Online Platforms Team
Competition & Markets Authority
Victoria House
Southampton Row
London WC1B 4AD
United Kingdom

30 July 2019

Online platforms and digital advertising market study

Dear Colleague,

1. We welcome the opportunity to comment on the CMA's market study of online platforms and digital advertising. We have professional and personal interests in this study.

   - Dr Ryan represents Brave, a rapidly growing Internet browser based in San Francisco and London, co-founded by Brendan Eich, the inventor of JavaScript and co-founder of Mozilla/Firefox.

   - Dr Lynskey is an Associate Professor at LSE, working in the areas of data protection and technology regulation. Dr Lynksey is an editor of International Data Privacy Law (OUP) and a member of the European Commission's GDPR Expert Stakeholder Group. She has previously worked in Competition Law practice in Brussels.

   We respond to the three themes defined in the CMA's statement of scope in turn, with reference to our previous work and expertise where relevant.

2. Data is power. Data is both a potential source of market power and is a source of power over individuals. As such, the control over and processing of personal data by undertakings is a matter that is relevant to multiple regulators and regulatory frameworks, including competition law, data protection law and consumer protection law. The issues raised are thus both substantive and institutional.

3. From a substantive perspective, intermediary platforms occupy a strategic place in the online environment, putting them in a privileged position to collect and process personal data across a wide variety of content and services. When these intermediaries are dominant, they are able to exploit this privileged position by extracting excessive personal data in exchange for the use of their platform. Moreover, many of the 'behind the scenes' practices which these platforms

provide an economic incentive for – most notably, online advertising and the real-time bidding process – operate in their shadow. As regulators cannot see this shadow economy, they have difficulties regulating it.

4. From an institutional perspective, it is critical that regulators collaborate to avoid unnecessary duplication and ensure consistency and coherence in the policies they pursue and in how they interpret and apply relevant legal frameworks.

Theme 1 The market power of online platforms in consumer-facing markets

The Factors Leading to Market Power

5. The factors that lead to market dominance in a given market are multi-faceted. Digital markets are no different.

6. While dominant companies, such as Facebook, maintain a strong proprietary claim over the personal data they process (for instance, by collecting data regarding user activity from webpages with embedded Facebook plug-ins but not sharing this data), it is often claimed that personal data is not itself a barrier to entry to digital markets. Rather, it is asserted that it is what is done with the personal data – the algorithm that it is applied to it, for example – that is decisive in obtaining a competitive advantage through data. We acknowledge that whether personal data is a barrier to entry is an empirical question that must be subject to a context specific assessment. In making this assessment, we concur with the German and French competition authorities that the volume of data alone is not decisive and that an assessment of the 'quantity and quality of the established company's data set' is required.[1]

7. Beyond control over data, it is possible to identify several factors that contribute to dominance in the online environment: direct and indirect network effects; a permissive competition framework, permissive oversight of data-driven mergers and acquisitions; commercial data-agreements between dominant undertakings and other parties enabling data-sharing; and a flexible data protection framework with weak enforcement mechanisms.[2]

8. The example of Facebook will illustrate how these factors can be brought to bear in order to consolidate the market power of a digital platform. First, we could say

---

[1] Autorité de la Concurrence and Bundeskartellamt, 'Competition law and data', Joint Report, 10 May 2016, p 13. Available at: www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

[2] Orla Lynskey, 'Grappling with "Data Power": normative nudges from data protection and privacy' (2019) Theoretical Inquiries in Law 189-220.

that network effects have played a significant role in Facebook's success as a platform and in the failure of would-be competitor platforms. Facebook now has over 2 billion active users with no sign of a viable competitor on the horizon. Put simply, this is because consumers want their social networking service to be social: it is critical for consumers that their friends and family also use the platform. This direct network effect can lead to indirect network effects: advertisers will be attracted to the Facebook platform for advertising given the large number of active users it has attracted and its potential to mine its data to profile these users for targeted advertising purposes.

9. Facebook has further consolidated this market power, through a series of data-driven acquisitions, the most notable of which being its acquisition of potential competitors Instagram and Whatsapp as well as Onavo. The latter was a virtual private network (VPN) which enabled Facebook to gain a strategic oversight of how its users were using other mobile phone applications.[3] Although the European Commission examined the Whatsapp merger and granted it merger clearance, the commercial rationale for Facebook's acquisition of Whatsapp – the acquisition of Whatsapp user data – fell in the blind spot of the Commission's analysis.[4] Furthermore, the implications of the transaction from a data protection perspective, were entirely overlooked by the Commission, which delegated this issue to data protection law.

10. This is unfortunate as the strain on the data protection regime brought about by ubiquitous data processing and a weak data protection framework has itself contributed to the dominance of Facebook. The entry into force of the General Data Protection Regulation (GDPR) is likely to improve the effectiveness of the framework, in particular from an enforcement perspective.[5] Yet, as the market's response to the recently announced USD5 billion fine for Facebook indicates, given its high turnover and the centrality of personal data processing to its operations, a concerted and consistent approach to its legal compliance is required.

