understanding-cohorts> accessed 1 July 2022

IAB, 'Annual Report 2021' (*IAB,* 9 March 2022) <https://www.iab.com/wp-content/uploads/2022/02/IAB_Annual_Report_2021_Web_Version.pdf> accessed 20 May 2022

Meta, 'Privacy-enhancing Technologies and Building for the Future' (*Meta,* 2021) <https://www.facebook.com/business/news/building-for-the-future> accessed 29 May 2022

Meta, 'What are Privacy-enhancing Technologies (PETS) and How Will They Apply To Ads?' (*Meta,* 2021) <https://about.fb.com/news/2021/08/privacy-enhancing-technologies-and-ads/> accessed 28 May 2022

Mozilla, 'Privacy Analysis of FloC' (*Mozilla,* 2021) <https://blog.mozilla.org/en/privacy-security/privacy-analysis-of-floc/> accessed 27 May 2022

Privitar, 'K-Anonymity' (*Privitar,* 2017) <https://www.privitar.com/blog/k-anonymity-an-introduction/> accessed 26 May 2022

Profila, 'Profila Zero Knowledge Token Crypto-Asset White Paper' (*Profila,* 2022) <https://profila.com/token/downloads/Profila_ZKT-Whitepaper.pdf> accessed 26 May 2022

Rescorla E and Thompson M, 'Technical Comments on FLoC privacy' (*Mozilla,* 2021) <https://mozilla.github.io/ppa-docs/floc_report.pdf> accessed 25 May 2022

Ryan J, 'Update on GDPR Complaint (RTB ad auctions)' (*Brave*, 2019) <https://brave.com/update-rtb-ad-auction-gdpr/> accessed 28 May 2022