

GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech

Damien Geradin , Theano Karanikioti & Dimitrios Katsifis

To cite this article: Damien Geradin , Theano Karanikioti & Dimitrios Katsifis (2020): GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech, European Competition Journal, DOI: [10.1080/17441056.2020.1848059](https://doi.org/10.1080/17441056.2020.1848059)

To link to this article: <https://doi.org/10.1080/17441056.2020.1848059>



© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 18 Dec 2020.



[Submit your article to this journal](#)



Article views: 131



[View related articles](#)



[View Crossmark data](#)

GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech

Damien Geradin ^{a,b,c,d}, Theano Karanikioti^e and Dimitrios Katsifis^f

^aPartner, Geradin Partners, Brussels, Belgium; ^bProfessor, Competition Law & Economics, Tilburg University, Brussels, Belgium; ^cVisiting Professor, University College London, Faculty of Laws, London, UK; ^dVisiting Professor, University of East Anglia (UEA), Centre for Competition Policy, Norwich, UK; ^eAssociate, Geradin Partners, Brussels, Belgium; ^fSenior Associate, Geradin Partners, Brussels, Belgium

ABSTRACT

This paper argues that while the GDPR has arguably delivered positive outcomes by enhancing the protection afforded to data subjects, it has also had adverse effects on competition by strengthening the position of large online platforms in certain markets. In addition, the GDPR has given large platforms a tool to harm rivals by restricting access to the data they need to compete effectively. The present paper focuses on digital advertising and the ad tech industry, where the GDPR appears to have strengthened Google and Facebook. The purpose of this paper is not to call for the weakening of the GDPR, whose positive impact on users cannot be ignored. While from a policy standpoint regulators should thus maintain or even increase the level of protection offered by this legislation, it is vital that they take steps to mitigate its adverse effects on other dimensions of welfare, such as competition.


ARTICLE HISTORY Received 13 August 2020; Accepted 3 November 2020

KEYWORDS GDPR; privacy; Google; Facebook; online platforms; ad tech; programmatic advertising; online advertising; competition

JEL CODES K21; K42; L41; L86; M37; M38

I. Introduction

The General Data Protection Regulation (“GDPR”) lies at the core of the EU digital privacy legislation,¹ and is arguably one of the world’s most

CONTACT Damien Geradin  dgeradin@geradinpartners.com, dgeradin@edgelegal.eu

¹Regulation (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

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

comprehensive data protection legislations. At a time when personal data are one of the primary inputs for an increasingly large number of economic activities, the GDPR is likely to have a significant impact on businesses operating in the EU, in that it may impose restrictions on the way they conduct their operations, affect their costs, and alter the structure of the markets in which they operate. In an ideal world, the regulatory requirements contained in the GDPR, and the way they are implemented, should deliver the best outcome for society in terms of enhancing the privacy of individuals without undermining other components of social welfare, such as competition, investment and innovation.

However, as this paper will argue, while the GDPR has delivered positive outcomes by enhancing the protection afforded to users of digital services and strengthening the rights of data subjects, it has also had adverse effects on competition by strengthening the position of large online platforms on digital markets, at the very same time that the European Commission (the “Commission”) has expressed concerns about the market power held by these companies,² and is even considering adopting ex ante regulation for so-called digital gatekeepers.³ This is what we understand by “GDPR Myopia”: in its effort to improve the protection of data subjects, the GDPR worsened one of the main problems experienced in digital markets today, which is increased market concentration and reduced contestability. In addition, the GDPR seems to have given large platforms a tool to harm rivals by reducing access to the data they need to run their business.

There is a growing body of economic literature and commentary showing that the costs of implementing the GDPR benefit large online platforms, and that consent-based data collection gives a competitive

such data, and repealing Directive 95/46/EC (“GDPR”), L 119/1GDPR provides for a strong and coherent data protection framework in the EU and aims to ensure the free flow of data. Together with the ePrivacy Directive, (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201), they provide the legal framework to ensure digital privacy for EU citizens. See European Commission, ‘Shaping Europe’s digital future: Digital Privacy’ <<https://ec.europa.eu/digital-single-market/en/online-privacy>>.

²See Commission Communication (n 1) 8:

Some platforms have acquired significant scale, which effectively allows them to act as private gatekeepers to markets, customers and information. We must ensure that the systemic role of certain online platforms and the market power they acquire will not put in danger the fairness and openness of our markets.

³See the Commission’s website on the Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers <<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>>.

advantage to firms offering a range of consumer-facing products compared to smaller market actors. This in turn increases concentration in a number of digital markets where access to data is important, by creating barriers to entry or encouraging market exit.⁴ While it is still early to quantify the impact of the GDPR on competition in these markets, some papers are already providing empirical evidence supporting the view that market concentration has increased.

The present paper uses as a case study the adverse consequences of the GDPR on competition in the so-called ad tech industry, which comprises the various categories of companies that provide online advertising services to advertisers and publishers of online content. Broadly speaking, online advertising may be divided between search advertising (whereby search ads are shown in the search results of a search engine) and display advertising (whereby display ads are shown in the website or app of a publisher). In turn, display advertising may take place on owned and operated properties of large online platforms such as those of Facebook and Google or on the open web, i.e. the myriads of publishers of online content.⁵ Google and Facebook alone capture the lion's share of digital ad revenue.⁶ In the case of advertising on the open web, interactions between publishers and advertisers are typically facilitated by a range of so-called ad tech intermediaries, such as ad servers, ad exchanges/Supply-Side Platforms (“SSPs”) and Demand-Side Platforms (“DSPs”).⁷ These actors help match the demand for ad inventory by advertisers (e.g. Nike, BMW or Nestle) with the supply of such

⁴See, e.g. James David Campbell, Avi Goldfarb and Catherine Tucker, ‘Privacy Regulation and Market Structure’ (2015) 24(1) *Journal of Economics & Management Strategy* 47; Michal S Gal and Oshrit Aviv, ‘The Unintended Competitive Effects of the GDPR’ (2020) *Journal of Competition Law and Economics* <<https://papers.ssrn.com/abstract=3548444>>; Jian Jia, Ginger Zhe Jin and Liad Wagman, ‘The Short-Run Effects of GDPR on Technology Venture Investment’ 8 November 2019 <<https://papers.ssrn.com/abstract=3278912>>; Daniel L Rubinfeld and Michal S Gal, ‘Access Barriers to Big Data’ (2017) 59 *Arizona Law Review* 339 <<https://papers.ssrn.com/abstract=2830586>>; Eline Chivot and Daniel Castro, ‘What the Evidence Shows About the Impact of the GDPR After One Year’ Center for Data Innovation, June 2019 <www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>. See, also, Ivana Kottasová, ‘These Companies Are Getting Killed by GDPR’ (*CNN Business*, 11 May 2018) <<https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>>; ‘How the GDPR Impacts and Suffocates Small and Medium Businesses’ (*i-Scoop*) <www.i-scoop.eu/gdpr/gdpr-small-medium-businesses/>; Kevin Koerner, ‘GDPR – Boosting or Choking Europe’s Data Economy?’ (*DB Research*, 13 June 2018) <www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD000000000470381>; Jedidiah Yeh, ‘GDPR Will Make Big Tech Even Bigger’ (*Forbes*, 26 June 2018) <www.forbes.com/sites/forbestechcouncil/2018/06/26/gdpr-will-make-big-tech-even-bigger/>.

⁵See Competition and Markets Authority, ‘Online Platforms and Digital Advertising’ Market Study Final Report, 1 July 2019, <https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf>; ‘CMA Final Report’, para 5.23 et seq.

⁶Nicole Perrin, ‘Facebook-Google Duopoly Won’t Crack This Year’ (*eMarketer*, 4 November 2019) <www.emarketer.com/content/facebook-google-duopoly-won-t-crack-this-year>.

⁷For an overview of the ad tech supply chain, see CMA Final Report, paras 5.204–5.211.

inventory by publishers (e.g. news publishers, online game developers and other providers of digital content) and/or provide the necessary tools for the display of the ad. The ad tech industry – which is now dominated by “programmatic advertising”,⁸ including “real time bidding” or “RTB” (which allows publishers to monetize their inventory by selling it to buyers through a real-time auction system)⁹ – represents an ideal case study on the effects of the GDPR on competition for two reasons.

First, access to user data plays a central role in the provision of ad tech services. With the rise of programmatic advertising, there has been a shift in online advertising from the context (i.e. the content of the website) to the user. Advertisers place less emphasis on where their advertisement will be shown (aside from brand-safety issues), and instead base their decision according to the specific user that will be exposed to the ad, which explains why access to data about the user (e.g. behavioural, socio-demographic or geographical data) is so critical.¹⁰ Because the GDPR places restrictions on the extent to which data can be collected and processed, it is therefore likely to have a material impact on this industry.

Second, the ad tech industry is characterized by the presence of a particularly strong player, Google, which dominates the ad tech ecosystem (as illustrated in Figure 1).¹¹ In this market, Google competes with a relatively small number of medium-size players, as well as a range of small market actors. While Facebook also offers ad tech tools, it mainly uses its tools to serve ads on its own “walled gardens” (i.e. Facebook, Instagram, etc.), rather than on the open web.

Through acquisitions and organic growth, Google is present at virtually every step of the value chain between advertisers wishing to buy third-party display inventory and publishers.¹² Google offers the

⁸See Allison Schiff, ‘Zenith: Programmatic Display Will Eat The World By 2019’ (*AdExchanger*, 20 November 2017) <www.adexchanger.com/online-advertising/zenith-programmatic-display-will-eat-world-2019/>; Joe Mandese, ‘IAB: Programmatic Now 85% Of All U.S. Digital Advertising’ (*MediaPost*, 24 February 2020) <www.mediapost.com/publications/article/347524/iab-programmatic-now-85-of-all-us-digital-adve.html>.

⁹See Ian Simpson, ‘Real-Time Bidding (RTB) & Programmatic: One and the Same?’ (*The Clearcode Blog*) <<https://clearcode.cc/blog/difference-between-rtb-programmatic/>>; Michael Sweeney, ‘How Real-Time Bidding (RTB) Changed Online Display Advertising’ (*The Clearcode Blog*) <<https://clearcode.cc/blog/real-time-bidding-online-display-advertising/>>.

¹⁰Damien Geradin and Dimitrios Katsifis, ‘An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age’ (2019) 15(1) *European Competition Journal* 61; ‘5 Ways to Use Data-driven Advertising’ (*MarTech Advisor*, 21 May 2018), <www.martechadvisor.com/articles/data-management/5-ways-to-use-datadriven-advertising/>.

¹¹Autorité de la concurrence, ‘Opinion 18-A-03 of 6 March 2018 on Data Processing in the Online Advertising Sector’ para 218.

¹²Notably Google acquired the following ad tech companies: DoubleClick, a company that owned the leading publisher ad server tool DART for Publishers, in 2007; mobile ad network AdMob in 2009; leading DSP Invite Media in 2010; Admeld, leading SSP, in 2011; and ad attribution company

leading ad server for publishers (DoubleClick for Publishers or “DFP”, now part of Google Ad Manager or “GAM”), the leading ad server for advertisers (DoubleClick Campaign Manager, now known as Campaign Manager), two ad networks (AdSense, AdMob) the leading ad exchange/SSP (Google Ad Exchange or “AdX”, now part of GAM) and the leading third-party display ad buying solutions (AdWords, now known as Google Ads, and DoubleClick Bid Manager, now known as Display & Video 360 or “DV360”). As shown in [Figure 1](#), the CMA found Google to have very high market shares (at least 50%) in each step of the ad tech chain.

In this paper, we do not try to show that the GDPR has an adverse impact on publishers, as we already know from the economic literature that restrictions on the use of data on privacy grounds negatively impact publishers’ revenues.¹³ Rather, we show that while it could have been initially thought that the GDPR would have negatively impacted Google’s ability to deliver ad tech services given the enormous amount of data it collects and processes, and thus weaken its dominance in such services, the opposite scenario happened. For reasons that will be explained in this paper, the GDPR has strengthened Google’s market position compared to smaller rivals, which have been less capable of absorbing the implementation costs of the GDPR and coping with the restrictions on the collection and processing of data. Google’s questionable data-related practices, and in particular its “internal data free-for-all”, have also so far been left unchallenged by the Irish Data Protection Authority (“DPA”), while the practices of much smaller actors have been subject to harsh intervention by overly zealous DPAs.

Moreover, as will be demonstrated below, large online platforms are increasingly invoking the GDPR – or privacy concerns more generally – as an excuse to engage in controversial and potentially restrictive

Adometry, in 2014. See Michael Arrington, ‘Breaking: Google Spends \$3.1 Billion to Acquire DoubleClick’ (*Tech Crunch*, 13 April 2007) <<https://techcrunch.com/2007/04/13/google-spends-31-billion-for-doubleclick/>>; Brian Morrissey, ‘Google to Acquire AdMob for \$750 Mil’ (*Adweek*, 9 November 2009) <www.adweek.com/digital/google-acquire-admob-750-mil-100852/>; Erick Schonfeld, ‘Google Confirms Invite Media Acquisition, Brings Bidding to Display Ads’ (*Tech Crunch*, 3 June 2010) <<https://techcrunch.com/2010/06/03/google-confirms-invite-media/>>; Michael Learnmonth, ‘Google Acquires Ad-Optimization Firm Admeld for \$400 Million’ (*AdAge*, 9 June 2011) <<https://adage.com/article/digital/google-acquires-ad-optimization-firm-admeld-400-million/228108/>>; Anthony Ha, ‘Google Acquires Adometry To Bring More Attribution to Google Analytics’ (*Tech Crunch*, 6 May 2014) <<https://techcrunch.com/2014/05/06/google-acquires-adometry/>>.

¹³See, e.g. Avi Goldfarb and Katherine Tucker, ‘Privacy Regulation and Online Advertising’ May 2010 <<https://papers.ssrn.com/abstract=1600259>> (“showing empirically that even moderate privacy regulation reduces the effectiveness of online advertising”); Garrett Johnson, ‘The Impact of Privacy Policy on the Auction Market for Online Display Advertising’ Simon School Working Paper No. FR 13-26, October 2013 <<https://papers.ssrn.com/abstract=2333193>> (“estimating the financial impact of privacy policies on the online display advertising industry and showing that depending on the type of privacy policy in place the revenues of online publishers drop between 3.9 and 38.5%”).