Cascading Monopolies and the Leveraging of Market Power in Data-Driven Markets

[3] PC Magazine, 'Apple: Facebook's Onavo VPN Violates App Store Rules', 23 August 2018. Available at: https://uk.pcmag.com/news-analysis/117034/apple-facebooks-onavo-vpn-violates-app-store-rules.

[4] Orla Lynskey, Non-price Effects of Mergers - Note. OECD - Directorate for Financial and Enterprise Affairs - Competition Committee DAF/COMP/WD(2018)70.

[5] Orla Lynskey, "The 'Europeanisation' of Data Protection Law" (2017) Cambridge Yearbook of European Legal Studies 252-286.

11. We believe that dominant digital companies use their position of market power as intermediaries to create cascading monopolies.

12. The leveraging of market power from one digital market to another through a combination of the mechanisms mentioned above – acquisitions; network effects; weak data protection enforcement – is evident in the following example.

GOOGLE: A DATA GRAB?

Google operates over eighty services. Until 2012, Google held these data in distinct silos. In 2012, Google pooled the data it processed about individuals across its services. As a result, this integrated data set enabled Google Shopping, for instance, to use data collected on YouTube or other Google services to offer advertisements to individuals.

Separately, Google acquired a large advertising technology firm called DoubleClick in April 2007. DoubleClick builds up profiles about what people do online in order to define for advertisers what people should see which advertising. When Google bought DoubleClick, it promised to never combine Google users' personal data from Gmail, YouTube and other accounts with DoubleClick's data about them. In June 2016 Google went back on that promise, combining personal data about every online individual from its DoubleClick business and all other Google businesses. DoubleClick is active on 8.4 million websites,[6] which means that its data concerns every single person in the UK.

Indeed, Google was already acquiring one company per week in 2011, thereby increasing the volume and variety of the data it amassed.[7]

It also entered into strategic agreements involving data sharing with one such example being a partnership between Deepmind (held by Alphabet, Google's parent company) and the NHS Royal Free Trust in London. This partnership saw the NHS Trust hand over the data of 1.6 million patients of the Trust without their consent and without a commitment on Deepmind's part to separate this data from that held by its parent company.[8]

Finally, in September 2018, Google modified its "Chrome" web browser so that users would automatically be signed in to the browser when they use any

[6] DoubleClick.Net Usage Statistics, (URL: https://trends.builtwith.com/ads/DoubleClick.Net).

[7] Leena Rao, Eric Schmidt: Google is Buying One Company a Week ", TechCrunch, (Dec. 7, 2011. Available at: https://techcrunch.com/2011/12/07/eric-schmidt-google-isbuying-one-company-a-week/.

[8] Julia Powles & Hal Hodson, 'Google DeepMind and healthcare in an age of algorithms' 7 Health & Technology (2017) 351.

individual Google service. In other words, it was no longer possible to use Chrome without being signed in to the browser once one signed in to Gmail, or any other Google product. Google did not announce this change.

13. In this example, Google acts as a cascading monopoly, leveraging its power from one market to the next in a way that actively circumvents individual control over personal data.

14. It may be argued that such practices are not unique to dominant digital firms, and this is undoubtedly true. Yet, as competition experts are aware, the actions of dominant firms merit particular attention because (a) these firms shape the markets on which they operate and (b) the implications of their actions are felt most acutely by all those dependent on them. Indeed, it is for this reason that these firms have a 'special responsibility' in competition law[9] and should also have a 'special responsibility' when it comes to respecting the rights of individuals.[10]

15. As outlined briefly below, the actions of dominant digital firms militate against effective data protection regulation. We wish to highlight two aspects of this tension.

16. First, not only do the actions of dominant companies render individual control over personal data virtually impossible, they also unsettle established data protection principles designed to ensure the collective benefits of data protection. This aspect is often overlooked in competition reports, which focus on perfecting individual control over data and thus ensuring efficient data markets. Second, dominant firms have created a norm of data excess, in much the same way as banks created a norm of credit excess prior to the financial crisis. This norm in turn incentivises a shadow economy based on unnecessary and insecure data processing (which is beyond the scope of this note).

Theme 2 Consumer control over data collection practices

Individual Control over Personal Data and its Data Protection Limits

17. While much of the focus in the statement of scope is on the mechanisms of 'consent' and 'transparency' in data protection law, it is imperative to recall that while data protection law seeks to give individuals control over personal data,

[9] Case 322/81, *Michelin v Commission,* para 70.
[10] Lynskey, 'Grappling with Data Power' (above).

this control is not absolute, nor should it be.[11] Individual control over personal data is, in some instances, neither a necessary nor a sufficient aspect of the data protection framework. Indeed, attempts to create a framework based entirely on such individual control would be tantamount to creating a property right in personal data, and a market for such data, a route which data protection law in Europe deliberately eschews.

