CONFIDENTIAL

Report by the European Publishers Council on the Impact of the General Data Protection Regulation "GDPR" on News Media Publishers

April 2020

European Publishers Council's public ID number in the Transparency Register is: 4456380381-30

On the basis of an internal questionnaire sent to our members, this Report from the European Publishers Council has been prepared for the European Commission to consider as part of their review of the General Data Protection Regulation "GDPR", and is divided into five Parts:

Part I – Introduction and Overview looking at the effects of the GDPR on news publishers and to inform the European Commission of the unintended consequences of the GDPR on news publishers and on the online advertising eco-system more widely on which they critically depend as a source of revenue.

Part II – Looking Forward: Key Recommendations While the GDPR has played a major role in strengthening data protection in the EU, we have seen increasing market concentration to the detriment of smaller market participants in the ad tech ecosystem which negatively impacts news publishers. We invite the European Commission to consider and remedy the shortcomings we have identified which affect innovation and competition in the market.

Part III provides our short overview of the objectives of the GDPR, the principles it enshrines and draws some conclusions from its implementation.

Part IV analyses the GDPR's unintended consequences in more detail: As will be seen, the GDPR has increased concentration in the markets in which the collection and processing of personal data is important, including in online advertising markets on which news publishers are so heavily dependent. We will also show that the GDPR and privacy considerations have been used by Google to engage in anticompetitive conduct.

Part V identifies some problematic practices that the GDPR has *not* prevented: First, the GDPR has not prevented Google from combining the data it collects across its user-facing services (e.g., YouTube, Search, Maps) and use it for a wide variety of purposes, hence allowing what has been labelled an "internal data free-for-all". Second, due to the narrow approach of DG Competition, the GDPR has done nothing to prevent big data mergers, which once again strengthen the position of large online platforms.

I. Introduction and Overview

This Report presents the views of the European Publishers Council ("EPC")[1] on the General Data Protection Regulation ("GDPR")[2] and its effects on news publishers and the wider online community. Its purpose is to inform the European Commission of the unintended consequences of the GDPR on news publishers, and on the online advertising eco-system on which they critically depend as a source of revenue. While the GDPR has provided important benefits to society at large in terms of increased privacy, it has also strengthened the dominant position of large platforms in online advertising markets, such as Google and Facebook, to the detriment of their smaller rivals and news publishers. This increased market concentration harms news publishers in terms of choice, innovation and revenues and arguably undermines the benefits of GDPR for the users of large platforms. For these reasons, the current situation is in our view unsustainable.

The regulatory changes brought by the entry into force of the GDPR have affected news publishers significantly:

- First, on the positive side, the GDPR has raised privacy-awareness for their readers and initiated and promoted social debate on the important topic of data protection. GDPR has increased privacy-awareness in corporations across business sectors, and placed this important fundamental right on the agenda across Europe, as well as globally.

- Second, on a more negative side, compliance with GDPR is a particularly challenging task for news publishers. There are many reasons for this, but the main issue is that processing of personal data is a key aspect of most publishers' business models. Processing of personal data is an absolute necessity both when providing a news publisher service (providing services over the internet always involves processing personal data in the form of IP addresses, but also often for such purposes as personalisation of the services), as well as for revenue generation through ads. The publishers' products cannot be provided without processing personal data; nor can the revenues needed to fund the content production be generated without processing personal data. For news publishers, it is therefore not a question of whether personal data must be processed, but how personal data can be processed ensuring the right to privacy but without removing the financial fundament for the publisher's business.

[1] The EPC is a high-level group of Chairmen and CEOs of Europe's leading media groups representing companies with newspapers, magazines, online publishing, journals, databases, books and broadcasting. We have been communicating with Europe's legislators since 1991 on issues that affect freedom of expression, media diversity, democracy and the health and viability of media companies in the European Union.

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

The competition landscape within advertising is a particularly challenging one, where publishers' main competitors are not usually other publishers, but rather a few major global corporations which often operate under different jurisdictions to the publishers, or which through their platforms create a dominant market position that makes it possible for them to both capitalise on certain legal positions in relation to GDPR, and to dictate to the wider market. When it comes to consent, publishers are not required to put Consent Management Platforms (CMP) in place in order to process data on their own account; but are forced to do so by the buy-side, which needs the publishers to get the consents of the users on their behalf in order for them to operate, and if publishers do not help them to obtain consent they will quite simply put their money elsewhere.

The human resources and capital costs involved in ensuring compliance with the GDPR, together with the threat of a high level of fines, disproportionately burden the smaller publishers – which are limited by both financial resources and by personnel. For example, Microsoft had 1.600 engineers working on GDPR compliance since its enactment in 2016.[3] By contrast, news publishers, many of which are SMEs, do not have the lawyers, data experts and programmers necessary to make compliance with the GDPR a smooth and effective process.[4] Additionally, compliance with certain requirements of the GDPR, such as adopting technical and organisational measures, and monitoring and documenting data flows, exhibits economies of scale and scope, which tend to create a competitive advantage for large organisations. Even though the GDPR is by nature "scalable", the requirements are extremely challenging for smaller companies working in businesses where data is necessarily an intrinsic part of participation.