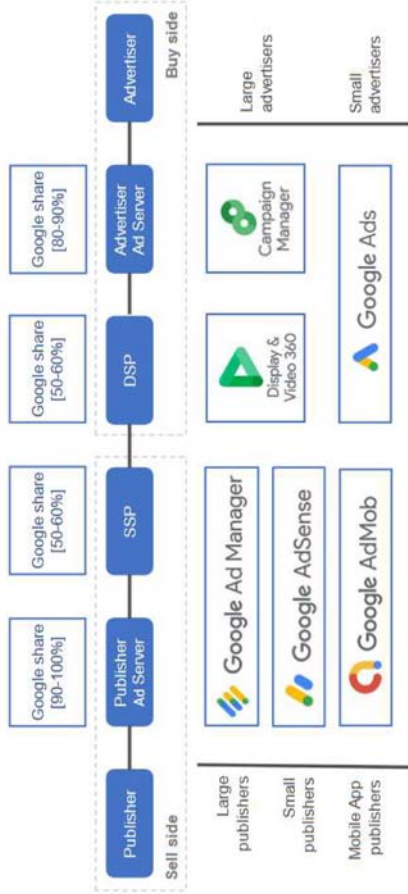


Figure 1. Google's position in the ad intermediation chain. Source: CMA, Online platforms and digital advertising Market study final report (2020)

practices. This could be referred to as the “weaponization” of the GDPR and privacy. We will also see that large online platforms like Google have become *de facto* privacy regulators able to impose their view on privacy to thousands or even millions of businesses that rely on them. On the positive side, it seems that competition enforcers are gradually becoming aware of this worrying trend and seem willing to engage.

Studying the effects of the GDPR on the ad tech market is important for two reasons. First, ad tech companies offer effective tools to advertisers to target the users who are the most likely to be interested in their products and services. Second, online advertising on the open web, which is facilitated by ad tech tools, represents a major – and, in some cases, the only – source of revenues for the tens of thousands of publishers (from large news brands to online game producers to specialist bloggers) that provide valuable content and services to Internet users for free. Both advertisers and publishers, which are central actors of the digital economy, therefore share an interest in the competitive provision of ad tech services, as competition is necessary to maintain low intermediation fees, choice and innovation.

This does not mean that the ad tech industry is the only sector affected by the GDPR. For instance, Johnson and Shriver have shown in a recent paper that the GDPR has increased concentration among the broad category of web technology vendors.¹⁴ Similarly, Peukert et al. have shown that with the introduction of the GDPR, Google has increased its market share in web technology markets.¹⁵ In addition, as many digital products and services rely on access to data – including banking, music and video streaming, online travel agencies, online retailing, healthcare, and even manufacturing – competition could also be affected in these industries. Moreover, our analysis of the adverse effects of the GDPR on competition in the ad tech sector cannot be interpreted as suggesting that the GDPR does not have adverse effects on other desirable outcomes from a welfare standpoint, such as the development of new technologies, the funding of startups, etc., but these effects have either been documented elsewhere¹⁶ or should be the subject of sector-specific analysis.

The purpose of this paper is not to call for the weakening of the GDPR, whose positive impact on users of digital services cannot be ignored. The

¹⁴Garrett Johnson and Scott Shiver, ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’ November 2019 <<https://papers.ssrn.com/abstract=3477686>>.

¹⁵Christian Peukert et al., ‘European Privacy Law and Global Markets for Data’ CEPR, DP 14475, March 2020 <https://cepr.org/active/publications/discussion_papers/dp.php?dpno=14475>.

¹⁶See Jia and others (n 4); Chivot and Castro (n 4).

GDPR has considerably increased privacy awareness among both companies and data subjects across the EU. Moreover, the GDPR has strengthened the rights of data subjects, allowing them to “obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data” and detailed information on *inter alia* the purposes of processing, the categories of personal data being processed, the recipients of any data transfers and whether any automated decision-making, including profiling, is involved.¹⁷ Data subjects avail themselves of the opportunity to exercise their rights and are more than eager to submit complaints if they consider that violations of their rights have occurred.¹⁸

However, the adverse effects of the GDPR on competition and innovation in certain digital industries should not be ignored. From a policy standpoint, the Commission, as well as the authorities that are entrusted with the enforcement of the GDPR, should aim at maintaining or even increasing the level of protection offered by this legislation, while at the same time trying to mitigate its adverse effects on other dimensions of welfare, such as competition (and its positive impact on choice, innovation and investment), which are equally important for both businesses and consumers. It is with this objective in mind that the present paper offers various solutions that could be explored to ensure a better balance between privacy and these other welfare dimensions.

This paper is divided in six parts. **Part II** briefly discusses the principles of the GDPR that are particularly relevant in the context of online advertising, such as the principles of lawfulness and purpose limitation. It also explains the GDPR’s enforcement mechanism, which relies on a decentralized “one-stop-shop” system. **Part III** analyses the unintended consequences of the GDPR, namely the risk that it increases market concentration in the ad tech industry, which was already characterized by a high degree of concentration on some of its segments. The risk of increased market concentration is due to the following reasons. First, compliance costs may create barriers to entry or may cause exit. Second, large online platforms benefit from advertisers’ trust, which therefore prefer to concentrate their ad spending on such platforms.

¹⁷GDPR, Article 15.

¹⁸As of January 2019, more than 95,000 complaints have been submitted by data subjects who believe that their rights under the GDPR have been violated or by organizations mandated by such individuals. European Commission, ‘GDPR in numbers – Infographic’ 25 January 2019 <https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf>.

Third, it is easier for a large platform to obtain end-user consent through their consumer-facing products. Fourth, restrictions on data sharing following from the GDPR give a competitive advantage to large platforms which are able to acquire large volumes of data through their own consumer-facing products. Finally, the GDPR's one-stop-shop mechanism has led to arbitrary enforcement to the benefit of tech companies established in "friendly" jurisdictions.

Part IV shows that, although the GDPR imposes heavy compliance costs and has triggered investigations with significant consequences on small ad tech players, it has done nothing so far to address criticizable practices, such as Google's tactic of combining data it collects across its user-facing services and using it for a wide variety of purposes. We consider that this "internal data free-for-all" is questionable under the GDPR, while at the same time it allows Google to engage in so-called envelopment strategies through cross-data use. **Part V** discusses a worrying trend, which is the use of the GDPR (or privacy concerns more generally) as an excuse by large platforms to engage in anticompetitive conducts. We discuss various examples, namely Google's decision to remove YouTube inventory from AdX, restrict the portability of the DoubleClick ID, as well as phase out third-party cookies on Chrome within a period of two years. Finally, **Part VI** provides recommendations to remedy the GDPR's shortcomings that affect competition.

II. The GDPR in a nutshell

The GDPR came into force on 25 May 2018 with the aims of strengthening the data protection framework within the EU, providing a uniform regulatory data protection environment and ensuring the free movement of data.¹⁹ The GDPR is a flexible instrument: it takes a risk-based approach, based on key principles that must be complied with, and does not prescribe a single way of compliance. Consequently, it can be applied to a range of organizations and situations, allowing for new things to be done in new ways, all while upholding personal data protection.

This Part provides a brief overview of the regulatory principles enshrined in the GDPR which are particularly relevant to the ad

¹⁹GDPR, Recitals 1, 7 and 10 and Article 1(2) and 1(3). The right to the protection of natural persons in relation to the processing of personal data is a fundamental right enshrined in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union.

tech sector (Section A), as well as of the way in which it is enforced (Section B).

A. The principles enshrined in the GDPR

The GDPR centres around seven principles: “lawfulness, fairness and transparency”, “purpose limitation”, “data minimization”, “accuracy”, “storage limitation”, “integrity and confidentiality” and “accountability”.²⁰ Any data collection and processing must comply with the above principles.

In the ad tech context, the obligations imposed on data controllers on the basis of the principles of “lawfulness” (Subsection 1), “purpose limitation” (Subsection 2) and “accountability” (Subsection 3) are particularly worthy of discussion, as their implementation has been subject to considerable debate, leading to legal uncertainty.

1. The principle of lawfulness

The “principle of lawfulness” only allows processing of personal data if one of the six legal bases for processing set out in Article 6(1) of the GDPR is applicable.²¹ In most cases, data processing in the context of online advertising will rely on the data subject’s consent.²² The GDPR

²⁰GDPR, Article 5.

²¹GDPR, Article 6(1):

Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for **compliance with a legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [Emphasis added]

²²While this discussion does not fall within the scope of this paper, it must be noted that there is industry-wide uncertainty as to whether and under which circumstances the “legitimate interests” legal basis can be used when Real-Time Bidding (RTB), a core feature of programmatic advertising, is involved. The prevailing view is that “legitimate interests” might not be an appropriate legal basis in this context for the following reasons. First, RTB protocols often include data fields that constitute special categories of personal data within the meaning of Article 9(1) of the GDPR and for which the explicit consent of the data subject is required. Second, RTB usually involves the use of cookies in order to build profiles of users based on their habits and online behaviour and serve better-targeted ads. According to Article 5(3) of the e-Privacy Directive, the use of cookies requires the positive and unambiguous consent of the data subject. Third, it is argued that even in cases not involving the processing of sensitive personal data or the use of cookies, the balancing exercise required – which consists in proving that processing is not disproportionate, intrusive and unfair – is highly unlikely to tilt in favor of the data controller, given the scale of creation and sharing of personal data profiles involved

requires that consent be “freely given, specific, informed and unambiguous”. It must also be given “by a statement or by a clear affirmative action”.²³ Consequently, scrolling or swiping through a webpage or a similar activity does not satisfy the requirement of a clear and affirmative action.²⁴ Moreover, it is imperative that the data subject be given “the right to withdraw his or her consent at any time” and that withdrawal of consent be “as easy [...] as to give consent”.²⁵

In essence, the GDPR emphasizes the granular nature of consent and sets out various conditions, by requiring keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent and avoiding making consent a condition of a contract or of provision of a service.²⁶ In practice, and in order to help the wider ad tech ecosystem comply with the GDPR, the Interactive Advertising Bureau Europe (“IAB Europe”), in collaboration with the IAB Tech Lab, has developed the Transparency and Consent Framework, a standardized framework publishers may use to collect user consent (with the help of so-called Consent Management Platforms) and transmit it across the supply chain.²⁷

Consent can only be “freely given” when the data subject has a real choice between consenting to the processing of her data or not, does not feel compelled to consent and will not face negative consequences if she does not consent.²⁸ According to the GDPR, when establishing whether consent is freely given, “account shall be taken of whether, inter alia, [...] the provision of a service, is conditional on consent to

in RTB. See ICO, ‘Update report into ad tech and real time bidding’ 20 June 2019, 18 <<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>>; Article 29 Data Protection Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC’ WP 217, 9 April 2014, pages 26 and 30. However, as the GDPR does not prescribe what legal basis has to be used *in abstracto*, the “legitimate interests” legal basis might be relevant for some types of data processing in the context of online advertising (e.g. for a publisher’s processing of personal data when online advertising is a crucial part of a publisher’s business model) but not for other types of processing (e.g. processing by third parties such as ad tech vendors).

²³GDPR, Article 4(11).

²⁴European Data Protection Board, ‘Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.0’ 4 May 2020, para 86.

²⁵GDPR, Article 7(3).

²⁶See ICO, ‘Consent – Is This a Big Change?’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/whats-new/>>.

²⁷For more information, see <<https://iab europe.eu/transparency-consent-framework/>>. IAB launched the Transparency and Consent Framework (TCF) v.1.1 in April 2018. In August 2019 IAB launched TCF v.2.0, which is expected to replace TCF v.1.1 in summer 2020. Note that TCF’s compliance with the GDPR is currently the subject of an investigation by the Belgian DPA. The latter has taken the preliminary view that the TCF could be in breach of the GDPR. See ‘Vista Equity Partners CEO Nabbed For Tax Fraud; IAB Europe’s TCF Disputed In Belgium’ (*AdExchanger*, 19 October 2020) <www.adexchanger.com/ad-exchange-news/monday-10192020/>.

²⁸EDPB (n 24) para 13.

the processing of personal data”.²⁹ Therefore, if consent is bundled with the acceptance of terms and conditions or if the provision of a contract or a service is tied to a request for consent to the processing of personal data that are not necessary for the performance of that contract or service, consent is not deemed to be valid.³⁰

Consent must moreover be “specific” to the purpose for which data are collected. In other words, if the data collected are processed for various purposes, the data subject must consent to each of these purposes. Consent must furthermore be “informed” in the sense that prior to giving consent, the data subject should be informed in an “intelligible and easily accessible form, using clear and plain language” about the terms and purposes of the processing.³¹ The GDPR sets out minimum content requirements for consent to be deemed “informed”, including information on the purpose of each of the processing operations for which consent is sought, the type of data collected and used, and any recipients or categories of recipients of personal data.³²

2. The principle of purpose limitation

The principle of purpose limitation comprises two “building blocks”, requiring first, that personal data are “collected for specified, explicit and legitimate purposes” (purpose specification) and second, that they are “not further processed in a manner that is incompatible with those purposes” (compatible use).³³ In case processing takes place for “a purpose other than that for which the personal data have been collected”, the controller must ascertain whether “processing for another purpose is compatible with the purpose for which the personal data are initially collected”.³⁴

The first building block of the purpose limitation principle requires that, no later than the time when personal data collection occurs, the

²⁹GDPR, Article 7(4).

³⁰EDPB (n 24) para 26.

³¹GDPR, Article 7(2).

³²GDPR, Articles 13 and 14.

³³Article 29 Data Protection Working Party, ‘Opinion 03/2013 on purpose limitation’ WP 203, 2 April 2013, 11.

³⁴GDPR, Article 6(4): for this reason the processor must take into account, *inter alia*:

- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- (d) the possible consequences of the intended further processing for data subjects;
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

purposes of processing must be “clearly revealed, explained or expressed in some intelligible form”.³⁵ It further requires that processing be at all times in accordance with all provisions of applicable data protection law, as well as other applicable laws such as contract or consumer protection laws.³⁶ But most importantly, the purpose specification component of this principle requires that the purpose of the collection “must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied”.³⁷ The degree of detail depends on the personal data involved and the particular context in which they are collected.³⁸

The second building block of the purpose limitation principle, namely compatible use, requires a substantive rather than formal assessment to be carried out by the data controller. Key factors in this assessment are the relationship between the initial purpose and the purpose of further processing, the context in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context, the nature of the data and the impact of the further processing on the data subjects and the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.³⁹

3. The principle of accountability

The principle of accountability requires that the controller implement “appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]”.⁴⁰ Compliance with this principle is burdensome as it requires, *inter alia*, adopting and implementing data protection policies, maintaining documentation of processing activities, recording and, where necessary, reporting data breaches, carrying out Data Protection Impact Assessments and appointing a Data Protection Officer (“DPO”).⁴¹

It must be noted that such compatibility examination is not required if the further processing is based on “the data subject’s consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)”.