18. Rather, the objectives served by data protection – as with other fundamental rights such as freedom of expression – are both individual and collective. The legal framework therefore strikes a balance between competing rights and interests. It recognises situations where individual consent is not necessary and principles that must be respected irrespective of individual consent.[12] Two such principles – particularly relevant in the context of online data processing – are purpose limitation and data minimisation.

19. Purpose limitation ringfences the personal data processed by undertakings.[13] According to this principle, personal data can only be processed for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes'. Further regulatory guidance on this principle has been provided by European data protection authorities in 2013. The then 'Article 29 Working Party' advised that a purpose must be "sufficiently defined to enable the implementation of any necessary data protection safeguards," and must be "sufficiently unambiguous and clearly expressed."[14] The objective of this test was to ensure that 'individuals will know what to expect' and to prevent 'unanticipated uses' by the controller or third parties of the data.[15]

20. Consider for example the act of posting a photo on a hypothetical social media service for the first time. The distinct processing purposes involved might be something like the following list. The person posting the photo is only interested in the first four or five of these purposes:

    - To display your posts on your feed.
    - To display posts on tagged friends' feeds.

---

[11] The data protection framework allows for data processing in the public interest, irrespective of whether an individual concurs with such processing for example (Article 6(1)(e) GDPR). Data protection, and individual control over personal data, is also balanced with other rights and interests (for example, freedom of expression: Article 85 GDPR).

[12] See generally, Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015, 229-254.

[13] Article 5(1)(b) GDPR.

[14] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 12.

[15] "Guidelines on consent under Regulation 2016/679", Article 29 Working Party, 28 November 2017, p. 12.

- To display friends posts that tag you on your feed.
- To identify untagged people in your posts.
- To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc…, to make our feed more relevant to you.
- To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc…, to make ads relevant to you.
- To record your reaction to posts to refine future content for you, which may include ethnicity, politics, sexuality, etc…, for advertising fraud prevention.

If a company were to rely on consent, for example, then consent must be requested in a granular manner for each "specified, explicit" data processing purpose. In other words, consent cannot be bundled, as an Advocate General of the Court of Justice of the EU has recently affirmed.[16]

21. In the Working Party guidelines on consent, European Data Protection Authorities observed that:

> "data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes … If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific …. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose."[17]

22. If we return to the example above of the Google 'Single Sign-In' for Chrome browser users, it is unlikely it would meet the standard of 'predictability' or the requirement that information be presented to individuals in an accessible and unbundled format. Following outcry about this new mechanism, rather than reversing the change, Google added a way for users to deactivate the automatic sign-in. However, this was buried in an 'Advanced' settings menu.

23. Thus, it is clear that any focus on simply ensuring 'notice and choice' for consumers in data-driven markets will ignore the broader remit and potential

---

[16] C-673/17 *Planet49 GmbH*, Opinion of Advocate General Bobek, paras [97]-[99].

[17] "Guidelines on consent under Regulation 2016/679", Article 29 Working Party, 28 November 2017, p. 11.

impact of data protection law. The effective enforcement of principles such as purpose limitation by data protection authorities will have consequences for digital competition. If undertakings are actually required to have a separate legal basis for each data processing operation they undertaking, and this purpose must be legitimate and predictable, then this could lead to a 'soft' break-up of dominant digital firms. Prohibiting the unlawful conflation of personal data would force incumbents to compete in each new line of business on the merits alone, rather than to allow their strategic market position to cascade across markets as currently occurs. This is therefore a matter for regulatory co-operation, as we describe later.

24. Finally, it is worth reiterating that to the extent that data protection law does seek to facilitate individual control over personal data in the digital environment, the limits of such control are apparent to any user of the Internet. Dominant digital companies are alive to the threat of regulation, in particular in the aftermath of data scandals like Cambridge Analytica. The market has therefore responded to calls for individual control over personal data by introducing tools such as data dashboards. However, such tools over inadequate control.[18] Even if they provided consumers with robust control, this would only cover what 'frontstage'. However, what is happening backstage – such as the processing of personal data in the context of the real-time bidding process described below– remains impossible for users to control.

Data Glut: The Extraction of Excess Personal Data

25. Players with a position of market power in data-driven markets can use this position to extract quantities of data from individuals in excess of that which would be predicted or predictable by consumers, or might be considered a fair or reasonable exchange. This is both a competition law issue and a data protection issue.

26. It is a data protection issue in at least two ways. First, 'data minimisation' is a core principle of data protection. The GDPR provides that personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[19] This requires undertakings to store and process only the minimum quantity of data necessary for their purposes. At present,

[18] See for example Johnny Ryan, "Risks in IAB Europe's proposed consent mechanism", PageFair, 20 March 2018 (URL: https://pagefair.com/blog/2018/iab-europe-consent-problems/); and Johnny Ryan, "French regulator shows deep flaws in IAB's consent framework and RTB", Brave Insight, 20 November 2018 (https://brave.com/cnil-consent-rtb/).