- Third, an even more negative impact of the GDPR on news publishers is that it has a large impact on one of their main sources of revenue (or in some cases their *only* source of revenue), which is online *display* advertising. While historically news publishers directly negotiated advertising deals with advertisers or their agencies, in the digital space news publishers increasingly rely on programmatic advertising,[5] and on providers of ad intermediation services, such as Google. Moreover, as online advertising increasingly relies on behavioural targeting, it is essential for advertising intermediaries to collect and process data about online users. Even delivering non-personalised advertisements also requires personal data since a cookie ID, which is the most widespread vehicle of ad serving, is considered personal data within the GDPR. Given that the data collected and / or processed

[3] Jule Brill, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft Blog*, 21 May 2018, available at https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

[4] Ivana Kottasová, "These companies are getting killed by GDPR", *CNN Business*, 11 May 2018, available at https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

[5] Programmatic advertising consists in automated decision-making, where dedicated software and complex algorithms fueled by various categories of user data are used to sell and purchase ad inventory within fragments of a second, avoiding "human" negotiation between publishers and advertisers.

qualifies as "personal data" under EU data protection rules, compliance with the GDPR has become a major issue across the online advertising ecosystem. In this context, it is easy to see why a regulation that, as will be demonstrated below, has the effect of increasing concentration in (already concentrated) online advertising markets is likely to result in less innovation, inefficiencies and higher advertising intermediation fees to the detriment of news publishers and ultimately their readers.

- The great paradox described in this Report is that while large online platforms, such as Google and Facebook are responsible for some of the most egregious data collection and processing practices, the GDPR has effectively strengthened their market position to the detriment of smaller rivals, but also to news publishers which depend heavily on their market-dominant advertising intermediation tools to monetise their content.

- While a reduced ability to monetise their content hurts news publishers directly and may even drive some of them to bankruptcy, it can also have wider societal implications as the dissemination of high quality (and therefore costly to produce) information is essential to a well-functioning democracy.

II. Looking Forward: Key Recommendations

While the GDPR has played a major role in strengthening data protection in the EU, as we describe below in more detail it has had unintended consequences which resulted in further strengthening the large players especially Google and Facebook, and increasing market concentration to the detriment of smaller market participants in the ad tech ecosystem. This in turn negatively impacts news publishers in depriving them of choice and innovation, while allowing Google to extract excessive intermediation.

It is crucial therefore that the Commission distinguishes between the collection and usage of data by publishers as 1st parties, in comparison to the widespread collection and usage of data by 3rd parties. Publishers' 1st party data processing should be regarded differently and as more privacy secure, and this we believe should be reflected in future privacy legislation.

It is imperative to identify and remedy these shortcomings which affect competition in the market as follows:

- First, we ask that the Commission takes into account the imbalance of power in terms of financial and human resources that exist between large and small players. This is crucial considering the substantial implementation and compliance costs the GDPR entails, and we ask the Commission to examine the differentiated effects of the GDPR to different-sized companies and should respond by adopting a proportional approach, including the level of fines.

- Second, it is important to level the playing field in the enforcement of the GDPR. The one-stop-shop principle allows big players to escape liability due to the reluctancy of certain DPAs to undertake investigations and impose sanctions in fear of losing investment in their countries. At the same time, news publishers have been subject to rigorous scrutiny by certain DPAs. The Commission should encourage more effective and uniform enforcement of the GDPR and should consider allowing DPAs other than that of the main establishment of a company to carry out investigations for potential GDPR-violations.

- Third, appropriate action is needed to ensure that the GDPR cannot be used as a pretext to restrict data sharing and distort competition. While in principle complying with data protection legislation could amount to an objective justification under EU competition law, merely *invoking* the GDPR or broadly defined privacy considerations does not suffice. Instead, to the extent a firm has multiple options at its disposal to ensure compliance with the GDPR, there is a valid argument that it should opt for the least restrictive measure, in line with the principle of proportionality. It is important that competition authorities – be it the Commission or national competition authorities – should examine closely any justification based on data protection legislation, if need be in close cooperation with the DPAs.

- Fourth, processing of personal data within online advertising should be governed by the same legal bases as all other kinds of processing of personal data. This means, that legitimate interest as legal basis might be relevant for some (for instance when online advertising is a crucial part of a publisher's business model and the publisher takes measures to mitigate privacy risk), but not for others (ad tech vendors compiling profiles on individuals or processing of special categories of data for ads purposes). Additionally, it should be made clear that dictating another legal entity's legal basis (for example Google requiring publishers to collect consent) may be a misuse of dominant market position. Each data controller is responsible for and shall have the liberty to choose their legal basis according to applicable law and their own processing.

- Fifth, recognising that limitations on data sharing which follow from the GDRP erect barriers to entry and strengthen the competitive position of dominant players holding abundant first-party data, the Commission should ensure that small businesses and new entrants have access to data that are necessary for them to power their advertising businesses and compete with large players.

- Finally, we would urge the Commission to consider carefully Google's decision to **phase out third-party cookies on Chrome**, and to question the appropriateness of Google leading development of what will follow. Therefore, close attention to the evolution of the Privacy Sandbox is essential, as the outcome is bound to alter fundamentally the shape of online advertising in the open web. Though formally an open source project, we are sceptical as to what extent stakeholders will have any meaningful say in the process, as past experience from the Android Open Source Project shows how Google may end up running initiatives which are only nominally open source. Given the Privacy Sandbox's potential to further

strengthen walled gardens to the detriment of the open web (and thus news publishers), the Commission should engage with Google and if need be extract commitments to ensure that its implementation will not distort competition.