³⁵Article 29 Data Protection Working Party, ‘Opinion 03/2013 on purpose limitation’ (n 33) 17.

³⁶*ibid* 19.

³⁷*ibid* 15.

³⁸*ibid* 16.

³⁹*ibid* 21 et seq.

⁴⁰GDPR, Article 24(1).

⁴¹See ICO, ‘Accountability and Governance’ <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/>>.

What is more, the principle of accountability is not limited within the company's walls but extends to ensuring compliance with the GDPR by all organizations that provide data to or receive data from the company.⁴² In other words, when a company receives data from an external data provider it must ensure that the data have been extracted and used in accordance with the GDPR – for example, with the valid consent of the data subject. Similarly, when a company supplies data to third parties, it must also ensure that the receiver complies with the GDPR – for example, that processing takes place only for reasons for which the data subject has given consent or that the rights of the data subject are respected. Compliance with the accountability principle thus entails both direct costs, i.e. the cost of monitoring, screening and auditing of data activities of third parties, and indirect costs in the sense of the lost ability to use any data that are non-compliant. The onus is greater for smaller companies as they have limited resources to comply with the GDPR and monitor compliance by third parties.

B. Enforcement of the GDPR: the one-stop-Shop principle

The GDPR provides for a decentralized implementation system, whereby each Member State “shall provide for one or more independent public authorities to be responsible for monitoring the application of [the GDPR]”.⁴³ Each supervisory authority “shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with [the GDPR]”.⁴⁴

When cross-border processing takes place, the GDPR establishes a one-stop-shop system, according to which “the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority”.⁴⁵ Put simply, the authority of the main establishment of the controller or processor will have the primary responsibility for dealing with and investigating any complaints from data subjects across the EU regarding the

⁴²See Gal and Aviv (n 4) 16.

⁴³GDPR, Article 51(1).

⁴⁴GDPR, Article 55(1).

⁴⁵GDPR, Article 56(1). While under certain circumstances a supervisory authority other than that of the main establishment of the controller or processor may be competent to handle a complaint or to investigate a possible infringement of the GDPR – notably when “the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State” – this can only be done if the lead supervisory authority decides not to handle the case. GDPR, Article 56(2), (3) and (5).

processing of their personal data.⁴⁶ This allows businesses operating in different countries to deal with one DPA – the DPA of their main establishment being the “sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor”.⁴⁷

At the same time, the GDPR establishes a “cooperation and consistency” mechanism that sets out the framework for cooperation, exchange of information and the conduct of joint operations between the lead and other supervisory authorities.⁴⁸ As a result, DPAs other than the lead DPA can play their part in investigations of and decisions against controllers or processors that engage in cross-border processing. The ultimate aim is to reach consensus. Thus, the lead DPA must “submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.”⁴⁹ If other DPAs express relevant and reasoned objections to the draft decision and the lead supervisory authority does not wish to follow the views of these DPAs, it must submit the matter to the consistency mechanism set out in the GDPR, whereby the matter is handled within the European Data Protection Board (“EDPB”).⁵⁰ The EDPB issues a binding decision and the lead supervisory authority must adopt its final decision on the basis of the board’s decision.⁵¹

While the cooperation and consistency mechanism is a positive development in that it allows non-lead DPAs to have an active role in investigations and decisions (even though it may not have yet reached its full potential),⁵² the one-stop-shop principle has arguably granted disproportionate enforcement power to certain DPAs, namely the DPAs of EU Member States in which the large digital platforms, such as Apple, Google, Facebook and Amazon, are established. In the online advertising sector, Ireland – home, amongst others, to Google and Facebook – is at the forefront of GDPR enforcement. Its ability and

⁴⁶Article 29 Data Protection Working Party, ‘Guidelines for Identifying a Controller or Processor’s Lead Supervisory Authority’ WP 244 rev.01, 5 April 2017, page 4.

⁴⁷GDPR, Article 56(6); European Commission, ‘The GDPR: New Opportunities, New Obligations – What Every Business Needs to Know About the EU’s General Data Protection Regulation’ page 2 <https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf>.

⁴⁸GDPR, Chapter VII.

⁴⁹GDPR, Article 60(3).

⁵⁰GDPR, Articles 60(4), 63 and 65. The EDPB comprises “the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives”. GDPR, Article 68(3).

⁵¹GDPR, Article 65.

⁵²Communication from the Commission to the European Parliament and the Council of 24 June 2020, ‘Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation’ COM(2020) 264 final, page 5.

willingness to investigate and sanction these companies therefore determines whether these companies will be able to get away with questionable data processing activities or will be held to account.⁵³ At the same time, controllers and processors that fall under the supervision of zealous DPAs are more likely to be subject to lengthy investigations and hefty fines.

III. GDPR's unintended consequences

The GDPR has altered profoundly the modern privacy landscape, placing the EU at the forefront of data protection in the digital era. Besides affording individuals with greater control over their data, the GDPR has also the potential to strengthen competition in digital markets, particularly by affording data subjects with the right to “data portability”,⁵⁴ that is the right to transfer their data from one controller to another. As the authors of the expert report on Competition Policy for the digital era observe, the right to data portability may facilitate the data subject’s switching between services, in that it helps reduce data-induced lock-in effects (e.g. a user of a social network can switch to a new network without losing her data, which could otherwise discourage her from switching).⁵⁵ The potential of data portability to strengthen competition in digital markets has been widely acknowledged in literature and in various reports,⁵⁶

⁵³Of course, if the Irish DPA investigates, e.g. Facebook, according to the cooperation and consistency mechanism, other DPAs, e.g. the CNIL, will be involved and will input into the final decision. However, the Irish DPA will still be the “lead”.

⁵⁴Article 20 of the GDPR provides that

the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

According to recital 68, the right to data portability was introduced “[t]o further strengthen the [data subject’s] control over his or her own data”.

⁵⁵Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, ‘Competition Policy for the Digital Era, Final report’ (2019) pages 81 and 83 <<https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>>. The authors note, however, that Article 20 of the GDPR has not been designed “as a right to continuous data access or to request data interoperability between two or more services employed by the data subject”. Thus, while it may facilitate switching, it has not been designed “to facilitate multi-homing or the offering of complementary services, which frequently relies on continuous, and potentially real-time, data access”. See *ibid* 81–82. For an overview of how consumer data rights may affect competition, see Organisation for Economic Co-operation and Development, ‘Consumer Data Rights and Competition’ DAF/COMP(2020)1, 29 April 2020 <[https://one.oecd.org/document/DAF/COMP\(2020\)1/en/pdf](https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf)>.

⁵⁶See e.g. Jan Krämer, Pierre Senellart and Alexandre de Streeel, ‘Making Data Portability More Effective for The Digital Economy’ Report for the Centre on Regulation in Europe, (June 2020) pages 55–60 <<https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/>>. For an earlier view, see Inge Graef, Jeroen Verschakelen and Peggy Valcke, ‘Putting the Right to Data Portability into a Competition Law Perspective’ (2013) *Law: The Journal of the Higher School of Economics*,

including the CMA's Final Report on its market study on online platforms and digital advertising.⁵⁷

On the other hand, the GDPR may have negative effects on competition. While there is a growing public concern about the unparalleled amounts of data accumulated by a few digital platforms,⁵⁸ one of the paradoxes of the GDPR is that it may strengthen these large platforms to the detriment of smaller market actors. As pointed out by Gal and Aviv in a recent paper, the GDPR could therefore lead to further market concentration.⁵⁹ While their paper is general in nature, in that it does not focus on one digital market in particular, we will see that Gal and Aviv's concern that the GDPR could increase market concentration applies with full force in the ad tech sector for the reasons discussed hereafter.

First, the implementation of the GDPR and the related compliance costs may create barriers to entry or may cause exit (Subsection 1). Second, large online platforms, such as Google, benefit from advertisers' trust, which therefore tend to concentrate their ad spend on them (Subsection 2). Third, it is easier for large platforms to obtain end-user consent through their numerous consumer-facing products (Subsection 3). Fourth, the GDPR's restrictions in data sharing give a competitive advantage to ad tech players that are able to acquire large troves of data through their consumer-facing products (Subsection 4). Fifth, the one-stop-shop system provided for in the GDPR seems to have led to arbitrary enforcement to the benefit of large platforms located in "friendly" jurisdictions (Subsection 5). Finally, while it is early to quantify the impact of the GDPR on concentration in ad tech markets, we discuss the results of two recent empirical papers addressing this issue (Subsection 6).

Annual Review 53 <<https://ssrn.com/abstract=2416537>>. But see also Gabriel Nicholas and Michael Weinberg, 'Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?' Engelberg Center on Innovation Law & Policy (arguing that the ability of data portability to address competition concerns raised by large social networks is limited).

⁵⁷The CMA explored data portability as a potential data-related remedy in social media and digital advertising markets. See CMA Final Report, 'Appendix W, Assessment of Pro-Competition Interventions in Social Media' <https://assets.publishing.service.gov.uk/media/5efb5fcbd3bf7f769a4e776b/Appendix_W_-_Interventions_in_Social_Media_v.3.pdf>; CMA Final Report, 'Appendix Z, Assessment of Potential Data-Related Interventions in Digital Advertising Markets' <https://assets.publishing.service.gov.uk/media/5efc3f7ae90e075c5aeb9947/Appendix_Z_-_Data_related_interventions_in_digital_advertising_markets.pdf>.

⁵⁸See, for example, Forbrukerrådet, 'New Analysis Shows How Facebook and Google Push Users into Sharing Personal Data' 27 June 2018 <www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/>; Oscar Gonzalez, 'Here's How Much Information Facebook and Google Have on You' (*Inverse*, 27 March 2018) <www.inverse.com/article/42883-facebook-google-user-info>.

⁵⁹Gal and Aviv (n 4).

1. Implementation costs create barriers to entry or may even cause exit

Compliance with the GDPR is a particularly onerous task for small and medium-size ad tech providers, as it places a particularly heavy burden on their resources. They must *inter alia* put in place consent gathering mechanisms (for example, have a Consent Management Platform), provide detailed information regarding their data processing activities, implement technical and organizational measures to ensure compliance with the GDPR, monitor and document GDPR compliance (e.g. by keeping detailed records of their processing activities), carry out Data Protection Impact Assessments and have a designated DPO.⁶⁰ Companies with data presence in the EU have been required to spend millions to comply with the GDPR.⁶¹

The human resources and capital costs involved in ensuring compliance with the GDPR disproportionately burden small and medium-size vendors – which are limited in terms of both financial resources and personnel. While a big company has dozens if not hundreds of experts working on GDPR compliance,⁶² most ad tech companies do not have the lawyers, data experts and programmers necessary to make compliance with the GDPR a smooth and effective process.⁶³ Additionally, compliance with the burdensome requirements of the GDPR, such as adopting technical and organizational measures and monitoring and documenting data flows, exhibits economies of scale and scope, which tend to create a competitive advantage for large organizations.

In a sector with high concentration in some segments,⁶⁴ that has already suffered from a large drop in investment in recent years,⁶⁵ and

⁶⁰See, for example, GDPR, Articles 12, 13, 24, 30, 35 and 37.

⁶¹Chivot and Castro (n 4).

⁶²For example, Microsoft had 1600 engineers working on GDPR compliance since its enactment in 2016. Julie Brill, 'Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data' (*Microsoft Blog*, 21 May 2018) <<https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/>>.

⁶³Kottasová (n 4).

⁶⁴Concentration is particularly high at the publisher ad server level where Google is likely to have above 90% market share. Concentration is also significant at the DSP and SSP levels, where Google has market share of 50–60%. See CMA Final Report, para 5.213.

⁶⁵See Madhumita Murgia, 'Adtech Funding Drops in Face of Facebook-Google duopoly' *Financial Times* (3 January 2017) <www.ft.com/content/c4c358ca-c6af-11e6-8f29-9445cac8966f>; Ronan Shields, 'Investment in Ad Tech Grows Increasingly Scarce, With Forrester Predicting a 75% Drop in Venture Capital' *Adweek* (7 November 2018) <www.adweek.com/programmatic/investment-in-ad-tech-grows-increasingly-scarce-with-forrester-predicting-a-75-drop-in-venture-capital/>; Nick Chasinov, 'How Ad Tech Entrepreneurs Can Combat Google and Facebook's Dominance' (22 January 2019) <www.entrepreneur.com/article/326591>; Ricardo Bilton, 'Venture Capital Gives Ad Tech the Cold Shoulder' *Digiday* (29 October 2015) <<https://digiday.com/media/venture-capital-gives-ad-tech-cold-shoulder/>>; Megan Rose Dickey, 'Advertising Giants Leave Little Room for Adtech Startups, and VCs are Noticing' *Tech Crunch* (14 June 2017) <<https://techcrunch.com/2017/06/13/advertising-giants-leave-little-room>>

has seen several ad tech players struggling or even exiting the market,⁶⁶ the additional costs generated by the GDPR could further precipitate market concentration. While a large company has no difficulty to absorb the compliance costs of GDPR, the situation may be different for market players that are already struggling to make money and attract investment.⁶⁷ The anticipated compliance costs of the GDPR could also delay or discourage market entry by making it more costly and risky, hence depriving advertisers and publishers of new and innovative tools, as well as the competitive pressure they would bring on Google.

This imbalance is further aggravated by the uncertainty surrounding the GDPR. For instance, immediately after the entry into force of the GDPR, numerous independent ad exchanges and other vendors in the ad tech ecosystem saw their ad demand volumes shrink dramatically between 20 and 40%.⁶⁸ The text of the GDPR left open a number of questions and authorities had not clarified fundamental issues, such as what legal basis is appropriate in the context of online advertising, how to

[for-adtech-startups-and-vcs-are-noticing/](#)>; Claire Ballentine, 'Google-Facebook Dominance Hurts Ad Tech Firms, Speeding Consolidation' *The New York Times* (12 August 2018) <www.nytimes.com/2018/08/12/technology/google-facebook-dominance-hurts-ad-tech-firms-speeding-consolidation.html>.