[19] Article 5(1)(c) GDPR.

dominant companies are trying to have their cake and eat it. On the one hand they claim that the vast volume and variety of data they process is of little utility and does not itself confer a competitive advantage on them. On the other hand, if this data is not necessary for their commercial purposes, data protection regulators may query on what basis it is processed. In other words, it is unlikely that data lacks commercial utility for competition law purposes and can satisfy 'data minimisation' for data protection purposes.

27. A second way in which data protection law can examine the volume and variety of data extracted from an individual is when the performance of a contract is made conditional on the extraction of that data. An undertaking must have a legal basis or justification to engage in lawful data processing. If this justification is the performance of a contract, then the data processed must in fact be 'necessary' for the performance of this contract. Alternatively, if the legal justification is 'consent', but the contract will not be performed unless the individual consents to unnecessary processing, then it is likely this consent will not be 'freely given' and therefore lawful. It follows that in data protection law, it is crucial to consider whether the data processing is 'necessary'.

28. 'Necessity' in data protection law has been construed narrowly, in recognition of the power and information asymmetries between individuals and those who process their personal data. Courts and regulators have yet to issue decisive guidance on whether some data monetisation is appropriate in the context of contracts that are provided for 'free' at the point of access (such as Facebook's social networking service). The European Data Protection Supervisor highlights the limits imposed on such monetisation as a result of data protection's fundamental rights character .[20] An advisor to the Court of Justice has suggested that some monetisation is appropriate, noting however that this monetisation should be necessary for the performance of the contract.[21] However, even if such a transaction were to be authorised, the volume, variety and sensitivity of data derived from the usage of the 'free' services of dominant platforms is excessive. At a minimum, dominant companies should be required to lay bare to regulators how much data they process for a typical user, the value they derive from this data and how this relates to the cost of the service provision. Indeed, the transparency principle of the GDPR appears to require them to do this.[22]

---

[20] Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, European Data Protection Supervisor, 14 March 2017 (URL: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf).

[21] C-673/17 *Planet49 GmbH*, Opinion of Advocate General Bobek, para [99].

[22] Article 1(a) and Article 36 of the GDPR.

29. In addition, data protection law requires that processing be fair[23] and proportionate.[24] If the minimisation and necessity tests are failed, the fairness and proportionality tests are too.

30. An analogy might be drawn between the assessment required of data protection authorities in this context to determine how much data it is reasonable to extract from individuals in such circumstances and the assessments competition authorities make in excessive pricing cases. Indeed, this issue could be viewed from a competition perspective by querying whether excessive data collection whether directly or via third party trackers could constitute a form of excessive pricing.[25]

Theme 3 Competition in the supply of digital advertising in the UK

31. There are several market problems that disadvantage publishers and foreclose innovative entrants. First, cross-usage of data by dominant players creates barriers to entry to innovative market entrants. This is described in the discussion about theme 1, above.

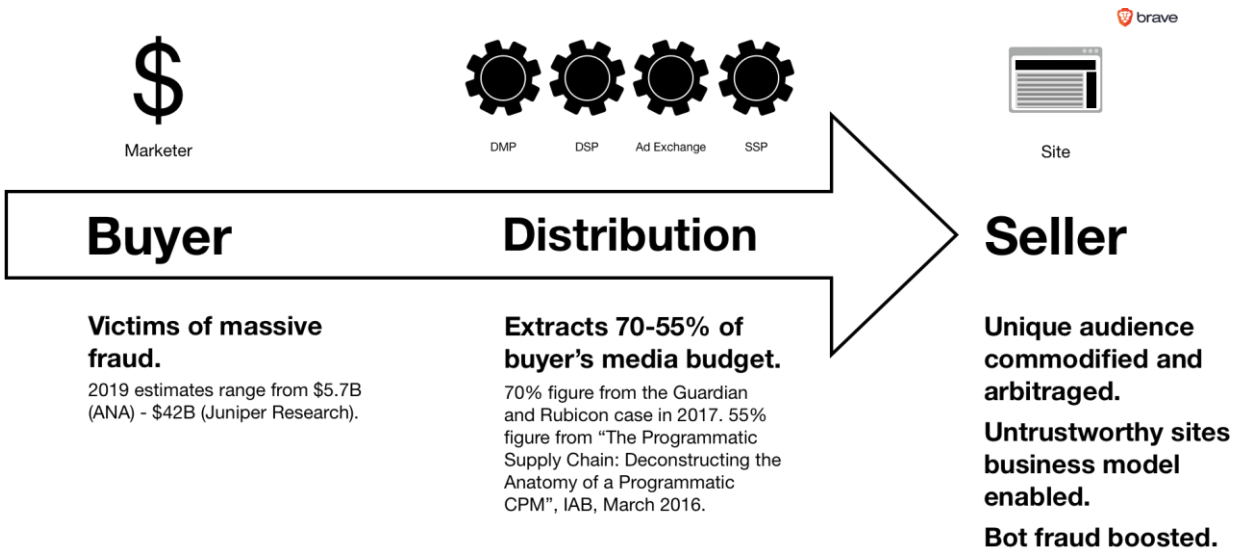
32. Second, monopsony/cartel practices in the "real-time bidding" online advertising market disadvantage publishers. Publishers lose their ability to monetize their unique audience, and pay enormous – and generally opaque – percentages to distribution intermediaries when selling ad space.