III. GDPR in a nutshell

This Part provides a brief overview of the objectives of the GDPR (Section A), its core principles (Section B) and the implementation system of the GDPR with particular reference to news media (Section C).

The objectives of the GDPR

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.[6] Given the increasing importance of digital technologies in all sectors of the economy and society in general, ensuring a "*consistent and high level of protection of natural persons*" with regards to "*their right to the protection of personal data*" has become crucial.

First, the scale of the collection, use and sharing of personal data by private companies and public authorities is unprecedented, and "*[n]atural persons increasingly make personal information available publicly and globally.*" Moreover, "*[t]he economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data*", between a wide range of public and private actors, including natural persons, associations and undertakings across the Union, as well as national authorities.[7] These market realities necessitate the establishment of a "*strong and more coherent*" data protection framework within the EU and the existence of strong enforcement mechanisms. Only if data are collected and used in a way that places the rights and interests of the individuals first, EU citizens will have real control over their data and "*trust and embrace data-driven innovations*."[8]

Second, it is necessary that legal and practical certainty and transparency are increased not only for natural persons, but also for economic operators, including micro, small and medium-sized enterprises, and public authorities. In this regard, the GDPR seeks to level the playing field in all EU Member States regarding the obligations and responsibilities of controllers and processors, the

---

6 GDPR, 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.

7 GDPR, Recitals 5 and 6.

8 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European strategy for data, COM(2020) 66 final, 19 February 2020, page 1; GDPR, Recital 7.

monitoring of processing of personal data, the legally enforceable rights of natural persons and the sanctions available in the hands of National Authorities.[9]

The principles enshrined in the GDPR

The GDPR centers around seven principles: "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", "integrity and confidentiality" and "accountability".[10] In the context of online advertising, which as noted above is a major source of revenue for news publishers, there is industry-wide uncertainty as to how to conform with the principle of lawfulness when real-time-bidding ("RTB"), a core feature of programmatic advertising, is involved. Part of the challenge here is that before GDPR many technology providers in this area have been operating without having regard to privacy requirements, and have not sufficiently revised their practices after GDPR came into effect.

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. Even though all legal grounds are equal, there is a worrisome tendency in some Member States to rule out the use of certain grounds for the purpose of advertising or direct marketing. While it is clear that processing can be carried out on the basis of the data subject's consent,[11] considerable uncertainty has arisen as to whether the "legitimate interests" legal basis can be used. As publishers have relied on revenues through advertising long before the birth of the internet, this is both concerning and problematic. If collecting consent in order to be able to generate revenues to finance the production of the content becomes *de facto* the only legal basis, this would mean that users would be free to choose whether or not publishers could generate revenues to compensate a user's access to their content through advertising. This would lead publishers to switch to a model where access to content would only be available when purchasing a subscription. This would have severe negative effects for democracies and freedom of speech across Europe, and not only pose a substantial threat to the fundamental interest in media pluralism, but also hinder other fundamental rights and interests covered by the EUs charter on fundamental rights.

A prevailing view is that the "legitimate interests" legal basis cannot be used by **third parties** for the processing of personal data for building profiles to be used for online advertising. A general prohibition on using legitimate interest for processing personal data for advertising purposes is also argued by some; however such a prohibition would have far-reaching consequences for media

---

9 GDPR, Recital 13.

10 GDPR, Article 5.

11 Although it is argued that valid consent under the GDPR cannot be obtained in the context of RTB, as it is unrealistic to believe that data subjects can give informed and specific consent to the processing of their data. See, for example, ICO, "Update report into adtech and real time bidding", 20 June 2019, available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf; Digital Europe, "Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework", 21 January 2020, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/01/Position-paper-on-GDPR-review.pdf.

pluralism and democracy, and the discussions are often at a level that does not take into account the privacy-enhancing measures that can be put in place, or the fundamental interest of publishers in obtaining advertising revenue. The discussions around this topic are generally characterised by a very low level of technical insight into what actually happens when online advertisements are served and how a publisher is able to control what happens to the data when online ads are shown.

Additionally, the debate often disregards the importance of advertising for the creation of journalistic content, and focuses mainly on "bad practice" examples which are clearly in violation of privacy rights where publishers or ad tech vendors do not strike a fair balance between the rights and interests at stake. Common misunderstandings are for instance that publishers are unable to control what kind of data is shared with third parties, which third parties' data is shared, and what those third parties may use the data for. All of this is possible to control. Other misunderstandings are that special categories of data (such as data regarding health, religion, etc.) must be shared or that direct identifiers are shared (such as name, e-mail etc.). Sharing sensitive data is not at all necessary for online advertising, and if it is indeed processed, there is no question that consent is necessary, as this is explicitly required by the GDPR. Direct identifiers are generally unnecessary to disclose, and publishers can set requirements both technically and legally to hinder this. In practice, we expect the limits of legitimate interest to be set during the coming years, also through legal remedies.

In certain jurisdictions, the requirements regarding consent for cookies are the same as those for processing personal data. This includes for instance the UK. In jurisdictions where the consent requirements are the same, the discussions around legitimate interest are redundant, as publishers and vendors would always need to collect consent for online advertising because cookies are an inherent part of how online advertising works. Open questions that are not yet clarified, and that could potentially revive such discussions are whether bundling consent for different purposes or making access to a site available only for those who consent, are in line with the principles regarding consent bundling and conditionality in GDPR.