⁶⁶The challenges faced by ad tech companies such as Sizmek, Rocket Fuel, The Rubicon Project, OpenX and Verizon Media have been widely reported in the press. Sizmek filed for bankruptcy in 2019 and parts of its business were eventually acquired by Amazon. See Nico Neumann, 'The Sizmek Saga Underscores Ad Tech's Flaws and Market Weaknesses' (*AdExchanger*, 4 April 2019) <www.adexchanger.com/data-driven-thinking/the-sizmek-saga-underscores-ad-techs-flaws-and-market-weaknesses/>. In 2018 Verizon announced it would write down Verizon Media (previously known as Oath, a company formed after the merger of AOL and Yahoo) by \$4.6 billion, cutting its goodwill valuation to half. See 'Verizon Media Group Revenue Falls; Finance Brands Spend More on Social' (*AdExchanger*, 24 April 2019) <<https://adexchanger.com/ad-exchange-news/wednesday-04242019/>>; Simon Owens, 'Verizon Made a \$9 Billion Bet on Digital Media. Here's Why It Failed' (*Intelligencer*, 13 December 2018) <<http://nymag.com/intelligencer/2018/12/why-verizons-usd9-billion-bet-on-digital-content-failed.html>>. In December 2018 OpenX laid off 100 employees and announced it would shut down its ad server in 2019. See Sarah Sluis, 'OpenX Lays off 100 Employees and Pivots to Video' (*AdExchanger*, 18 December 2018) <<https://adexchanger.com/platforms/openx-lays-off-100-employees-and-pivots-to-video/>>. In 2018 The Rubicon Project reported a 57% drop in quarterly revenues and fired 100 employees. See Ronan Shields, 'Rubicon Project axes 100 staff as it counts the cost of killing its buy-side fees as quarterly revenue drops 57%' (*The Drum*, 14 March 2018) <www.thedrum.com/news/2018/03/14/rubicon-project-axes-100-staff-it-counts-the-cost-killing-its-buy-side-fees>. In 2017 Rocket Fuel was acquired at a fraction of its initial valuation. See Mike Shields, 'Ad Tech Company Rocket Fuel Sold for a Fraction of Its Peak \$2 Billion Valuation, and It Marks the End of an Era' (*Business Insider*, 18 July 2017) <www.businessinsider.com/rocket-fuels-sale-to-sizmek-marks-the-end-of-an-era-in-ad-tech-2017-7>. See also Archie Sharma, 'At-Tech Exits' *OpenX*, 19 July 2016 <www.openx.com/uk_en/resources/blog/62042/>.

⁶⁷See Hannah Kuchler, 'US Small Businesses Drop EU Customers Over New Data Rule' *Financial Times* (24 May 2018) ('Tech start-ups, video games makers and advertising technology businesses are among several small US companies pulling out of the EU rather than risk falling foul of the new General Data Protection Regulation, which comes into force on Friday').

⁶⁸Jessica Davies, 'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers' (*Digiday*, 4 June 2018) <<https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/>>.

obtain user consent or who can be considered as a controller or processor in the complex online advertising ecosystem, which ultimately benefitted Google as advertisers decided to fly to safety. Regulatory uncertainty may further penalize small and medium-size ad tech vendors when DPAs are not responsive to the need for clarity on some opaque areas of the GDPR.⁶⁹

However, the shift in demand towards Google products was not only the result of advertisers trusting that it is better placed to ensure compliance. It was also heavily incited by Google's position in the wake of the GDPR. Google interpreted the GDPR as requiring consent as the lawful basis for data processing activities in the ad tech ecosystem and it thus required advertisers using Google's ad tech products to only buy through its own ad tech products for which it could guarantee that it has valid user consent.⁷⁰

2. Rightly or wrongly, large platforms benefit from advertiser trust

The fear of liability and the large fines that can be imposed on the basis of the GDPR have led advertisers to concentrate their ad spending on the largest players, as they trust that they are compliant with its regulatory requirements.⁷¹ Since the entry into force of the GDPR, Google and Facebook's position in online advertising has been further strengthened.⁷² Trust in these players follows from three assumptions. First, that such companies have the resources to comply with the GDPR. Second, that companies holding vast amounts of data will be closely monitored by regulatory authorities and thus will be compliant. Third, that such companies will be more careful with users' personal data as they have more to lose in case of non-compliance. For reasons that will be discussed below, the second and third of these assumptions are not necessarily true in practice.

⁶⁹See, for example, Olivier Magnan-Saurin, 'La CNIL, nous a touer' (*Medium*, 5 February 2020) <<https://medium.com/@olivier.magnan.saurin/la-cnil-nous-a-tuer-6b982601eeec>>.

⁷⁰Davies (n 68).

⁷¹Nick Kostov and Sam Schechner, 'GDPR Has Been a Boon for Google and Facebook' *The Wall Street Journal* (17 June 2019) <www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219>. In fact, the trust that large players are GDPR compliant is ironic, considering the numerous investigations into GDPR violations by Google and Facebook which have affected millions of users, in particular with regards to the lack of transparency, inadequate information and lack of valid consent regarding the processing of users' personal data for advertising purposes.

⁷²Mark Scott, Laurens Cerulus and Laura Kayali, 'Six Months in, Europe's Privacy Revolution Favors Google, Facebook' (*Politico*, 23 November 2018) <www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/>; Cale Guthrie Weissman, 'One Year in, GDPR Seems to have Helped Google & Facebook' (*FastCompany*, 17 May 2019) <www.fastcompany.com/90351655/gdpr-helps-google-and-facebook-grow-uk-market-share-in-2019>.

3. It is easier for large platforms to obtain user consent

The strengthened data protection framework set out by the GDPR has made it harder for small and medium-size players to collect and use data. Privacy-aware consumers might be hesitant to give consent to the processing of their data to market players they do not necessarily know – especially when seeing that their data might be used for a variety of purposes, such as advertising and measurement.

On the contrary, the leading position of large platforms like Google and Facebook in consumer-facing services perceived as “must-have” allows them to easily obtain users’ consent to the collection of personal data.⁷³ For instance, billions of people are dependent on Google’s services, such as Gmail, Search, YouTube and the likes, which they consider an indispensable part of their personal or even professional life – a part that they do not consider letting go. Evidence shows that about half of all Internet users and about two thirds of users aged 14–29 classify Google Search as “absolutely essential”.⁷⁴ While some users are unhappy about the way consent is sought – for example, that it is often a take-it-or-leave-it approach or that it is too cumbersome to read all relevant notices – the perceived essential nature of the services provided by Google, combined with the lack of credible alternatives, outweigh their concerns about their data being collected.⁷⁵

Moreover, in the case of logged-in environments (e.g. Android or Facebook), user consent needs only be obtained once, when the user is required to accept the terms and conditions in order to use the service. In contrast, outside the “walled gardens”, user consent must be obtained each time a user visits a publisher or advertiser’s website. Users faced with repetitive requests to consent to the collection and processing of their data are more likely to refuse granting the required consent. Additionally, the fragmentation of consent in the open web hampers the business of ad tech vendors which must ensure that user consent has been obtained in various touchpoints, in order to be able to provide their services without infringing data protection laws.

4. Limiting the ability to share data also helps large platforms

The GDPR has considerably limited data sharing between companies, by requiring free, specific, informed and unambiguous consent for data

⁷³Jon Markman, ‘GDPR is Great News for Google and Facebook, Really’ (*Forbes*, 22 May 2018) <www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/#fac153448f63>.

⁷⁴Anne Niedermann, ‘Freely-Given and Informed Consent? The User’s Perspective’ Presentation of the Results of the Allensbach Survey, DLD Europe, 9 September 2019.

⁷⁵*ibid.*

transfers, as well as by requiring the data supplier to monitor and follow the data transferred – as the data collector must ensure that data are only used in accordance with the data subject’s consent and that the data subject can exercise its rights (such as the right to erasure) – and by imposing liability in cases of violation of the GDPR.⁷⁶ Data sharing is therefore risky and many data holders may decide to take the extreme measure of refusing to share their data with smaller ad tech players as they may not trust their ability to comply with the GDPR. This is problematic as these smaller actors are generally the ones that would benefit the most from accessing third-party data.

In contrast, there is limited incremental value from data transfers for large market actors holding massive amounts of data, as they already capture the data they need within their ecosystem. At the same time, when entities decide to engage in data sharing, they prefer to deal with large market actors, whom they trust to comply with the GDPR. This may create a competitive advantage for large, well-known players, as smaller suppliers or new entrants will often be overlooked. The limitations to data sharing have therefore widened the gap between Google and Facebook and small players, making the former much more attractive to advertisers who value the amount of data they possess.

5. The one-stop-shop mechanism benefits companies located in friendly jurisdictions

The one-stop-shop system envisaged in the GDPR means that companies have to deal with only one DPA – the supervisory authority of their single or main establishment. It moreover entails that investigations into the likes of Google or Facebook will be typically controlled by the same few authorities, where the largest tech firms are established in the EU. This creates serious bottlenecks which, coupled with the reluctance of certain DPAs to intervene, results in tech giants escaping close monitoring and liability, despite regularly engaging in dubious practices.⁷⁷

⁷⁶Consider, for example, that the controller must, at the time when personal data is obtained from the data subject, inform the data subject of any recipients or categories of recipients of the personal data (GDPR, Article 13(1)(c)). Additionally, if the data subject exercises his or her right of access, the controller must be able to inform him or her of the recipients or categories of recipient to whom the data personal data have been or will be disclosed (GDPR, Article 15(1)(c)) and if the data subject wants to exercise his or her right to erasure, the controller must inform other controllers which are processing such data (GDPR, Article 17(2)).

⁷⁷Nicholas Vinocur, “We Have a Huge Problem”: European Tech Regulator Despairs over Lack of Enforcement’ (*Politico*, 27 December 2019) <www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605>.

In recent years, an upheaval against the practices of Big Tech has been observed. Campaigns have been organized across the EU by civil rights organizations urging authorities to take the risks of RTB seriously.⁷⁸ Commentators have strongly criticized Google's data practices, in particular Google tracking users' location or granting third parties with access to (often sensitive) user data.⁷⁹ Google's practices have also led to numerous complaints submitted to DPAs across Europe since the entry into force of the GDPR,⁸⁰ which claim, *inter alia*, that Google violates the purpose limitation principle with its "internal data free-for-all" practices and by tracking users' location.⁸¹

⁷⁸See, for example, Eva Simon, 'Prevent the Online Ad Industry from Misusing Your Data – Join the #Stop-SpyingOnUs Campaign' (*Liberties EU*, 4 June 2019) <www.liberties.eu/en/campaigns/stop-spying-on-us-fix-ad-tech-campaign/307>; Fix AdTech, 'A Campaign to Make Online Advertising Work Better and Safer' <<https://fixad.tech/about/>>.

⁷⁹See, for example, Laura Hautala and Richard Nieva, 'Google's Gmail Controversy is Everything People Hate About Silicon Valley' (*CNET*, 3 July 2018) <www.cnet.com/news/googles-gmail-controversy-is-everything-wrong-with-silicon-valley/>; Sarah McDermott, 'Android Phones Still Track You When Location Services are Off' (*CNET*, 21 November 2017) <www.cnet.com/news/android-phones-still-track-you-when-location-services-are-off/>; Ryan Nakashima, 'AP Exclusive: Google Tracks Your Movements, Like It or Not' (14 August 2018) <<https://apnews.com/828aefab64d4411bac257a07c1af0ecb>>; Natasha Lomas, 'Mental Health Websites in Europe Found Sharing User Data for Ads' (*Tech Crunch*, 4 September 2019) <<https://techcrunch.com/2019/09/04/mental-health-websites-in-europe-found-sharing-user-data-for-ads/>>; DJ Pangburn, 'How – and Why – Apple, Google, and Facebook Follow You Around in Real Life' (*Fast Company*, 22 December 2017) <www.fastcompany.com/40477441/facebook-google-apple-know-where-you-are>.

⁸⁰Under the GDPR, each data subject can decide to lodge a complaint with the supervisory authority in the Member State of its habitual residence, place of work or place of the alleged infringement (GDPR, Article 77). However, when cross-border processing takes place, the role of the lead supervisory authority is central. DPAs other than the DPA of the main or the single establishment of the controller or processor that receive the complaints shall notify the lead supervisory authority about such complaints, which then decides whether it will handle the case or delegate it (GDPR, Article 56). When the lead authority decides to handle the case, it will have the leading role in the investigations, being the main point of contact for the company and drafting the decision which will be submitted to the supervisory authorities concerned. In other words, even though complaints against e.g. Google and Facebook, can be submitted (and have been submitted) to DPAs across the EU, ultimately it is Ireland that has control over these companies (GDPR, Article 60).

⁸¹For example, in November 2018, seven consumer organizations filed complaints against Google with the DPAs in Norway, the Netherlands, Greece, the Czech Republic, Slovenia, Poland and Sweden, notifying of breaches of the GDPR in relation to how Google tracks – and monetizes through online advertising – its users' location. Moreover, in September 2018 Dr Johnny Ryan of Brave, Jim Killock of the Open Rights Group and Michael Veale of University College London filed simultaneous complaints to the UK and the Irish DPAs against Google and other ad tech firms notifying regulators of a massive and ongoing data breach in the context of behavioural advertising that affects virtually every user on the internet. See Privacy International, 'Regulatory Complaint Against Google and Other "Ad Tech" Companies Under Europe's GDPR by Johnny Ryan, Jim Killock, and Michael Veale' (12 September 2018) <<https://privacyinternational.org/examples/2983/regulatory-complaint-against-google-and-other-ad-tech-companies-under-europes-gdpr>>. In January 2019, a new complaint was filed to the Polish DPA, accompanied by new evidence on the massive leakage of special categories of user data that takes place in the RTB process. See Privacy International, 'Panoptikon Foundation Files Complaint Against Google and Other "Ad Tech" Companies with the Polish Data Protection Authority' (28 January 2019) <<https://privacyinternational.org/examples/2982/panoptikon-foundation-files-complaint-against-google-and-other-ad-tech-companies>>. In May 2019, GDPR complaints regarding RTB were filed with DPAs in Spain, the Netherlands, Belgium and Luxembourg, bringing the total of complaints on this matter to seven to mark one year of the GDPR. See Privacy International, 'Ad Tech GDPR Complaint is Extended to Four More European Regulators' (20 May

As a result of the one-stop-shop principle, Google falls under the supervision of the Irish Data Protection Commission (“DPC”). However, the DPC, which oversees, among other giants, Google, Facebook, Microsoft and Twitter, has long been criticized for catering to the very companies it is supposed to oversee, by not actively seeking to monitor compliance, undertake investigations or impose fines for GDPR violations.⁸² There is a practical reason behind that; the case load of the DPC is horrifying. Since 25 May 2018, the DPC has received more than 8.800 complaints under the GDPR, has had more than 9.600 data security breaches notified to it and it has received 593 cross-border processing complaints via the GDPR’s one-stop-shop mechanism.⁸³ With a decelerating budget⁸⁴ and a staff limited to 140 regulatory lawyers, investigators and technologists,⁸⁵ it is not surprising that the DPC is overwhelmed.