Overview of market problems in real-time bidding market

[23] Article 1(a) GDPR.

[24] For example, Article 9 (2) g, Article 35 (7) b, GDPR.

[25] Vicktoria H.S.E Robertson, 'Excessive Data Collection: Privacy Considerations in Abuse of Dominance in the Era of Big Data', Working Paper, June 2019.



In this market, publishers of websites and apps supply the online audience who view advertising. Marketers, who pay for advertisements to be shown to this audience, are the buyers. Advertising technology companies such as "real-time bidding ad exchanges" are the distributors.

33. We are concerned by the degree to which concentration in the adtech sector, which controls distribution, may have created a monopsony or cartel situation, where publishers who supply advertising views are compelled to do business with a small number of highly concentrated real-time bidding advertising exchanges and systems that purchase or facilitate the purchase of their advertising space, and dictate terms. The table below shows the scale, in numbers of transactions (bid requests) per day, of the seven largest RTB advertising exchanges.

RTB exchanges: bid requests per day

Ad Exchange name	**Bid requests per day**
Index Exchange	50 billion[26]
OpenX	60 billion[27]
Rubicon Project	Unknown (Claims to reach 1 billion people's devices[28])
PubMatic	70 billion[29]

[26] "Tour IX's Amsterdam and Frankfurt Data Centers", Index Exchange, 2 July 2918 (URL: https://www.indexexchange.com/tour-ix-amsterdam-frankfurt-data-centers/).
[27] "OpenX Ad Exchange", OpenX (URL: https://www.openx.com/uk_en/products/ad-exchange/).
[28] "Buyers", Rubicon Project, (URL: https://rubiconproject.com/buyers/).
[29] "How PubMatic Is Learning Machine Learning", PubMatic, 25 January 2019 (URL: https://pubmatic.com/blog/learning-machine-learning/)

Oath/AOL	90 billion[30]
AppNexus	131 billion[31]
Google DoubleClick	Unknown billions. DoubleClick is the dominant exchange. Google's DoubleClick/Authorized Buyers advertising system is active on 8.4 million websites.[32]

34. As the table shows, Google is by far the dominant participant in the market. We are concerned that publishers may be required to agree to practices such as the use of unique identifiers in RTB "bid requests" that enable companies that receive these to turn each publishers' unique audience into a commodity that can be targeted on cheaper sites and apps. In addition to the data protection implications of such practices, this strips a reputable publisher of their most essential asset.

35. We are also concerned about the degree to which "adtech" firms that control the distribution of the advertising slots supplied by web site publishers have distorted the market. 70%-55% of advertising revenue now goes to distribution "adtech" firms.[33]

36. Third, consumer harm is caused when advertising spending is diverted from content producing publishers to criminal fraudsters, the bottom of the web, and platforms that do not contribute content. The result appears to be a reduction in choice of quality content.

---

[30] "Maximize yield with Oath's publisher offerings", Oath, 3 April 2018 (URL: https://www.oath.com/insights/maximize-yield-with-oath-s-publisher-offerings/)

[31] "Transacting at a peak of 11.4 billion daily impressions, our marketplace handles more traffic each day than Visa, Nasdaq, and the NYSE combined" at https://www.appnexus.com/sell. Note that in 2017, AppNexus said in "AppNexus Scales with DriveScale", 2017, (URL: http://go.drivescale.com/rs/451-ESR-800/images/DRV_Case_Study_AppNexus-final.v1.pdf) that 10.7 billion "impressions transacted" came as a result of running 123 billion auctions. The impressions transacted to auctions ratio appears to be roughly 1:11.5. Therefore, the 11.4 daily impressions reported in 2018 equates to 131 billion auctions per day.

[32] DoubleClick.Net Usage Statistics, (URL: https://trends.builtwith.com/ads/DoubleClick.Net).

[33] 70% figure from the investigation by The Guardian, which purchased advertising on its own web site as a buyer, and received only 30% of its spend as a supplier. See "Where did the money go? Guardian buys its own ad inventory", Mediatel Newsline, 4 October 2016 (URL: https://mediatel.co.uk/newsline/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/). 55% figure from "The Programmatic Supply Chain: Deconstructing the Anatomy of a Programmatic CPM", IAB, March 2016 (URL: https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf).