Implementation of the GDPR

The GDPR provides for a decentralised 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]*."[12] 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].*"[13]

Supervisory authorities from all EU Member States "*shall cooperate with each other and the Commission*" in order to "*contribute to the consistent application of [the GDPR].*"[14] The GDPR establishes an one-stop-shop mechanism when cross-border processing takes place, according to

[12] GDPR, Article 51(1).

[13] GDPR, Article 55(1).

[14] GDPR, Article 51(2).

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."*[15] This allows businesses operating in different countries to deal, in most cases, with one Data Protection Authority ("DPA").[16] However, **this system does not make it any simpler for publishers** as they are regulated in each and every one of their markets; while many of the 3rd parties work across the countries and may be regulated by authorities in other markets, and thus not necessarily consistent with the local interpretation in the particular market of the publisher.

IV. GDPR's unintended consequences

Despite the hope that the GDPR would provide a strengthened data protection framework across the EU, the reality is that the GDPR has had unfortunate, unintended consequences. In particular, the GDPR led to an increase in market concentration, notably in the online advertising field (Section A) and has been used as a justification for potentially anticompetitive conducts (Section B).

A. Increased market concentration

In this Section, we provide an overview of the ways in which the GDPR has increased market concentration. First, implementation and compliance costs create barriers to entry or may cause exit (Subsection 1). Second, large online platforms benefit from advertisers' trust (Subsection 2). Third, it is easier for large platforms to obtain end-user consent, either directly through their numerous consumer-facing products or indirectly through publishers (Subsection 3). Fourth, the GDPR entails restrictions in data sharing, which has benefited large players that have their own troves of data (Subsection 4). Finally, the one-stop-shop system provided for in the GDPR has led to arbitrary enforcement to the benefit of dominant platforms (Subsection 5).

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

The GDPR has significantly increased compliance costs; from acquiring user consent through a CMP, employing a DPO, documenting data flows and ensuring internal compliance with the GDPR to monitoring the use of data by third parties with which the data has been shared. Such costs may disincentivise market entry in the EU, as new entrants – in addition to facing the numerous challenges of entry – have to invest heavily in GDPR compliance. In this respect, GDPR compliance may be too much of a (financial and operational) burden on smaller ad tech players, most of which are unknown to end-users as they are further down the ad tech funnel. These players may find it preferable – or in

[15] GDPR, Article 56(1).

[16] European Commission, "The GDPR: new opportunities, new obligations – What every business needs to know about the EU's General Data Protection Regulation", available at https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf, page 2.

some cases be forced – to exit the (European) market altogether,[17] hence increasing market concentration in a market already dominated by Google and Facebook.

2. Large online platforms benefit from advertisers' trust

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%.[18] Since then, the market dominance of Google and Facebook in online advertising has further strengthened.[19]

The fear of liability and the large fines envisaged on the basis of the GDPR have led advertisers to concentrate their ad spending on the largest players (in particular Google), as they trust that they are compliant with the Regulation.[20]

Trust in larger players follows on three – not necessarily correct – 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. Third, that such companies will be more careful with users' personal data as they have more to lose in case of non-compliance.

However, this dramatic shift in demand towards Google products was not only the result of advertisers trusting that large platforms are 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**. It thus required advertisers using Google's ad tech products to buy only through its own ad tech products for which it could guarantee that it has valid user consent.[21] However, on the sell-side, Google has never really

---

17 See 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.")

18 Jessica Davies, "'The Google Data Protection Regulation': GDPR is strafing ad sellers", *Digiday*, 4 June 2018, available at https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

19 Mark Scott, Laurens Cerulus and Laura Kayali, "Six months in, Europe's privacy revolution favors Google, Facebook", *Politico*, 23 November 2018, available at https://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, available at https://www.fastcompany.com/90351655/gdpr-helps-google-and-facebook-grow-uk-market-share-in-2019.

20 Nick Kostov and Sam Schechner, "GDPR Has Been a Boon for Google and Facebook", *The Wall Street Journal*, 17 June 2019, available at https://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.

21 Jessica Davies, "'The Google Data Protection Regulation': GDPR is strafing ad sellers", *Digiday*, 4 June 2018, available at https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

enforced the need for consent with sites that are running Google ads. Any site can implement google ad tags without Google check for consent. Google just requires the site owner to guarantee that consent has been gathered.

Effectively Google exploited its dominance in the ad tech sector to strengthen its position even further in the name of the GDPR – benefitting from the dependency and trust of advertisers. While advertisers and (indirectly) publishers became more dependent on Google, smaller vendors felt the repercussions.

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

While obtaining user consent to the processing of their personal data may be challenging for small ad tech vendors, it has not been a problem for large online platforms, as they can easily obtain direct consent through log-in requirements from users through their consumer-facing products as a condition of use, but also indirect user consent through news publishers.

a. Large platforms can more easily obtain direct consent from users

The strengthened data protection framework set out by the GDPR has made it harder for smaller players to collect and use data. Privacy-aware consumers might be hesitant to give consent to the processing of their data – especially when seeing that their data might be used for a variety of purposes, such as advertising and measurement.