However, it is also a matter of willingness to enforce the GDPR and punish violators. In fact, besides being completely overwhelmed, one possible reason which may explain the passive stance of the DPC relates to the strong economic dependency that exists between Ireland and the tech giants. This dependency may disincentivize rigorous GDPR enforcement against these companies, raising the question of whether Ireland is best-suited for regulating Big Tech.⁸⁶ It is indeed surprising that despite the numerous complaints against Google and Facebook, the Irish DPA only opened its first investigation into Google one year after the entry into

2019) <<https://privacyinternational.org/examples/2992/ad-tech-gdpr-complaint-extended-four-more-european-regulators>>. In March 2020, Brave filed another complaint against Google with the Irish DPC arguing that Google’s internal data “free-for-all” practices are in violation of the GDPR. At the same time, Brave wrote to the European Commission, the Bundeskartellamt, the UK Competition & Markets Authority, the French Autorité de la concurrence and the Irish Competition and Consumer Protection Commission to make them aware of this purpose limitation complaint. See Johnny Ryan, ‘Formal GDPR Complaint Against Google’s Internal Data Free-for-All’ (16 March 2020) <<https://brave.com/google-internal-data-free-for-all/>>.

⁸²Nicholas Vinocur, ‘How One Country Blocks the World on Data Privacy’ (*Politico*, 24 April 2019) <www.politico.com/story/2019/04/24/ireland-data-privacy-1270123>.

⁸³See Irish Data Protection Commission, ‘Annual Report: 25 May–31 December 2018’ <www.dataprotection.ie/sites/default/files/uploads/2019-02/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf>; Irish Data Protection Commission, ‘Annual Report: 1 January–31 December 2019’ <www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf>.

⁸⁴The Irish DPA’s budget stands at €16.9 million and is the sixth among DPAs in Europe. Despite seeking a budget increase of €5.9 million, it only got a third of that amount. The chair of the Irish DPC said she was “frustrated by the budget restrictions” and graded Ireland’s performance as an “A for effort” but a “C-plus/B-minus in terms of output”. See Adam Satariano, ‘Europe’s Privacy Law Hasn’t Shown Its Teeth, Frustrating Advocates’ *The New York Times* (27 April 2020) <www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html>.

⁸⁵In fact, Google and Facebook’s lead authority only has 21 specialist tech investigators. See Brave, ‘Europe’s Governments Are Failing the GDPR: Brave’s 2020 Report on the Enforcement Capacity of Data Protection Authorities’ (April 2020) page 7 <<https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf>>.

⁸⁶Vinocur, “We Have a Huge Problem”: European’ (n 77).

force of the GDPR.⁸⁷ It is also surprising that Ireland continues taking a softer approach in its investigations, by avoiding on-site inspections and sanctions, opting for negotiations with the companies instead.⁸⁸

At the same time, DPAs in other EU Member States – and particularly in France – have zealously enforced the GDPR. The CNIL did not waste any time and already issued formal warnings on ad tech companies a month after the entry into force of the GDPR, forcing companies to devote months of work both on GDPR compliance and on liaising with their supervisory authority.⁸⁹ For instance, in July 2018, the CNIL issued formal warnings to two small local ad tech companies, Fidzup and Teemo, stating that their data processing for targeted advertising did not rely on valid consent. First, the CNIL alleged the companies did not provide data subjects with the information required under the GDPR, as such information was provided only after users' geolocation data and advertising ID were already collected. Moreover, Fidzup's privacy policy was found to be incomplete as it did not mention targeted advertising or the details of the data controller. In addition, the CNIL claimed consent to processing by Fidzup and Teemo was neither freely given nor specific, as consent for the deployment of their tool (the "SDK-tool") and the processing of geolocation data for targeted advertising was bundled with consent obtained for other data processing activities of the app provider. The CNIL also found that Teemo was keeping geolocation data for longer than necessary.⁹⁰

Fidzup was a successful enforcement story according to the CNIL. After months of work (and after having its initial proposal rejected by the CNIL), Fidzup managed to get the green light from the CNIL with regards to its processing activities, after having found a solution that was acceptable both by the CNIL and Fidzup's business partners.⁹¹ But in reality, it drove Fidzup out of business. According to its founder, the

⁸⁷Padraic Halpin, 'Irish Regulator Opens First Privacy Probe into Google' (*Reuters*, 22 May 2019) <www.reuters.com/article/google-dataprotection/irish-regulator-opens-first-privacy-probe-into-google>.

⁸⁸For example, despite numerous investigations into Facebook's practices, the Irish DPA has not sent any regulatory agents to Facebook's Dublin headquarters, choosing to rely on "updates" by Facebook that reveal little more than the company's public statements. See Vinocur, 'How One Country Blocks the World on Data Privacy' (n 82).

⁸⁹CNIL, 'Applications mobiles: mises en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire' (19 July 2018) <www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire>.

⁹⁰*ibid.*

⁹¹CNIL, 'Applications mobiles: clôture des mises en demeure à l'encontre des sociétés FIDZUP et SINGLE-SPOT' (29 November 2018) <www.cnil.fr/fr/applications-mobiles-cloture-des-mises-en-demeure-lencontre-des-societes-fidzup-et-singlespot>. See also 'GDPR: Fidzup, an Exemplary Case' (7 March 2019) <www.altavia-group.com/en/21st-century-shopper/gdpr-fidzup-an-exemplary-case/>.

lack of effective cooperation by CNIL (which prolonged the duration of the proceedings), combined with the fact that the CNIL made the procedures public (causing distrust among Fidzup’s customers), effectively killed his promising start-up.⁹²

But for the one-stop-shop system, the CNIL could have better used its resources looking at the questionable practices of Google (as discussed below), hence ensuring a more effective and unbiased enforcement of the GDPR in Europe, than going after small ad tech vendors whose practices, even if problematic, could only produce limited effects given their size. In this respect, the CNIL has made it clear that it is more than willing to investigate Google for breaches of the GDPR. In January 2019, the CNIL imposed a € 50 million fine on Google for lack of transparency, inadequate information and lack of valid consent regarding ads personalization, but it had jurisdiction to do so only because the “one-stop-shop mechanism” was not applicable to the particular investigation, as Google could not yet be considered to have a main establishment in the EU.⁹³

Finally, DPAs across Europe have endorsed diverse interpretations of the GDPR, with some – particularly the CNIL – adopting a stricter approach than other DPAs. For example, the CNIL has interpreted the requirement of *freely given consent* under the GDPR when the use of cookies or other trackers is involved as necessitating data collectors to afford data subjects

the ability to express refusal as easily as indeed the counterpart of the ability to express free consent. Therefore, in order not to affect the user’s freedom of choice, the mechanism for expressing consent should be presented at the same level and in the same technical manner as the mechanism for expressing refusal.⁹⁴

Put simply, the user must have a clear choice between to “accept” and “refuse” or to “consent” and to “not consent”. The CNIL’s interpretation goes beyond the interpretation adopted by the Irish DPC, which requires data collectors using an “accept” button to give equal prominence to a

⁹²Magnan-Saurin (n 69).

⁹³CNIL, ‘The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC’ (21 January 2019) <www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

⁹⁴CNIL, ‘Draft Recommendation on the Practical Procedures for Collecting the Consent Provided for in Article 82 of the French Data Protection Act, Concerning Operations of Storing or Gaining Access to Information in the Terminal Equipment of a User (Recommendation “Cookies and other trackers”)’ (14 January 2020) para 35 <www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf>.

“reject” button *or* to a “manage cookies” button, bringing data subjects to another layer of information in order to allow them to manage cookies, by cookie type and purpose. What matters for the DPC is that the user is not nudged into accepting cookies over rejecting them.⁹⁵

As a result, data subjects are more likely to reject the use of cookies by companies regulated by the CNIL (as an explicit “reject button” must be available) than companies regulated by the DPAs adopting an approach similar to that of the Irish DPC (as data subjects might only have the opportunity to reject cookies at the second information layer). Given the importance of cookies in the ad tech ecosystem, the approach adopted by the CNIL places ad tech actors in a competitive disadvantage compared to their counterparts regulated by other DPAs. If they comply with the CNIL’s stringent consent requirements, they might suffer revenue losses as a result of their reduced ability to track users. If they do not comply, they risk investigations and fines for practices that more lenient DPAs might consider compliant with the GDPR.⁹⁶ Even though the GDPR was aimed at levelling the playing field across the EU, data controllers remain subject to different consent requirements depending on their place of establishment.

6. Has the GDPR increased market concentration? Some empirical data

For the reasons discussed in the preceding sections, the GDPR appears to benefit Google, a player that is already dominating the ad tech markets. One challenging issue, however, is to quantify the impact of the GDPR on market concentration in the advertising sector. A couple of recent empirical studies suggest that the short-run impact of the GDPR was indeed increased market concentration. For instance, in their paper analysing the impact of the GDPR on web technology vendors, Johnson and Shiver show that the highest impact on such vendors both in terms of market shares and concentration ratio was felt in the advertising category.⁹⁷ Similarly, in their paper analysing the impact of the GDPR on

⁹⁵Irish Data Protection Commission, ‘Guidance Note: Cookies and Other Tracking Technologies’ (April 2020) page 9 <www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf>.

⁹⁶The GDPR has granted DPAs across Europe significant enforcement powers, including the power to impose fines up to €20 million or 4% of a company’s global annual turnover, whichever higher. Given the grave economic implications these fines can have, especially for small and medium-size companies, it would be responsible for DPAs to conduct an impact assessment prior to adopting any recommendations or guidelines interpreting the GDPR and setting out their approach to GDPR enforcement. In this regard, they should consider the broader economic consequences of any interpretation of data protection rules, as well as any effects on competition in the online advertising market.

⁹⁷See Johnson and Shiver (n 14).

web technology services, Peukert et al. show that “[w]ith the introduction of GDPR, the dominant firm in many markets for web technologies, Google, increases its market share whereas all other firms that supply web technology either do not see a change in market share or suffer losses”.⁹⁸ They also find that among the service categories analysed in their paper, Google’s largest market share increases where in the analytics market (7.2%) and the advertising market (4.5%).⁹⁹ These papers thus suggest that the GDPR does have an effect on market concentration and competition in the advertising field.

IV. The GDPR may not prevent criticizable data accumulation and processing practices

As we have seen in **Part III**, the GDPR imposes heavy compliance costs on small and medium-size ad tech vendors and the various restrictions it contains tend to favour large digital platforms like Google, hence increasing market concentration. That problem is accentuated by the one-stop-shop principle with the companies engaged in the largest data collection and processing operations being generally located in “friendly” jurisdictions, such as Ireland, where the level of oversight has so far been inadequate.

In this Part, we analyse what we perceive as a key shortcoming of the way the GDPR has been interpreted so far, which is that while DPAs have imposed limits on *external* data transfers (data transfers between different companies), they have not done anything to limit any *internal* data sharing within various units of large digital platforms. This inadequate enforcement of GDPR’s purpose limitation principle not only constitutes a major threat to user privacy, but also places large, dominant platforms, which can combine consent requirements for all their data uses, in a competitive advantage.

For example, Facebook’s data policy allows it to combine extensive user data it collects directly from its user-facing products such as Facebook, Instagram, WhatsApp and Messenger,¹⁰⁰ as well as from its Business Tools¹⁰¹ – including Facebook’s social plugins, Facebook

⁹⁸See Peukert et al. (n 15) 2.

⁹⁹ibid 20.

¹⁰⁰For an overview of the Facebook Products see ‘What are the Facebook Products?’ *Facebook Help Centre* <www.facebook.com/help/1561485474074139>.

¹⁰¹See ‘The Facebook Business Tools’ *Facebook Help Centre* <www.facebook.com/help/331509497253087>. For information regarding APIs and SDKs see ‘APIs and SDKs’ *Facebook for Developers* <<https://developers.facebook.com/docs/apis-and-sdks>>. For information on the Facebook Pixel

Login, its APIs and SDKs, or the Facebook pixel – to (i) “provide, personalize and improve” its products, (ii) “provide measurement, analytics and other business services”, (iii) “promote safety, integrity and security”, (iv) communicate with the user, and (v) “research and innovate for social good”.¹⁰² Facebook now plans to integrate WhatsApp, Instagram and Facebook Messenger, a move that, if materialized, would allow Facebook to combine the data it has collected from the billions of users of these separate platforms.¹⁰³

Similarly, in 2012, Google consolidated more than 60 separate privacy policies into a single policy, in order to “create a beautifully simple, intuitive user experience across Google” and allegedly in response to regulators “calling for shorter, simpler privacy policies”.¹⁰⁴ As a result of this change, Google can combine the data it collects across its user-facing services (e.g. YouTube, Search, Maps) which it can use for a wide variety of purposes, including product improvement and, of course, online advertising.¹⁰⁵ Users have only limited ability to opt-out of having their data generated from one service (e.g. Maps) being used for another Google service (e.g. YouTube).¹⁰⁶ In 2016, Google changed its privacy policy again so that it may also associate data collected across third-party

see ‘The Facebook Pixel’ *Facebook for Business* <www.facebook.com/business/learn/facebook-pixel>. For information regarding Social Plugins see ‘Social Plugins’ *Facebook for Developers* <<https://developers.facebook.com/docs/plugins>>.

¹⁰²Facebook, ‘Data Policy’ <www.facebook.com/policy.php>.

¹⁰³Watchdog Collars Facebook Over Messenger Merger Plan’ (*Decision Marketing*, 29 January 2019) <www.decisionmarketing.co.uk/news/watchdog-collars-facebook-over-messenger-merger-plan>.

This announcement has been strongly contested by market players and authorities: Troy Wolverton, ‘Federal Regulators are Considering Blocking Facebook from Combining WhatsApp, Instagram and Its Other Apps’ *Business Insider* (12 December 2019) <www.businessinsider.com/facebook-could-face-an-injunction-from-the-ftc-2019-12>; Sissy Cao, ‘Mark Zuckerberg’s Plan to Merge All Facebook Apps Draws 4th Antitrust Probe’ *Observer* (17 January 2020) <<https://observer.com/2020/01/facebook-mark-zuckerberg-antitrust-lawsuit-over-merging-instagram-whatsapp-messenger/>>. This plan has moreover caused significant “internal strife” and has allegedly been part of the reason why Instagram and WhatsApp’s founders left the company. See Mike Isaac, ‘Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger’ *The New York Times* (25 January 2019) <www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html>.

¹⁰⁴Alma Whitten, ‘Updating Our Privacy Policies and Terms of Service’ (*Google Official Blog*, 24 January 2012) <<https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html>>.