37. Fourth, publishers of websites and apps have their audiences commodified and arbitraged on low-rent sites, and suffer further from the diversion of revenue away from their sites to fake sites by ad fraud scammers. This is described in a section below.

Lack of transparency & inefficiency: ad fraud

38. Because of the opacity of the online advertising market, advertisers do not know whether the people viewing their ads are humans or software "bots" masquerading as people to fraudulently extract money from the advertiser.

39. Juniper Research estimates that ad fraud will divert $42 billion of advertisers' spending to criminals in 2019, globally.[34] The US Association of National Advertisers estimates that at least $5.8 billion of their expenditure is wasted on ad fraud.[35]

40. Facebook 3 billion fake accounts in early 2019, and 1.3 billion fake accounts the year before.[36] (Facebook has only 2.4 billion users in a typical month). The enormous scale of the fraud problem makes it clear how inefficient the market is, and how little reporting received by a digital advertiser is reliable.

Lack of transparency & inefficiency: audience arbitrage

41. Recent research concluded that RTB increases publisher revenue by a mere 4 percent.[37] We believe that the reality is worse for publishers than this report suggests. This is because the study does not take account of two large costs that publishers bear: first, their audiences are commodified and arbitraged, and second, ad fraud diverts billions of dollars of advertising spending from their

---

[34] "The impact of AI for digital advertisers", Juniper Research, May 2019 (URL: https://www.juniperresearch.com/document-library/white-papers/the-impact-of-ai-for-digital-advertisers).

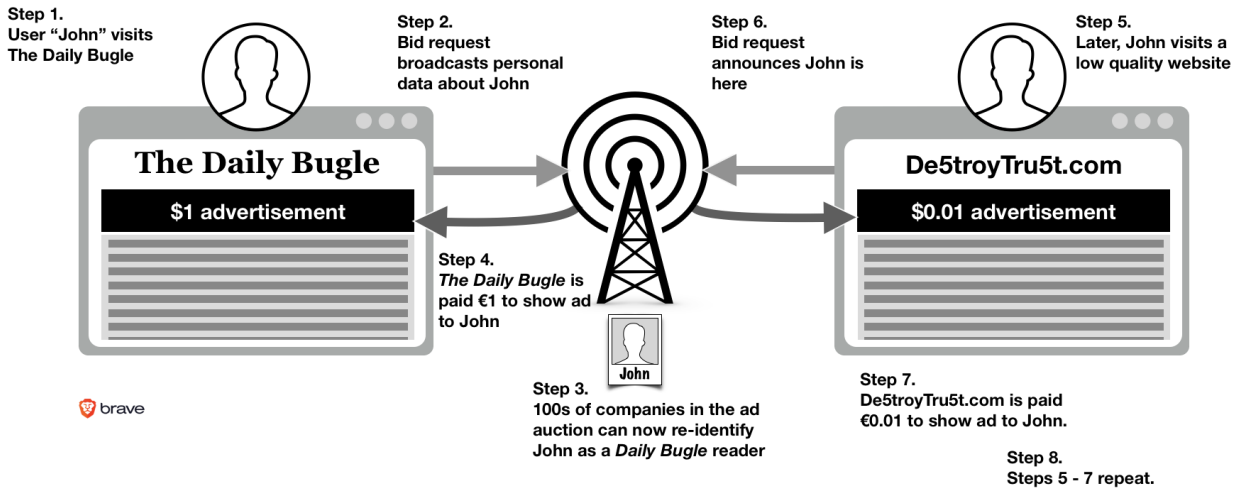
[35] "2018-2019 Bot baseline: fraud in digital advertising", Association of National Advertisers, 2019 (URL: https://www.ana.net/getfile/25093).

[36] "Facebook has disabled almost 1.3 billion fake accounts over the past six months", Recode, 15 May 2018 (URL: https://www.vox.com/2018/5/15/17349790/facebook-mark-zuckerberg-fake-accounts-content-policy-update); and "Facebook Removes 3 Billion Fake Accounts", Markets Insider, 23 May 2019 (URL: https://markets.businessinsider.com/news/stocks/facebook-removes-3-billion-fake-accounts-1028227191).

[37] FTC Hearing 6 – Nov. 6 Session 2 – The Economics of Big Data and Personal Information, FTC, 6 November 2018 (URL: https://www.ftc.gov/news-events/audio-video/video/ftc-hearing-6-nov-6-session-2-economics-big-data-personal-information).