On the contrary, Google and Facebook's market dominance and the existence of network effects allow them to obtain users' consent to the collection of personal data.[22] Billions of people are dependent on Facebook, Instagram, Gmail, WhatsApp and the likes, which they consider an indispensable part of their personal 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 engine and WhatsApp as "absolutely essential", as they help them maintain social contacts, offer a high level of service at no charge, adjust themselves to their personal interests and are highly useful in daily life. 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 sometimes too cumbersome to read all relevant notices or too difficult to refuse – the perceived essential nature of internet services outweighs their concerns about their data being collected.[23]

In addition, large and diversified controllers enjoy an advantage by combining the consent requirements for all their data uses. As a result, once they obtain user consent through *one* of their

[22] Jon Markman, "GDPR Is Great News For Google And Facebook, Really", *Forbes*, 22 May 2018, available at https://www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/#fac153448f63.

[23] Anne Niedermann, "Freely-Given and Informed Consent? The User's Perspective", *Presentation of the results of the Allensbach survey*, *DLD Europe*, 9 September 2019.

user-facing products, this consent can be used as a valid legal basis for the processing of personal data from *all* internal units and divisions. For example, in 2012, Google consolidated more than 60 separate privacy policies into a single privacy 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*."[24]

According to this new Privacy Policy, if a user is signed in, Google may combine information the user has provided from one service, with information from other services, and thus create aggregated and detailed profiles of users that can be used in advertising.[25] Such a massive collection of personal data places large platforms in a competitive advantage compared to smaller players. The larger the volume of a database, the diversity of its sources, its accuracy, reliability and freshness, the higher its commercial value, as elaborate databases allow the better and more accurate identification of users – and thus are more valuable for advertisers.

b. Platforms can extract end-user consent indirectly from publishers

Large platforms that offer products across the entire online advertising value chain – and especially Google – are indispensable ad tech partners for the majority of publishers. This market position allows them to request publishers to obtain end-user consent on their behalf for processing operations that will be independently determined by the platform. Even though not all publishers want to say yes, the alternative is daunting. For example, about 60% of publishers' programmatic revenue comes from Google.[26] Google's network is unmatched in terms of both size and scope and moving to other services would irreparably harm publishers.[27] If a publisher decided not to obtain consent on behalf of a large platform, they would see their revenues considerably decreasing and their continuing existence being at risk.[28] By using their market power to obtain indirectly end-user consent, the large players avoid the burden of providing all the information required by the GDPR for data subjects to

---

24 See Updating our privacy policies and terms of service, 24 January 2012, available at https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html

25 Alma Whitten, "Updating our privacy policies and terms of service", *Google Official Blog*, 24 January 2012, available at https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html; see, also, Leena Rao, "Google Consolidates Privacy Policy; Will Combine User Data Across Services", *Tech Crunch*, 24 January 2012, available at https://techcrunch.com/2012/01/24/google-consolidates-privacy-policy-will-combine-user-data-across-services/.

26 George P. Slefo, "Google and GDPR hand publishers a hard choice", *AdAge*, 30 April 2018, available at https://adage.com/article/digital/google-gdpr-force-a-hard-choice-publishers/313305.

27 Ellen Tannam, "Why are publishers unhappy with Google's GDPR proposal?", *SiliconRepublic*, 1 May 2018, available at https://www.siliconrepublic.com/enterprise/google-gdpr-publishers.

28 See Barry Levine, "Four publisher groups to Google: Your GDPR proposal 'severely falls short'", *MarTech Advertising*, 30 April 2018, available at https://martechtoday.com/four-publisher-groups-to-google-your-gdpr-proposal-severely-falls-short-214870; Paresh Dave, "Publishers rebuke Google's interpretation of EU privacy law", *Reuters*, 30 April 2018, available at https://www.reuters.com/article/us-alphabet-privacy-publishers-gdpr/publishers-rebuke-googles-interpretation-of-eu-privacy-law-idUSKBN1I11GG.

be able to give informed and specific consent, hence effectively transferring liability to publishers for not complying with the GDPR in getting data subject consent.[29]

This was clearly illustrated in March 2018 when, in anticipation of the entry into force of the GDPR, Google announced at the last minute that it was planning to adopt changes to its ad policies and required publishers and advertisers using Google's advertising services "*to get consent from end users to use [Google's] services*" that complies with the GDPR requirements of consent.[30] At the same time, Google designated itself as a data controller independent from the publishers, for data it receives from publishers and collects on publisher pages.[31] Google justified this announcement by stating that that it "*operate[s] as a controller for [its] publisher products because [it] regularly make[s] decisions on the data to deliver and improve the product.*" In other words, Google uses "*data across Ad Manager and Ad Exchange publishers for purposes of product improvement, including to test ad serving algorithms, to monitor end user latency, and to ensure the accuracy of [Google's] forecasting system.*"[32] Moreover, Google "*use[s] data to deliver relevant and high-performing ads in features like optimised pricing in the open auction.*"[33]

Put simply, this blanket self-proclamation of Google as an independent data controller constituted an outright prohibition on news publishers from using Google as a processor, and required publishers to obtain valid consent from their users for the processing carried out by Google, which benefits Google in ways beyond the knowledge or control of the publisher.

4. Limiting ability to share data also helps large platforms

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

---

29 See GDPR, Article 13. See, also, Joint letter of Digital Content Next, European Publishers Council, News Media Alliance and News Media Association to Google CEO, Sundar Pichai, 30 April 2018, available at https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf.

30 Carlo D'Asaro Biondo, "Changes to our ad policies to comply with the GDPR", *Google Ads Blog*, 22 March 2018, available at https://www.blog.google/products/ads/changes-to-our-ad-policies-to-comply-with-the-GDPR.