¹⁰⁵*ibid*; see, also, Leena Rao, ‘Google Consolidates Privacy Policy; Will Combine User Data Across Services’ (*Tech Crunch*, 24 January 2012) <<https://techcrunch.com/2012/01/24/google-consolidates-privacy-policy-will-combine-user-data-across-services/>>.

¹⁰⁶To the authors’ best knowledge, there seems to be no way for users to prevent Google from using data generated from one service to improve other services or develop new services. The only control users have is to disable ‘personalized advertising’ so that they will not be targeted with personalized ads (see <<https://myaccount.google.com/intro/data-and-personalization>>). However, we note that this is a specific use case limitation relating to targeting. Nowhere does Google state that it will not use data collected from one service to perform non-targeting advertising functions on other services, such as frequency capping or attribution.

websites (e.g. through DoubleClick cookies) with personal Google Accounts.¹⁰⁷

Yet this “internal data free-for-all” is problematic, at least for two reasons.¹⁰⁸ First, it enables the creation of unique user super-profiles, allowing large platforms such as Google and Facebook to obtain a panoptic view of Internet users. This represents a major threat for user privacy.¹⁰⁹ Worse, Google and Facebook use these data for a number of unspecific data processing activities. These platforms often use vague terms in their privacy policies, stating that they use data to “provide their services”, “maintain and improve their services”, “develop new services”, “provide personalized services, including content and ads”, “measure performance”, “promote safety, integrity and security”, etc.¹¹⁰ These general purposes do not conform with the purpose specification component of the purpose limitation principle, which requires that purposes be clearly and specifically identified.¹¹¹ On the contrary, this wording bears a strong resemblance with the examples of unlawful practice identified by the Article 29 Working Party in its Opinion on purpose limitation.¹¹²

Moreover, once user data enter the “walled garden” of the platform, they can be used internally in ways that are unknown to all but the platform, due to the complete lack of transparency of how the latter’s processing activities operate. For example, Google has built a complex system, which is extremely difficult if not impossible to navigate, with users being lost in links to external policies and procedures, vague language and insufficient information on the uses of data.¹¹³ In fact, a detailed examination of Google’s numerous privacy-related sources and documents unveils that Google uses hundreds of purposes to justify its data processing activities instead of the six identified legal bases of Article 6(1) of the

¹⁰⁷Julia Angwin, ‘Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking’ (*ProPublica*, 21 October 2016) <www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking>.

¹⁰⁸Submission of Johnny Ryan from Brave to the CMA in response to the CMA’s Interim report on online platforms and digital advertising, 12 February 2020 <<https://brave.com/wp-content/uploads/2020/02/12-February-2020-Brave-response-to-CMA.pdf>>.

¹⁰⁹See also Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick, F.T.C. File No. 071-0170; Dina Srinivasan, ‘The Antitrust Case against Facebook’ (2018) 16(1) *Berkeley Business Law Journal* <<https://papers.ssrn.com/abstract=3247362>>.

¹¹⁰‘Google, ‘Privacy Policy: Why Google Collects data’ <<https://policies.google.com/privacy#whycollect>>; Facebook, ‘Data Policy’ <www.facebook.com/policy.php>.

¹¹¹See Article 29 Data Protection Working Party, ‘Opinion 03/2013 on Purpose Limitation’ (n 33).

¹¹²*ibid* 15; See also Complaint to the Irish Data Protection Commission, *Dr Johnny Ryan v 1. Google Ireland Limited 2. Google LLC* <<https://brave.com/wp-content/uploads/2020/03/Purpose-Limitation-Google.pdf>>.

¹¹³See in this regard *id.*, pages 11 et seq.

GDPR.¹¹⁴ The result is that Google benefits from what has been aptly described as an “internal data free-for-all”, by ignoring a core GDPR principle, hence obtaining a considerable competitive advantage over companies which act in compliance with the GDPR and which do not have such a market position and a diversified portfolio of consumer-facing products.

Second, this cross-usage of data may enable a dominant platform to engage in anticompetitive conduct by “enveloping” new markets while entrenching its market power in its core market.¹¹⁵ At a high level, this envelopment strategy works as follows: a platform dominant in one market (the “origin market”, e.g. Google in the general search market) enters a new platform market (the “target market”, e.g. the market for flights search) with overlap among potential users and offers its service for free to *all* sides of the market. It recoups such service through data cross-usage, i.e. data generated in the target market is combined with data in the origin market and used there, e.g. to improve the service or inform advertising served in the origin market. This strategy has the potential to exclude a competitor from the target market as it forms a credible predatory mechanism. At the same time, it prevents competitors in the target market from gaining data superiority and entering the origin market. The platform has the incentive to repeat this strategy again and again in the hunt for more data, conquering new markets while further entrenching its position in the core market where it monetizes the collected data. This strategy would not be possible if the platforms were required to keep the data separate per service (data siloes) – or at the very least, if users were *by default* opted out of having their data generated from one service being used for another service.¹¹⁶

The concept of data siloes seems to have gained popularity among regulators. For instance, the Bundeskartellamt has adopted a pioneering decision prohibiting Facebook from making access to its services conditional on the user accepting that Facebook may combine user data from its website, Facebook-owned services and third-party websites.¹¹⁷ The Bundeskartellamt requested Facebook to adapt its terms of use

¹¹⁴ibid.

¹¹⁵Daniele Condorelli and Jorge Padilla, ‘Harnessing Platform Envelopment Through Privacy Policy Tying’ (14 December 2019) <<https://ssrn.com/abstract=3504025>>.

¹¹⁶In this case users would have to opt in in order for the platform to use the data generated from one service for other services.

¹¹⁷Bundeskartellamt 6th Decision Division of 6 February 2019, B6-22/16 Administrative proceedings against 1. Facebook Inc. 2. Facebook Ireland Ltd. 3. Facebook Deutschland GmbH 4. Verbraucherzentrale Bundesverband e.V <www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf>.

and change its business model. Put simply, for the first time a competition watchdog ordered “internal unbundling” of data held by a dominant platform, having carefully examined the anticompetitive effects of the data practices of Facebook and recognizing that “[t]oday data are a decisive factor in competition”.¹¹⁸ While in an appeal lodged by Facebook, the Dusseldorf Higher Regional Court suspended the application of the Bundeskartellamt’s decision,¹¹⁹ on appeal the German Supreme Court sided with the competition authority.¹²⁰ The remedy of data siloes was also considered at length by the CMA in its Final Report on its online platforms and digital advertising market study.¹²¹

V. GDPR and privacy considerations are used as a justification for potentially restrictive conduct

In this Part we explain how, over the past couple of years, large platforms have been increasingly invoking the GDPR or broader privacy considerations to engage in practices that are *prima facie* problematic under competition law. We examine how Google in particular has invoked privacy to pull YouTube inventory from AdX (Section A), restrict portability of the DoubleClick ID (Section B) and phase out support for third-party cookies in Chrome (Section C). Google’s tactic raises serious concerns and should be addressed by regulators (Section D).

As a preliminary remark, while in some of the cases examined below Google has justified its conduct more broadly on “privacy concerns” and not explicitly on the need to comply with the GDPR, there is little doubt that the GDPR has shaped profoundly the modern privacy landscape. Consequently, any discussion of the latter without having regard to the GDPR would be incomplete. As explained above, along with the ePrivacy Directive, the GDPR provides the legal framework protecting

¹¹⁸Bundeskartellamt, ‘Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources’ (7 February 2019) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

¹¹⁹See Natasha Lomas, ‘Facebook Succeeds in Blocking German FCO’s Privacy-Minded Order Against Combining User Data’ (*Tech Crunch*, 26 August 2019) <<https://techcrunch.com/2019/08/26/facebook-succeeds-in-blocking-german-fcos-privacy-minded-order-against-combining-user-data/>>; Denis Schlimpert, ‘Victory for Facebook as Düsseldorf Court Suspends the Bundeskartellamt’s Decision’ (*Lexology*, 30 August 2019) <www.lexology.com/library/detail.aspx?g=eb62ca02-bc17-4757-8ede-0dc8af0ec8b7>.

¹²⁰Adam Satariano, ‘Facebook Loses Antitrust Decision in Germany Over Data Collection’ *The New York Times* (23 June 2020) <www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html>.

¹²¹CMA Final Report, ‘Appendix Z: Assessment of Potential Data-Related Interventions in Digital Advertising Markets’ paras 129–64 <https://assets.publishing.service.gov.uk/media/5efc3f7ae90e075c5aeb9947/Appendix_Z_-_Data_related_interventions_in_digital_advertising_markets.pdf>.

the digital privacy of EU citizens. Meanwhile, the GDPR has served as a model and a source of inspiration for non-EU countries wishing to strengthen their citizens' privacy.¹²² It is thus highly likely that the various "privacy defences" put forward by platforms have been at least partly influenced by GDPR considerations and the growing privacy awareness this piece of legislation has brought to individuals and companies.

As a further preliminary remark, it is noted that Google is not the only platform invoking privacy considerations to justify otherwise controversial practices. For example, Apple has also relied on privacy concerns to engage in conduct that could harm competition.¹²³ Most recently, several trade associations in France filed a complaint with the French Autorite de la concurrence against Apple over certain upcoming changes affecting user tracking on iPhones, claiming the changes (which Apple has portrayed as a win for user privacy) are anti-competitive.¹²⁴ However, for the purposes of the present paper, we chose to focus on Google's practices, given the latter's position in online advertising. Even so, the concerns we express over Google's "privacy defences" could apply with equal force to other platforms such as Apple.

A. Google's decision to remove YouTube inventory from AdX

In 2015, Google decided to remove YouTube inventory from AdX, cutting access to third-party DSPs such as TubeMogul or AppNexus.¹²⁵ YouTube inventory may be purchased only directly from Google or through its own buy-side software, namely Google Ads (at the time called AdWords) and DV360 (at the time called DoubleClick Bid

¹²²See Catherine Armitage, 'GDPR: The Emergence of a Global Standard on Privacy?' (*World Federation of Advertisers*, 28 November 2018) <<https://wfanet.org/knowledge/item/2018/11/28/GDPR-the-emergence-of-a-global-standard-on-privacy>>. The US is also considering adopting a federal privacy legislation, while California has passed its own legislation, called California Consumer Privacy Act ("CCPA"). See Peter M Lefkowitz, 'Why America Needs a Thoughtful Federal Privacy Law' (*The New York Times*, 25 June 2019) <www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html>; 'How the CCPA is Similar to the GDPR' (*TermsFeed*, 23 April 2020) <www.termsfeed.com/blog/ccpa-similar-gdpr/>.

¹²³See e.g. Chance Miller, 'Lawmakers Suggest Apple may be Using Privacy "as a Shield for Anti-Competitive Behavior"' (*9to5Mac*, 26 November 2019) <<https://9to5mac.com/2019/11/26/apple-privacy-antitrust-concern/>>.

¹²⁴Keach Hagey and Patience Haggin, 'Apple Faces Antitrust Complaint in France Over Privacy Changes in iPhones' (*The Wall Street Journal*, 28 October 2020) <www.wsj.com/articles/apple-faces-antitrust-complaint-in-france-over-privacy-changes-in-iphones-11603893625>. The authors consult for the complainants.

¹²⁵Kelly Liyakasa, 'Google to Yank YouTube Inventory Out of AdX By Year's End' (*AdExchanger*, 6 August 2015) <www.adexchanger.com/ad-exchange-news/google-to-yank-youtube-inventory-out-of-adx-by-years-end/>.

Manager). Rival DSPs reported serious harm as a result. For instance, in his testimony before the US House Judiciary Committee in 2019, AppNexus co-founder Brian O’Kelley submitted that

[t]his was a devastating move for AppNexus and other independent ad technology companies. [...] Even WPP, our largest customer and largest investors, had no choice but to start using Google’s technology. AppNexus growth slowed, and we were forced to lay off 100 employees in 2016.¹²⁶

The CMA expressed the concern that Google might have used the importance of its own and operated inventory to strengthen its position as a DSP provider.¹²⁷ The fact that YouTube inventory is available only through Google’s own DSPs was found to

affects advertisers’ choices of DSP for non-Google inventory as well because, as discussed above, a single DSP is typically used for a given campaign. As a result, advertisers who want to include YouTube inventory in their campaigns have a strong incentive to use DV360 for the entire campaign. As we have seen above, access to YouTube is one of the main reasons why advertisers choose DV360; several DSPs submitted that exclusive access to YouTube provides a very significant advantage to DV360 and creates a barrier to the growth of competitors.¹²⁸

Google’s initial counterargument was that third-party DSPs accounted only for a small percentage of YouTube spend, and in any event some other DSPs managed to attract advertisers despite the policy change.¹²⁹ However, in its response to the CMA Interim Report, Google raised an additional argument, namely user privacy:

[...] restricting third-party access both to our targeting data and our own inventory (such as YouTube inventory) is the best way to maintain the privacy of user information and prevent it from being leaked to potentially malicious actors. Third-party DSPs with access to YouTube inventory could build profiles of users based on their viewing history, which would be a data protection risk.¹³⁰

¹²⁶Testimony of Brian O’Kelley before the US Senate Committee on the Judiciary, Hearing on Understanding the Digital Advertising Ecosystem and the Impact of Data Privacy and Competition Policy, pages 5–6 <<https://www.judiciary.senate.gov/imo/media/doc/O'Kelley%20Testimony.pdf>>.

¹²⁷CMA Final Report, paras 5.263–5.264.

¹²⁸ibid, para 5.264.

¹²⁹CMA, ‘Online Platforms and Digital Advertising’ Market Study Interim Report (18 December 2019) para 5.210 <https://assets.publishing.service.gov.uk/media/5ed0f75bd3bf7f4602e98330/Interim_report_---_web.pdf>.