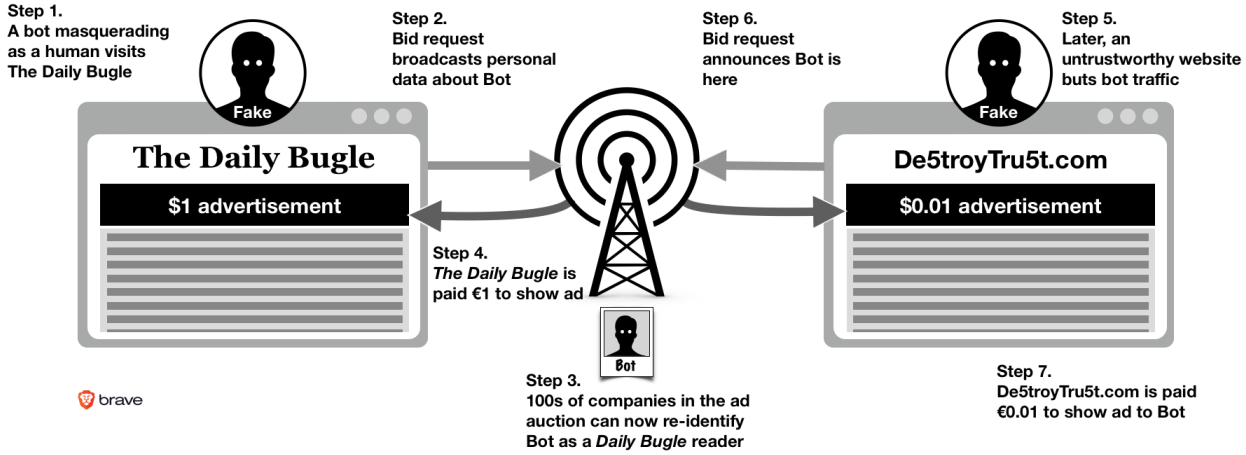
websites and in to the hands of criminals. The diagram below shows how these problems occur.

Audience arbitrage: how worthy publishers' audiences are commodified.



42. While *The Daily Bugle* may net £1 the first time this occurs, it finds itself undercut by De5troyTru5t.com thereafter. Thus, the online real-time bidding advertising system commodifies worthy publishers' unique audiences, and enables a business model for the bottom of the Web.

Example of an ad fraud scam: fake traffic bought by scam-publishers.



43. We believe that the current model of "broadcast behavioural" harms publishers. The way to solve this is to pressure the two standard-setting organizations that control the market: the IAB and Google, to remove personal data that enable audience arbitrage and much of the "bot fraud" problem from the system. This would also stop the real-time bidding from leakage of sensitive, profiling data about every single web user. Currently profiling data about web users is leaked

in hundreds of billions of broadcasts every day.[38]

44. Making this transition change at the industry standards level that affects everybody avoids individual companies facing a first mover disadvantage if they act alone. This is why it is essential that the relevant regulator acts to ban the broadcasting of personal data at the industry specification level, banning the IAB and Google from permitting personal data fields to be included in RTB bid requests.

45. We anticipate that a market in which all publishers make the same transition will yield far higher revenues to publishers. However, we also understand that for most publishers this is impossible to do alone. There is a first mover disadvantage, or prisoner's dilemma: one publisher is not able to make the first move on its own for fear that its competitors will not follow suit. It will then be at a market disadvantage in the short and medium term, and may not be able to enjoy the benefit of the transition to clean data in the long term.

46. The likelihood is that publishers can only enjoy this benefit if they move together. And this can only happen if the two IAB and Google real-time bidding industry standards is changed, causing the transition to apply to all publishers at the same moment.

An Institutional Perspective: Filling the Regulatory Gaps

47. There is the potential for competition law and policy in this area to be both internally and externally inconsistent. This internal inconsistency could, for instance, be claimed where – on the one hand – competition authorities permit data-driven acquisitions without imposing limits on the subsequent pooling of data across the merged entity while – on the other hand – later considering options to mitigate this data power through mechanisms such as data sharing.

48. There is also a danger of external inconsistency: for instance, it may be that both of these options, in fact, undermine individual control over personal data and undermine the legal framework for personal data processing. For instance, proposed data sharing or interoperability proposals would need to be closely examined in order to assess their compliance with purpose limitation. Moreover, even if the data sharing or interoperability served the same purpose, it may nevertheless be incompatible with the principle of fairness. A user may be happy

[38] "Bid request scale overview", submitted in evidence to the Irish Data Protection Commission, and UK Information Commissioner's Office, 20 February 20119 (URL: https://fixad.tech/wp-content/uploads/2019/02/4-appendix-on-market-saturation-of-the-systems.pdf).

to have their personal data processed by one provider for medical research purposes (eg the NHS) but not by another (eg. Google's Deepmind).

49. Competition law and data protection law should be working in tandem in digital markets, rather than pulling in opposite directions. Concrete proposals to facilitate such cooperation have been made by the European Data Protection Supervisor at EU level: such regulatory cooperation would also benefit the UK.