31 See Google, "Google Ads Controller-Controller Data Protection Terms", available at https://privacy.google.com/businesses/controllerterms/; Google, "Ad Manager and Ad Exchange program policies Tools to help publishers comply with the GDPR", *Google Ad Manager Help*, available at https://support.google.com/admanager/answer/7666366?hl=en.

32 Google, "Ad Manager and Ad Exchange program policies – GDPR FAQs", *Google Ad Manager Help*, available at https://support.google.com/admanager/answer/9035987?hl=en.

33 Google, "Ad Manager and Ad Exchange program policies – How Google uses Ad Manager and Ad Exchange data", *Google Ad Manager* Help, available at https://support.google.com/admanager/answer/7670381.

– and by imposing liability in cases of violation of the GDPR.[34] Data sharing is, therefore, risky. Small players are likely to abstain from data sharing, as this would further stretch their limited human and financial resources and expose them to liability.

The negative consequences from limited data sharing are mostly felt by smaller players, including news publishers that want to increase their ad targeting capabilities, which do not hold large amounts of data and therefore rely heavily on data they receive from other data controllers. For large companies holding massive amounts of data, there is limited incremental value from data transfers – as they 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 reputable data suppliers, whom they trust to comply with the GDPR. This affects competition and creates 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 and the identification possibilities they allow.

5. *One-stop-shop benefits large players*

The one-stop-shop system envisaged in the GDPR means that companies have to deal with only one DPA – the supervisory authority of their main establishment. This is advantageous to large players with processing operations across the EU, as it significantly reduces the number of investigations the company has to face and the number of contact points it has to deal with. However, while publishers are put under strict enforcement in the countries that have started local enforcement actions, these local interpretations do not in reality apply to the platforms.

The one-stop-shop system, moreover, entails that major Big Tech investigations will have to be carried out by a few authorities – mainly in Dublin or Luxembourg, where most tech firms are established in the EU. This creates serious bottlenecks which, coupled with the dubious role of certain DPAs and the arbitrary enforcement of the GDPR, results in tech giants escaping close monitoring and liability, and millions of web users being left unsatisfied.[35]

---

34 Consider, 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)).

35 Nicholas Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *Politico*, 27 December 2019, available at https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

Notably, the Irish DPA, which oversees, among other giants, Google, Facebook, Microsoft and Twitter, has long been accused of catering to the very companies it is supposed to oversee, by not actively seeking to monitor compliance with the GDPR, undertake investigations or impose fines.[36] This passive stance can be explained by the strong economic dependency that exists between the tech giants and Ireland – which raises questions as to whether Ireland is best-suited for regulating Big Tech.[37] It is 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 force of GDPR.[38] It is also surprising that Ireland continues taking a softer approach in its investigations, by avoiding on-site inspections and sanctions and opting for negotiations with the companies instead.[39]

At the same time, DPAs in other EU Member States – and in particular in France – have shown that they are more eager to hunt big platforms.[40] Were the one-stop-shop system not to be applied, these DPAs could go after the large tech players and ensure a more effective enforcement of the GDPR in Europe.

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

Over the past couple of years Google has been increasingly invoking the GDPR, or broader privacy considerations, to engage in conduct *prima facie* problematic under competition law, and in particular: restrict portability of the DoubleClick ID (Subsection 1), prevent publishers from matching Data Transfer files (Subsection 2), phase out third-party cookies on Chrome (Subsection 3), removal of context (URL information) from bid requests for any vendor other than Google, and poor match rates on cookie IDs between google and other ad technologies. By reducing match rates of Google data outside the Google tech stack, Google exploits their data preeminence to force publishers to use

36 Nicholas Vinocur, "How one country blocks the world on data privacy", *Politico*, 24 April 2019, available at https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123.

37 Nicholas Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement", *Politico*, 27 December 2019, available at https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

38 Padraic Halpin, "Irish regulator opens first privacy probe into Google", *Reuters*, 22 May 2019, available at https://www.reuters.com/article/google-dataprotection/irish-regulator-opens-first-privacy-probe-into-google.

39 For 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 Nicholas Vinocur, "How one country blocks the world on data privacy", *Politico*, 24 April 2019, available at https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123.

40 For example, in January 2019, the French Data Protection Commission (CNIL) imposed a 50 million fine on Google for lack of transparency, inadequate information and lack of valid consent regarding ads personalisation. See CNIL, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC", 21 January 2019, available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

the Google ad tech, in the name of GDPR. If publishers use another tech stack, the targeting in the Google buying systems deliberately does not recognise any users on the publishers' sites.

Considering the increasing importance of data protection rules across the world (the most recent example being the California Consumer Protection Act), we think this practice – of which the CMA recently took note[41] – will continue to gain popularity among digital platforms, and sooner or later regulators will have to address it.

1. *Restricting 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.[42] The restriction concerned the so-called "DoubleClick ID", a unique, cookie-based identifier assigned by Google to each user 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 provide 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.

The only way to access granular data now is through Ads Data Hub, Google's *own* measurement and attribution solution, originally developed for YouTube but then extended to DoubleClick and Google Display Network inventory.[43] But Ads Data Hub has an important limitation: while marketers may access granular data to perform their analysis,[44] they are prohibited from exporting anything other

---

41 Competition and Markets Authority, "Online platforms and digital advertising", Market study interim report, 18 December 2019, available at https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf, paragraph 5.233.