¹³⁰Google, ‘Online Platforms and Digital Advertising Comments on the Market Study Interim Report’ para 37 <https://assets.publishing.service.gov.uk/media/5e8c8290d3bf7f1fb7b91c2c/200212_Google_response_to_interim_report.pdf>. See also para 97: ‘The Interim Report suggests that it may be appropriate to integrate new sources of demand with our YouTube inventory

This was the first time Google publicly argued that its decision to pull YouTube inventory from AdX was motivated by privacy and data protection considerations. When Neal Mohan, then VP, Display & Video Advertising at Google, published a blog post in 2015 announcing the YouTube policy change, terms such as “privacy” or “data protection” were nowhere to be found.¹³¹ Instead, the decision to remove YouTube inventory from AdX was said to help Google focus its development efforts elsewhere:

To continue improving the YouTube advertising experience for as many of our clients as possible, we’ll be focusing our future development efforts on the formats and channels used by most of our partners. To enable that, as of the end of the year, we’ll no longer support the small amount of YouTube buying happening on the DoubleClick Ad Exchange.¹³²

We are thus skeptical as to whether Google’s decision was indeed motivated by privacy and data protection concerns. In any event, the concerns put forward by Google were dismissed by the CMA, which noted that “Privacy Enhancing Technologies (PETs) have been proposed by Google itself to allow targeted advertising without user profiling; similar solutions could be adopted for YouTube as well”.¹³³

B. Google’s decision to restrict portability of the DoubleClick ID

On 27 April 2018, on the eve of GDPR’s entry into force, Google announced that marketers would no longer be allowed to export certain data from its buy-side facing advertising products (DSP / ad server for advertisers) in order to ensure compliance with the new data protection rules.¹³⁴ The restriction concerned the so-called DoubleClick ID, a unique, cookie-based identifier assigned by Google to each user

(¶16.176). As noted above, restricting third-party access to YouTube inventory is the best way to keep user data private and to reduce the likelihood of ‘bad’ ads appearing alongside content”.

¹³¹Neal Mohan, ‘Focusing Investments to Improve Buying on YouTube’ (*DoubleClick Advertiser Blog*, 6 August 2015) <<https://doubleclick-advertisers.googleblog.com/2015/08/focusing-investments-to-improve-youtube-buying.html>>.

¹³²ibid.

¹³³CMA Final Report, para 5.265.

¹³⁴Alisson Weissbrot, ‘Google Sharply Limits DoubleClick ID Use, Citing GDPR’ (*AdExchanger*, 27 April 2018) <<https://adexchanger.com/platforms/google-sharply-limits-doubleclick-id-use-citing-gdpr/>> stating that “[i]n its note to advertisers, Google has included that the DoubleClick ID, tied to sensitive information like user search histories, could violate the strict data privacy requirements of GDPR”. Note that this restriction was accompanied by additional policy changes relating to YouTube, which however had been announced earlier. In January 2017 Google announced it would discontinue support for third-party measurement pixels on YouTube. Then, on 6 April 2018 Google announced it would no longer allow advertisers to use third-party ad servers to serve YouTube ads in the EU, “as part of [its] GDPR compliance efforts”.

exposed to a campaign executed through its products. Before the 2018 policy change, marketers could access this DoubleClick ID through Google's Data Transfer file service, which provided granular information for each campaign. Marketers would then export the DoubleClick ID to perform – with the help of independent ad tech vendors or their in-house tools – basic advertising functions such as cross-platform measurement (i.e. measuring the performance of the Google campaign against other platforms), frequency capping and multi-touch attribution.

After Google's policy change, the only way for marketers to access granular, event-level data is through Ads Data Hub, Google's cloud-based measurement and activation solution, originally developed for YouTube but then extended to DoubleClick and Google Display Network inventory.¹³⁵ Ads Data Hub is part of the Google Cloud Platform and has been touted as a solution providing access to event-level campaign data “in a privacy-centric environment”. Within Ads Data Hub marketers may upload their own first-party data and map it against Google's first-party data in order to analyse the performance of their campaigns.¹³⁶ Recently, it was reported that Google tests offering marketers the ability to create audiences within Ads Data Hub, which they may then target through Google's buy-side software, DV360.¹³⁷ But Ads Data Hub has an important limitation: marketers cannot export anything other than aggregated insights, and they are strictly prohibited from disaggregating Google's reports or identifying end users.¹³⁸ In other words, data goes in but does not leave the Ads Data Hub environment.¹³⁹

¹³⁵Kelly Liyakasa, 'Google Extends YouTube Measurement System To DoubleClick And GDN' (*AdExchanger*, 24 May 2017) <www.adexchanger.com/ad-exchange-news/google-extends-youtube-measurement-system-doubleclick-gdn/>.

¹³⁶Note that, perhaps in an attempt to sweeten the deal, Ads Data Hub grants marketers access to greater volumes of user data – instead of accessing the “DoubleClick ID”, marketers may now access the “User ID” which is tied to Google's logged-in environment and thus combines information about users collected across all Google properties and devices, including Android. See James Hercher, 'Marketers Struggle To Relearn The Former DoubleClick ID' (*AdExchanger*, 4 March 2020) <www.adexchanger.com/online-advertising/marketers-struggle-to-relearn-the-former-doubleclick-id>.

¹³⁷James Hercher, 'Google Tests Audience Buying In ADH, A Big Step from Analytics to Activation' (*AdExchanger*, 26 March 2020) <www.adexchanger.com/online-advertising/google-tests-audience-buying-in-adh-a-big-step-from-analytics-to-activation/>.

¹³⁸<<https://developers.google.com/ads-data-hub/policies>> accessed 27 March 2020.

¹³⁹As noted by Anthony Iacovone, co-founder and CEO of Barometric,

[t]he largest issue with Ads Data Hub is that it is a complete black box [...] It houses raw user and impression-level data, yet will not allow marketers to view or export anything in a format that will allow for granular optimizations per user. They [Google] are asking marketers to send all their data up into Ads Data Hub, and get nothing but aggregate counts back. There is no way for marketers to now verify or question the validity of any data that Google places within Ads Data Hub.

This policy change has been described by industry commentators as a move that “killed” independent attribution,¹⁴⁰ and as an example of “leveraging privacy concerns as a pretext” to further raise the walls of Google’s garden.¹⁴¹ A particular concern is that within Ads Data Hub marketers have no way to verify the accuracy and impartiality of Google’s measurement analysis. They simply have to trust that Google will “grade its own homework” fairly and will not overstate the performance of campaigns run through its own products vis-à-vis other campaigns.¹⁴² The fact that the same company is both a service provider and an auditor seems strange at best, and creates serious conflicts of interests at worst.

C. Chrome’s decision to phase out third-party cookies by January 2022

In January 2020, Google once more invoked privacy to justify perhaps its most controversial decision affecting online advertising: Chrome is expected to phase out support for third-party cookies within the next two years, as part of Google’s efforts to “increase the privacy of web browsing”.¹⁴³

Chrome is not the first browser to go after third-party cookies. For years Safari has blocked all third-party cookies by default, and since 2017 it also blocks alternative tracking methods as part of its Intelligent Tracking Prevention (“ITP”) feature.¹⁴⁴ In September 2019, Mozilla joined the club with its own anti-tracking mechanism for Firefox, called Enhanced Tracking Protection (“ETP”).¹⁴⁵ While not negligible,

See George Slefo, ‘Google’s Removal of DoubleClick ID Presents Litany of Issues for Brands, Agencies’ (*AdAge*, 8 May 2018) <<https://adage.com/article/digital/google-s-move-remove-doubleclick-id-presents-issues/313415>>.

¹⁴⁰Martin Kihn, ‘Did Google Just Kill Independent Attribution?’ (*AdExchanger*, 7 May 2018) <<https://adexchanger.com/analytics/did-google-just-kill-independent-attribution/>>.

¹⁴¹Robin Jurzer, ‘Google to Stop Media Buyers from Using DoubleClick IDs, Keeping Measurement & Attribution within Its “Walled Garden”’ (*MarTech Today*, 11 May 2018) <<https://martechtoday.com/google-to-stop-media-buyers-from-using-doubleclick-ids-keeping-measurement-attribution-within-its-walled-garden-215246>>.

¹⁴²George Slefo, ‘Google’s Removal of DoubleClick ID Presents Litany of Issues for Brands, Agencies’ (*AdAge*, 8 May 2018) <<https://adage.com/article/digital/google-s-move-remove-doubleclick-id-presents-issues/313415>>.

¹⁴³Justin Schuh, ‘Building a More Private Web: A Path Towards Making Third Party Cookies Obsolete’ <<https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>>.

¹⁴⁴Maciej Zawadzinski, ‘What Is Intelligent Tracking Prevention and How Does It Work? versions 1.0–2.3’ (*The Clearcode Blog*) <<https://clearcode.cc/blog/intelligent-tracking-prevention/>>.

¹⁴⁵Marissa Wood, ‘Today’s Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default’ (*The Mozilla Blog*, 3 September 2019) <<https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/>>.

the impact of ITP and ETP on the ad tech ecosystem has been rather limited, considering the modest market share of Apple and Mozilla when it comes to web browsing. Since Google, on the other hand, boasts a worldwide market share in excess of 64%,¹⁴⁶ it is fair to say that Chrome's policy change signals the demise of the third-party cookie.

To understand the profound consequences of Chrome's announced restriction, one should bear in mind that since its inception, online advertising – at least in the open web, as opposed to the walled gardens of Google or Facebook – has relied on third-party cookies for fundamental functions, such as frequency capping (i.e. limiting the number of times an ad is shown to the same person), targeting, conversion measurement and attribution.¹⁴⁷ For good or worse, no alternative to the third-party cookie has so far gained widespread industry adoption. As a result, in the absence of third-party cookies, online advertising in the open web risks crumbling. According to Google's own study, cookie-less impressions result in approximately 52% less revenue for publishers.¹⁴⁸ That seems consistent with the finding that impressions on Safari and Firefox (which already block third-party cookies) trade at a lower price, generating less revenue for publishers.¹⁴⁹

As an alternative to third-party cookies, Google has proposed to develop in collaboration with the wider online community (through the World Wide Web or "W3C" consortium) a set of Application Programming Interfaces (APIs) as part of the "Privacy Sandbox". The Privacy Sandbox is a Chromium initiative first announced in August 2019, whose mission is to enable online advertising while preserving user privacy, or as the Chromium Project puts it, "[c]reate a thriving web ecosystem that is respectful of users and private by default".¹⁵⁰ The basic concept behind the Privacy Sandbox is that all raw user data should be stored and processed on the device itself (and more specifically in the browser) and not made accessible to third parties. In order to perform advertising functions (e.g. frequency capping), third parties

¹⁴⁶See <<https://gs.statcounter.com/browser-market-share>> accessed 11 March 2020.

¹⁴⁷For an overview of what web cookies are, how they function and how they are used in online advertising, see Damien Geradin and Dimitrios Katsifis, 'Taking a Dive Into Google's Chrome Cookie Ban' (19 February 2020) <<https://papers.ssrn.com/abstract=3541170>>.

¹⁴⁸Deepak Ravichandran and Nitish Korula, 'Effect of Disabling Third-Party Cookies on Publisher Revenue' (27 August 2019) <https://services.google.com/fh/files/misc/disabling_third_party_cookies_publisher_revenue.pdf>.

¹⁴⁹Ari Paparo, 'Google, You Finally Really Did It' (*AdExchanger*, 14 January 2020) <www.adexchanger.com/data-driven-thinking/google-you-finally-really-did-it/>; Mat Bennett, 'Browser CPM Rates – When It Comes to Ad Revenue, All Browsers Aren't Equal' (*OKO Digital*, 5 July 2019) <<https://oko.uk/blog/cpm-by-browser>>.

¹⁵⁰See <www.chromium.org/Home/chromium-privacy/privacy-sandbox>.

(e.g. ad tech vendors, marketers etc.) will tap through the Privacy Sandbox APIs and extract aggregated insights. In other words, data collection will move to the *browser itself*, and advertising will move away from individuals and towards cohorts (larger group of users where individuals will not be identified).

As of the time of writing this paper, progress at the W3C on the Privacy Sandbox has been limited,¹⁵¹ and concerns have been expressed that it is a process dominated by Google.¹⁵² Considering Google's history of self-preferencing in the ad tech ecosystem,¹⁵³ legitimate questions can be raised as to whether the APIs will be implemented in a neutral manner or whether the owner of the browser, namely Google, will keep an advantage for itself. For instance, Google could grant its own buy-side solutions (DV360, Google Ads) superior access to information (e.g. access to non-aggregated data), and it is unclear whether third parties would be in a position to detect that.¹⁵⁴ In any event, given the central role of the browser in the various Privacy Sandbox proposals, there is a risk, as the CMA explained, that Chrome could become "the key bottleneck for ad tech". In this case, "[m]arket participants may be concerned that, under these proposals, Chrome would have the ability to use its position to favour Google's own ad tech intermediation services and raise barriers to entry".¹⁵⁵

Worse, if the APIs do not perform as well as third-party cookie-based tracking mechanisms, ad spend on "walled gardens" such as Google or Facebook will increase to the detriment of the open web and the ad tech ecosystem that supports it.¹⁵⁶ The reason is that walled gardens'

¹⁵¹Sarah Sluis, 'W3C Ad Tech Members Panicked About Slow Progress for Third-Party Cookie Alternative' (*AdExchanger*, 6 July 2020) <www.adexchanger.com/online-advertising/w3c-ad-tech-members-panicked-about-slow-progress-for-third-party-cookie-alternative/>.

¹⁵²See Allison Schiff, 'House Antitrust Report Highlights Unequal Power Dynamics at the W3C' (*AdExchanger*, 12 October 2020) <www.adexchanger.com/online-advertising/house-antitrust-report-highlights-unequal-power-dynamics-at-the-w3c/>.

¹⁵³CMA Final Report, para 5.271 et seq.

¹⁵⁴Mathew Broughton, 'The Hijacking of Privacy for Monopolisation' (*Exchange Wire*, 26 February 2020) <www.exchangewire.com/blog/2020/02/26/the-hijacking-of-privacy-for-monopolisation/>, noting that

[e]ven if Google releases the sandbox to everyone at once, as it should if user privacy is indeed its top priority, it could in theory give itself a helping hand by retaining user-level granularity, while offering others only aggregate data. One Privacy Sandbox API allows the allocation of a "privacy budget" purportedly to mitigate fingerprinting. Who sets the budget for each site? Who gathers and measures the data exposed to each site? Who enforces against violations of the budget? And who sets exemptions for the budget?

¹⁵⁵CMA Final Report, para 5.327.

¹⁵⁶James Rosewell, 'Google's Privacy Sandbox is a Plan Worthy of a Bond Villain' (28 February 2020) <www.linkedin.com/pulse/googles-privacy-sandbox-plan-worthy-bond-villain-james-rosewell/> ("[b]y only killing third-party cookies and attacking all technical alternatives under the guise of privacy,

ability to identify users on their platform relies on user login and will thus remain intact from any Chrome policy change. If online advertising in the open web cannot deliver its promise of one-to-one marketing, rational marketers would be expected to shift their budget towards the “walled gardens”, which already capture the lion’s share of digital ad spend.¹⁵⁷ This was concern was raised by the CMA in its Final Report on its market study on online platforms and digital advertising:

Therefore, to the extent that targeted advertising on open display inventory is less feasible or effective without third-party cookies, advertisers may substitute spending away from open display advertising and towards advertising on platforms’ owned-and -operated inventory.¹⁵⁸

After all, it should not be forgotten that at the same time Google competes for ad revenue with its very customers, namely publishers using its ad tech solutions. It thus appears questionable whether Google will have the incentive to invest in workable APIs that could replace third-party cookies in terms of effectiveness. If such APIs end up performing less effectively, Google might argue that this is a necessary compromise between enabling online advertising and maintaining higher privacy standards. Yet one cannot help but observe that Google seems to lack the same sensitivity towards privacy when it comes to online advertising on its *own* properties, where the Chrome restrictions will have little impact.