50. In particular, competition and data protection authorities should together consider whether there is adequate enforcement of the purpose limitation principle. Purpose specification protects a consumer's opportunity to choose what to opt-in to, and forbids a company from automatically opt-ing a person in to all of its services and tracking. The unfair conflation of data purposes, and cross-use of data, make it impossible for consumers to make informed choices, and expose sensitive information about them, such as their location and private browsing habits, that can disadvantage them in several important respects including fraud, invasion of privacy, disclosure of sensitive information about them in a breach or otherwise, erosion of trust, weakened bargaining position, manipulation, and ultimately a limit of the choice available to them in the market as a result of offensive leveraging of personal information.

51. A complex business that relies on data to operate can be analyzed by itemizing the following, for every data processing purpose: the specific purpose, the personal information it applies to, and the legal justification of the use of that personal information for that specific purpose. Provided a granular definition of purpose is adopted, this is a forensic method to build a detailed understanding of complex digital firms' operations. It also enables an examiner to determine whether the use of particular data for particular purposes is permissible, and if personal information is being cross-used and offensively leveraged. This is important, because the cross-use of data is a serious antitrust concern. Young, innovative companies can be snuffed by giant incumbents who erect barriers to entry by cross-using data for purposes beyond what they were initially collected for.

52. Regulators can correct anticompetitive data advantage without breaking up a company. By acting against unfair conflation of purposes that should be separate, data protection authorities can force incumbents to compete in each new line of business on the merits alone, rather than on the basis of leveraged data accrued by virtue of their dominance in other lines of business. For large digital firms with many distinct services, which may or tied or presented as a suite, this may be a powerful tool to prevent them from shutting down competition.

53. Finally, one may object that there is no scope for competition assessments in this regulated domain of activity. However, the jurisprudence of the Court of Justice of the EU indicates that where regulation leaves scope for discretion, there is scope for the application of the competition rules. It is in these grey areas of the regulatory framework that dominant firms are capitalising[39], rendering the additional oversight by competition and consumer protection authorities indispensable.

Conclusion

54. We are encouraged that the CMA has initiated this study, and believe that a market investigation is needed. We commend the CMA for its work so far, and are eager to support it in its future deliberations on this topic.

Faithfully

Dr Johnny Ryan FRHistS Dr Orla Lynksey

[39] For instance, when Richard Allan (a senior Facebook representative) was asked by International Grand Committee member Eamonn Ryan why Facebook had not implemented the 2011 recommendation of the Irish Data Protection Commissioner to end the possibility for application developers to access other people's data, he replied: The decision was taken, with the data protection team in Facebook Ireland and the broader company, to say, "Look, if we're not compelled to make this change, we will choose not to make it at this stage." Digital, Culture, Media and Sport International Grand Committee, Oral evidence: Disinformation and 'fake news', HC 363, Tuesday 27 November 2018, Q4177

Annex A

Survey overview

- The UK Information Commissioner's Office's survey, published in August 2018, reports that 53% of British adults are concerned about "online activity being tracked".

- In 2017, GFK was commissioned by IAB Europe (the AdTech industry's own trade body) to survey 11,000 people across the EU about their attitudes to online media and advertising. GFK reported that only "20% would be happy for their data to be shared with third parties for advertising purposes". This tallies closely with survey that GFK conducted in the United States in 2014, which found that "7 out of 10 Baby Boomers [born after 1969], and 8 out of 10 Pre-Boomers [born before 1969], distrust marketers and advertisers with their data".

- In 2016 a Eurobarometer survey of 26,526 people across the European Union found that:

  > "Six in ten (60%) respondents have already changed the privacy settings on their Internet browser and four in ten (40%) avoid certain websites because they are worried their online activities are monitored. Over one third (37%) use software that protects them from seeing online adverts and more than a quarter (27%) use software that prevents their online activities from being monitored".

- This corresponds with an earlier Eurobarometer survey of similar scale in 2011, which found that "70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected".

- The same concerns arise in the United States. In May 2015, the Pew Research Centre reported that:

  > "76% of [United States] adults say they are "not too confident" or "not at all confident" that records of their activity maintained by the online advertisers who place ads on the websites they visit will remain private and secure."

- In fact, respondents were the least confident in online advertising industry keeping personal data about them private than any other category of data processor, including social media platforms, search engines, and credit card companies. 50% said that no information should be shared with "online advertisers".

- In a succession of surveys, large majorities express concern about ad tech. The UK's Royal Statistical Society published research on trust in data and attitudes toward data use and data sharing in 2014, and found that:

    > "the public showed very little support for "online retailers looking at your past pages and sending you targeted advertisements", which 71% said should not happen".

- Similar results have appeared in the marketing industry's own research. RazorFish, an advertising agency, conducted a study of 1,500 people in the UK, US, China, and Brazil, in 2014 and found that 77% of respondents thought it was an invasion of privacy when advertising targeted them on mobile.