42 A. Weissbrot, "Google Sharply Limits DoubleClick ID Use, Citing GDPR", *AdExchanger*, 27 April 2018, available at 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*".

43 K. Liyakasa, "Google Extends YouTube Measurement System To DoubleClick And GDN", *AdExchanger*, 24 May 2017, available at https://www.adexchanger.com/ad-exchange-news/google-extends-youtube-measurement-system-doubleclick-gdn/.

44 Note 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 "Google ID" which combines information about users collected across all Google properties and devices, including Android.

than aggregated insights. In other words, data goes in but does not leave the Ads Data Hub environment.[45]

This policy change has been described by industry commentators as a move to "kill" independent attribution,[46] and as an example of "*leveraging privacy concerns as a pretext*" to further raise the walls of Google's garden.[47] 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.[48]

2. *Preventing publishers from matching Data Transfer files*

Google has relied (at least partially) on privacy considerations to also restrict the data made available to publishers. In September 2019, as part of Google Ad Manager's migration to a single unified first-price auction, Google announced the introduction of a new Bid Data Transfer File, a file including bidding data from the auctions organised by Google Ad Manager.[49] Google proclaimed that the new file would increase "*auction transparency*". However, the new file comes with a restriction: it cannot be linked with other Data Transfer Files from Google Ad Manager, "*in order to prevent bid data from being tied to individual users.*"[50] While at the time the precise rationale for making this policy change was not entirely clear, Google later confirmed to the CMA that it "*was also prompted by consumer privacy considerations*."[51]

---

45 As noted by A. 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*." See G. Slefo, "Google's removal of DoubleClick ID presents litany of issues for brands, agencies", *AdAge*, 8 May 2018, available at https://adage.com/article/digital/google-s-move-remove-doubleclick-id-presents-issues/313415.

46 M. Kihn, "Did Google Just Kill Independent Attribution?", *AdExchanger*, 7 May 2018, available at https://adexchanger.com/analytics/did-google-just-kill-independent-attribution/.

47 R. Jurzer, "Google to stop media buyers from using DoubleClick IDs, keeping measurement & attribution within its 'walled garden'", *MarTech Today*, 11 May 2018, available at https://martechtoday.com/google-to-stop-media-buyers-from-using-doubleclick-ids-keeping-measurement-attribution-within-its-walled-garden-215246.

48 G. Slefo, "Google's removal of DoubleClick ID presents litany of issues for brands, agencies", *AdAge*, 8 May 2018, available at https://adage.com/article/digital/google-s-move-remove-doubleclick-id-presents-issues/313415.

49 J. Bigler, "Rolling out first price auctions to Google Ad Manager partners", 5 September 2019, available at https://www.blog.google/products/admanager/rolling-out-first-price-auctions-google-ad-manager-partners/.

50 Id.

51 Competition and Markets Authority, "Online platforms and digital advertising", Market study interim report, 18 December 2019, available at

It is understood that this restriction has created considerable inefficiencies in the way publishers monetise their inventory and could affect competition among ad exchanges. Before the policy change publishers would typically link various Data Transfer Files from Google Ad Manager in order to make better informed decisions when monetising their inventory. For instance, publishers could link the files to measure the incremental value of non-Google ad exchanges participating through header bidding.[52] That is no longer possible. As the CMA observed in its Interim Report, as a result "*SSPs will find it increasingly difficult to demonstrate how they add value for publishers, while publishers will have less incentive to sustain the costs of integrating non-Google SSPs through header bidding*."[53] As a result, this can have a negative impact on the news publishers to monetise efficiently their content, hence affecting their revenues.

3. Phasing out third-party cookies on Chrome

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*."[54]

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.[55] In September 2019, Mozilla joined the club with its own anti-tracking mechanism for Firefox, called Enhanced Tracking Protection ("ETP").[56] The impact of ITP and ETP on the ad tech ecosystem has been patchy and dependent on the market share of Apple and Mozilla when it comes to web browsing which varies across the EU. Since Google, on the other hand, boasts a worldwide market share in excess of 64%,[57] for its browser, 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 on 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, targeting, conversion measurement and attribution (hence the need for the legal

https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf, paragraph 5.223.

52 Id., paragraph 5.222.

53 Ibid.

54 J. Schuh, "Building a more private web: A path towards making third party cookies obsolete", available at https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

55 M. Zawadziński, "What Is Intelligent Tracking Prevention and How Does It Work? [versions 1.0 – 2.3]", *The Clearcode Blog*, available at https://clearcode.cc/blog/intelligent-tracking-prevention/.

56 M. Wood, "Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default", *The Mozilla Blog*, 3 September 2019, available at https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/.

57 https://gs.statcounter.com/browser-market-share, last accessed on 11 March 2020.

ground of legitimate interest to be integrated into any new ePrivacy Regulation). For better 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.[58] 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.[59]

As an alternative to third-party cookies, Google has proposed to develop in collaboration with the wider online community (through the 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.*"[60] The basic concept behind the Privacy Sandbox is quite similar to that behind Ads Data Hub: all the raw user data will be stored in the browser and not made accessible to third parties. In order to perform advertising functions (e.g., frequency capping), third parties (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*.