Finally, it is interesting to note that Google has alternative ways, not relying on third-party cookies (and thus not affected by the upcoming change), to track users across sites, such as Chrome itself: whenever a user is signed into any Google service (e.g. Gmail), she is automatically signed into Chrome.¹⁵⁹ If the user enables sync with her Google account and turns web and app activity on, then her browsing history

while leaving first party cookies untouched the value of the Walled Gardens’ inventory increases while simultaneously nuking that of their smaller rivals”). See also Joshua Koran, ‘The Death of Third-Party Cookies Disproportionately Hurts Small Publishers’ (*AdExchanger*, 25 March 2020) <www.adexchanger.com/the-sell-side/the-death-of-third-party-cookies-disproportionately-hurts-small-publishers/>, (“[b]y eliminating third-party cookies, there is a high probability of effectively limiting smaller publishers’ ability to compete online.”) See also ‘The Death of Cookies Will Create Data Monopolies’ (*Medium*, 17 April 2020) <<https://medium.com/@ipullrank/the-death-of-cookies-will-create-data-monopolies-40b92b0e13ca>>, (“[u]ltimately, moving in this direction is going to create ‘walled gardens’ that put smaller ad networks at a disadvantage, further consolidating power in the hands of the Googles, Facebooks, and Amazons of the world. While Google may insist that this move is motivated by its altruism and a deep concern for the privacy of users, it’s pretty clear to me that this is a power move”).

¹⁵⁷Perrin (n 6).

¹⁵⁸CMA Final Report, para 5.325.

¹⁵⁹<www.google.com/chrome/privacy/> accessed 5 April 2020. This feature received significant criticism, in that the Chrome sync UI is a dark pattern. See Matthew Green, ‘Why I’m Leaving Chrome’

is saved in her Google account on Google's servers and may be used to personalize experience on other Google products.¹⁶⁰ This allows Google to have an accurate view on the browsing history of users, without any need to rely on third-party cookies.

D. Some thoughts on the “privacy defence”

If Google's response to the CMA Interim Report is to offer a glimpse in the future, we can expect the “privacy defence” to be raised more and more often. Indeed, Google's response is remarkable for using privacy as a sort of all-purpose justification.¹⁶¹ “Privacy concerns” are put forward to justify various controversial practices – from pulling YouTube inventory from AdX to limiting the bidding data provided to publishers and refusing to participate in header bidding¹⁶² – but also to challenge remedies the CMA proposed in order to increase competition in search (such as sharing click and query data with rival search engines),¹⁶³ and to increase fee transparency in the ad tech ecosystem (such as imposing transaction IDs).¹⁶⁴ This privacy rhetoric raises serious concerns.

In the first place, Google appears to suggest that merely invoking user privacy or data protection suffices to automatically shake any antitrust liability off its shoulders – or to put it differently, remove the “*special responsibility*” of a dominant undertaking under Article 102 TFEU.¹⁶⁵

(23 September 2018) <<https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome/>>.

¹⁶⁰<www.google.com/chrome/privacy/> accessed 5 April 2020.

¹⁶¹Google, ‘Online Platforms and Digital Advertising Comments’ (n 130). The word “privacy” alone appears a total of 42 times in the 25-page submission.

¹⁶²ibid para 37 (regarding YouTube inventory), 43 and 48 (regarding the bidding data provided to publishers) and 39 (regarding header bidding). Header bidding is an auction type to which the ad tech industry resorted in response to what it perceived as Google using its ad server to favour its own intermediation activities.

¹⁶³ibid para 76:

aside from the risk of a data breach, the very fact of us sharing query data with third-parties could do irreparable harm to our reputation. Users trust us to treat their queries appropriately. Handing over those queries to third-parties – especially if this is done for money – may cause users to lose confidence in their ability to search privately with us.

Whether users indeed trust Google to make private searches, including sensitive searches (e.g. health-related searches) is a different issue.

¹⁶⁴ibid para 100:

[i]mposing consistent transaction IDs raises potential privacy concerns by allowing advertisers to join Google's secure bid data with other information in a way that would allow individual users to be identified. It would also allow various market participants along the intermediation chain to “pool” user data without user consent.

¹⁶⁵Note that Google should be able to argue that it has no other choice but to engage in a certain practice in order to comply with mandatory EU data protection rules. However, the threshold to be met is

Under this approach, anything can be permissible, insofar it may somehow be grounded on (vaguely defined) “privacy concerns”. This is obviously far from satisfactory and threatens the *effet utile* of competition rules.

In the second place, the analysis in the preceding Sections shows how a dominant undertaking such as Google has become the *de facto* regulator of privacy – which has aspects of a public good¹⁶⁶ – wielding powers that match or even exceed those of any DPA. While post-GDPR DPAs may impose significant fines, Google may simply change the rules of the game depending on its own interpretation of “privacy” or “data protection”, leaving customers and rivals with no choice but to comply with its privately set rules. And while in the case of DPAs the law provides for due process and the ability to seek judicial review of their decisions, in the case of a private regulator such as Google there is little affected companies may do. At best, they are confined to participating in a consultation process run by Google, as in the case of the Privacy Sandbox. At worst, Google may abuse its regulatory function to favour its own business and exclude rivals under the pretext of privacy.

There is thus a compelling case for regulators to intervene and address Google’s *de facto* regulatory function. At the very least, regulators should go beyond the surface and determine whether the privacy defense put forward is genuine and not a smokescreen for anti-competitive conduct. This leads us to make four suggestions, which could apply more broadly, i.e. would not be necessarily limited to Google.

First, the digital platform invoking privacy should lay down in detail its “privacy concerns”, so that regulators may determine whether such concerns are substantiated. Simply referring to “privacy” or “data protection risks” should not be sufficient as an objective reason to justify otherwise anticompetitive practices.

Second, regulators should treat privacy concerns with great caution whenever these are raised selectively, e.g. only when it comes to rivals. For instance, Google’s policy change in Chrome rejects the very concept of one-to-one advertising on the open web as bad for user privacy, even if the user has granted her consent in compliance with the GDPR. On the other hand, Google does not seem to be concerned about privacy when it comes to its owned and operated properties, where one-to-one advertising will still be the norm. Google considers

high, as Google will have to show that it has no margin of discretion when implementing the rules and there are no less restrictive alternatives to secure compliance with the law.

¹⁶⁶Joshua AT Fairfield and Christoph Engel, ‘Privacy as a Public Good’ (2015) 65 Duke Law Journal 385.

user consent sufficient for it to engage in extensive data processing activities, including combining data across its user-facing services under a single privacy policy and associating data with real-world identities. The fact that Google seeks to hold its rivals to a higher standard than the one applied to itself raises suspicions as to whether its privacy concerns are genuine.

Third, regulators should be aware that even if a certain product change leads to increased privacy for users, that does not necessarily mean that it should escape antitrust scrutiny. Instead, any positive effects for consumers (e.g. in the form of increased privacy) should be balanced against any negative effects on competition. The net effect may eventually be negative for consumers. In the case of Chrome's policy change, the incremental benefit brought to consumers in the form of increased privacy may be much smaller than expected, considering that it will do nothing to increase privacy within the walled gardens of Google and Facebook – which are the most popular websites on the web.¹⁶⁷ After all, it should not be forgotten that advertising in walled gardens may be more privacy-intrusive than cookie-based advertising in the open web, as it involves profiling and targeting users based on their real-world identities (as opposed to random anonymous identifiers in the case of cookie-based advertising in the open web). On the other hand, the effects of Chrome's policy change on competition seem significant. If the open web is impoverished and data is centralized to a handful of companies across the world, consumers could end up being worse off on balance.¹⁶⁸ As the CMA observed,

[m]easures which enhance an aspect of consumer privacy in the near term, may have dynamic effects which risk a negative impact on consumer welfare, for example a concentration of personal data amongst fewer providers, so impacting consumer choices and control in the longer term.¹⁶⁹

¹⁶⁷The Top 500 Sites on the Web' (Alexa) <www.alexa.com/topsites> accessed 30 April 2020; Top Websites Ranking' (SimilarWeb) <www.similarweb.com/top-websites> accessed 30 April 2020.

¹⁶⁸See also Koran (n 156), noting that

[w]hile these business interests are important, societal interests should take precedence. Centralizing more data in fewer companies is likely not the desired outcome for most privacy advocates. The policies behind some regulations and browser changes ironically do just that. Freedom of expression is fundamental to thriving democracies. How should we evaluate policies that limit the number of platforms that enable consumers to interact with each other? How should we evaluate policies that limit the companies marketers and publishers can work with? Hopefully, we continue to support policies that increase the number of voices, rather than diminish them.

¹⁶⁹CMA Final Report, para 5.328.

Finally, on the enforcement side, it is crucial that different regulators (e.g. national competition authorities (“NCAs”), DPAs) cooperate with each other in order to avoid pursuing an overly narrow approach. On the positive side, it seems that regulators are gradually becoming aware of this worrying trend of invoking privacy considerations to engage in restrictive conduct. For instance, the CMA appears sensitive to the concerns raised by the Privacy Sandbox. The CMA has also found that “Google and Facebook have a clear incentive to apply a stricter interpretation of the requirements of data protection regulation when it comes to sharing data with third parties than for the use and sharing of data within their own ecosystems”, and proposed to work closely with the ICO in order to consider “the appropriate approach to such concerns in the future”.¹⁷⁰

VI. Looking forward

While the GDPR has played a major role in strengthening data protection in the EU, it seems to have had unintended consequences, such as further strengthening Google to the detriment of small and medium-size market players in the ad tech ecosystem. As we have seen, that is the case for two reasons. First, the GDPR has increased market concentration in ad tech markets already dominated by Google. Second, Google has been increasingly invoking the GDPR or broader privacy considerations to justify conducts which are *prima facie* problematic under competition law. At the same time, Google has bundled the privacy policies of its various products, allowing it to combine data it collects through its products for uses within its various internal units. This “internal data free-for-all”, which is of course advantageous to its ad tech activities, is questionable under the GDPR’s purpose limitation principle.

It is thus imperative that the Commission, DPAs and NCAs identify and remedy these shortcomings in the interpretation and enforcement of the GDPR which affect competition in the market.

First, it is crucial that the Commission takes into account the imbalance of power in terms of financial and human resources that exists between large and small players. Considering the substantial implementation and compliance costs the GDPR entails, the Commission should examine the differentiated effects of the GDPR to different-sized companies. While the GDPR already imposes additional obligations the riskier

¹⁷⁰ibid para 5.330.

the type of processing, the baseline obligations imposed still disproportionately affect medium and small size companies. A more differentiated approach might therefore be needed to avoid unintended consequences to the detriment of such companies.

Second, it is imperative that the GDPR be effectively and uniformly enforced across the EU. As shown above, the one-stop-shop principle allows large platforms to escape liability due to the reluctance of certain DPAs to undertake investigations and impose sanctions, but also due to the practical limitations following from the lack of human resources and technical expertise to deal with a vast amount of complaints against such players. At the same time, smaller ad tech players have been subject to rigorous scrutiny by certain DPAs. We recognize the benefits of the one-stop-shop system, in that it allows companies to only deal with one DPA and to avoid simultaneous investigations and possibly contradicting decisions in the different EU Member States. We therefore do not call for a repeal of this mechanism, as doing so would complicate GDPR compliance and enforcement for numerous companies engaged in cross-border processing.

We however consider it necessary that a more uniform enforcement of the GDPR be actively encouraged by the Commission and the EDPB. The EDPB should identify problematic areas where divergent interpretations of the GDPR have been adopted or might be adopted by DPAs across the EU and level the playing field by issuing more guidance on how to interpret and enforce the GDPR in the ad tech ecosystem. Moreover, the Commission should challenge Member States where DPAs are not effectively enforcing the GDPR and could even consider opening infringement proceedings, including in cases where Member States fail to give DPAs the human and financial resources necessary to perform their tasks as required by Article 52(4) of the GDPR.

We also recommend the establishment of a specialized “tech” unit at the EU level – possibly within the EDPB – which would be staffed with technical experts. This unit would help DPAs with the technical aspects of investigations involving large tech companies. It would thus help alleviate the burden of DPAs overwhelmed with complex investigations, and facilitate and accelerate their investigations. As a last resort, and only if GDPR enforcement remains ineffective – or distorted by the uneven enforcement of its provisions in the Member States – in the future, the Commission should consider whether the decentralized enforcement system is appropriate or whether it should be replaced by an EU privacy regulator with full supervision and enforcement powers.

Third, regulators should ensure that the GDPR cannot be used as a pretext to restrict data sharing and distort competition to the benefit of large players holding abundant first-party data. As explained above, the “privacy defence” raises serious concerns and threatens the *effet utile* of competition rules. It is important that competition authorities – be it the Commission or NCAs – should closely examine any justification based on data protection legislation, if need be in close cooperation with DPAs.

Finally, regulators should keep a watchful eye on Google’s decision to phase out third-party cookies on Chrome and the evolution of the Privacy Sandbox, as it is bound to fundamentally alter the shape of online advertising in the open web. Though formally an open source project, we are skeptical as to which extent third parties will have any meaningful say in the process, and past experience from the Android Open Source Project shows how Google may end up running initiatives which are nominally open source. There is a real risk that Chrome’s policy change will further strengthen walled gardens to the detriment of the open web (and the ad tech ecosystem). Indeed, the Privacy Sandbox risks making the browser the “gatekeeper” of data, on which third parties (be it publishers, advertisers or ad tech vendors) will be dependent. As more ad spend is concentrated on the walled gardens, the open web may become impoverished, with all the societal implications this entails. While regulators have a duty to ensure that user tracking on the web takes place in full compliance with the GDPR, they also have a duty to preserve competition in the open web, from which consumers stand only to benefit.

Acknowledgements

The authors advise a variety of ad tech vendors and publishers, including on matters adverse to Google. The views expressed in this paper are the authors’ only.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Damien Geradin  <http://orcid.org/0000-0001-5378-8354>