As of the time of writing this Report, the Privacy Sandbox is just a set of proposals, and it remains to be seen what shape the proposed APIs will eventually take. Considering Google's history of self-preferencing, 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 (e.g., in the form of granting its own buy-side solutions superior access to information).

Worse, if the APIs do not perform as well as cookie-based tracking mechanisms, ad spend on "walled gardens" such as Google or Facebook will increase to the detriment of the open web (and thus on the webpages of news publishers); and we would refer you to an earlier point to underline the problem due to the low match rate we already currently see in the cookie-based world outside the Google systems. The reason is that walled gardens' ability to identify users on their platform relies on first-party cookies / 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

---

58 Deepak Ravichandran and Nitish Korula, "Effect of disabling third-party cookies on publisher revenue", 27 August 2019, available at https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf.

59 A. Paparo, "Google, You Finally Really Did It", *AdExchanger*, 14 January 2020, available at https://www.adexchanger.com/data-driven-thinking/google-you-finally-really-did-it/; M. Bennett, "Browser CPM Rates – When it comes to ad revenue, all browsers aren't equal", *OKO Digital*, 5 July 2019, available at https://oko.uk/blog/cpm-by-browser.

60 https://www.chromium.org/Home/chromium-privacy/privacy-sandbox.

would be expected to shift their budget towards the "walled gardens", which already capture the lion's share of digital ad spend.[61]

V. The GDPR does not prevent unwarranted data accumulation and processing practices

Meanwhile, the GDPR has not prevented large digital platforms from engaging in certain data accumulation and processing practices to solidify their position, namely combining data internally across products and divisions (Section A) and acquiring data-rich targets (Section B).

A. Internal data flows of the large digital platforms

While imposing limits on external data transfers, the GDPR seems to do little to limit any internal data sharing within various units of large digital platforms. As explained above, Google's privacy policy enables it to combine the data it collects across its user-facing services (e.g., YouTube, Search, Maps) and use it for a wide variety of purposes, including product improvement and, of course, advertising. 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).[62] In 2016 Google changed its privacy policy again so that it may also associate data collected through its services and across the web (e.g., through DoubleClick cookies) with personal Google Accounts.[63]

Yet this "internal data free-for-all" within the large digital platforms is problematic, at least for two reasons.[64] First, it enables the creation of unique user super-profiles, allowing large firms to obtain a panoptic view of Internet users. This represents a major threat for user privacy.[65] Second, this cross-

---

61 Nicole Perrin, "Facebook-Google Duopoly Won't Crack This Year", *eMarketer*, 4 November 2019, available at https://www.emarketer.com/content/facebook-google-duopoly-won-t-crack-this-year.

62 In particular, 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, that 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.

63 J. Angwin, "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking", *ProPublica*, 21 October 2016, available at https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.

64 Submission of J. Ryan from Brave to the CMA in response to the CMA's Interim report on online platforms and digital advertising, 12 February 2020, available at https://brave.com/wp-content/uploads/2020/02/12-February-2020-Brave-response-to-CMA.pdf.

65 See also Dissenting Statement of Commissioner Pamela Jones Harbour in the matter of Google/DoubleClick, F.T.C. File No. 071-0170.

usage of data may enable a dominant platform (e.g., Google) to envelop new markets while entrenching its market power in its core market.[66]

At a high level, this envelopment strategy could work as follows: a platform dominant in one market (the "origin market", e.g., Google in general search) enters a new platform market (the "target market", e.g., 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., in order 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 monetises the collected data. This strategy would not be possible if the platforms were required to keep the data separate per service – 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.[67]

B. Big data mergers are still allowed

Data-driven mergers have long been a tool in the hands of large players allowing them to acquire even more data. For example, Google acquired DoubleClick in 2008, Microsoft acquired Skype in 2011 and LinkedIn in 2017, and Facebook acquired Instagram in 2012 and WhatsApp in 2014. The Commission has cleared such acquisitions without taking proper account of the effects the combination of data would have on competition and European consumers. While the ignorance of the effects of a combination of large datasets could be justified back in 2008, the value of data has been well-understood in recent years. It will therefore be interesting to see whether the Commission will take a more privacy-oriented approach in an examination of the planned acquisition of Fitbit by Google.

Despite the realisation of the immense value of data online advertising, the GDPR has not restricted – or even been a factor – such mergers. A merger is, however, the easiest way for large platforms to enlarge their databases and enrich the profiles of their users. The only "restriction" placed by the GDPR regarding the consolidation of databases in the case of mergers is that merging databases cannot be automatic. In other words, the merged entities must obtain valid consent of their data subjects to the use of their data by the merged entity, unless another legal basis for processing can be used. However, companies have long been adopting clauses in their privacy policies that provide for the sharing of data in the case of a merger or acquisition – and to which users consent by accepting the privacy policy. Whether that is in compliance with the GDPR is another question – especially since

---

66 D. Condorelli and J. Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", 14 December 2019, available at SSRN: https://ssrn.com/abstract=3504025.

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

the user cannot be informed about the merging parties or give granular consent to specific purposes of processing when the merger is not even envisaged. However, given the lack of enforcement of the GDPR – especially against tech giants which are more likely to proceed with acquisition of smaller players – conditions like these are still allowing merging parties to combine datasets.

Contact details

Angela Mills Wade
Executive Director
European Publishers Council
Avenue des Arts 43, 1040 Brussels
Telephone: +322 231 1299
angela.mills-wade@epceurope.eu