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

12 February 2020

Response to consultation regarding "online platforms and digital advertising"

1. I write on behalf of Brave, the private web browser. This submission follows the submission from Dr Ryan and Dr Lynskey of 30 July 2019, to the CMA's Online platforms and digital advertising market study statement of scope.

2. This submission makes two recommendations for the CMA's consideration. These actions are absent from the CMA's interim report of December 2019.

   - First, we recommend that a consumer-led functional separation of digital platforms should be carefully considered.
   - Second, we caution that a functional "real-time bidding" (RTB) market requires two dimensions for enforcement: internal and external.

   We itemise specific recommendations for action in our conclusion.

I. Consumer-led functional separation of platforms.

The platforms' monopoly-sustaining internal data free-for-alls

3. Vertically integrated platforms operate an internal data free-for-all. The CMA notes in its interim report that:

   "Google and Facebook have a competitive advantage because they collect a large amount and variety of data types from their widely used consumer-facing services and their broad coverage of third-party sites and apps."[1]

4. In 2012 Google revealed that it was combining disparate sets of user data from across its business. European data protection authorities examined this and

[1] "Online platforms and digital advertising: Market study interim report", December 2019 (URL: https://assets.publishing.service.gov.uk/media/5df9ecc040f0b609402e2838/Appendix_E_The_role_of_data.pdf), Appendix E, paragraph 4(c).

described the "absence of any limit concerning the scope of the collection and the potential uses of the personal data. … [Google's] new Privacy Policy allows Google to combine almost any data from any services for any purposes".[2]

5. In 2019, the Bundeskartellamt used virtually identical language to describe how Facebook is "combining all data in a Facebook user account, practically without any restriction".[3]

6. The CMA makes similar observations about the combination and cross-use of personal data collected from disparate lines of business, including integrations with websites, apps, and operating systems, to advantage the vertically integrated platforms' advertising businesses.[4]

7. The CMA's interim report quotes an internal Google document that says "Google has more data, of more types, from more sources than anyone else".[5] The CMA rightly concludes that Google and Facebook's competitors are at a significant disadvantage because they do not have a comparable quantity and quality of data with which to perform advertising targeting:

   "Compared with Google and Facebook, we consider that other platforms' data and targeting capabilities are relatively limited to user data from their own services, and are extremely limited in their ability to collect data about consumers on third-parties' websites and apps and combine it with their own first-party data."[6]

8. Internal data free-for-alls raise several competition concerns: tying, bundling, excessive collection and use of valuable personal data, and offensive leveraging of personal data. The net effect is "platform envelopment"[7], entrenched dominant positions, reinforced barriers to entry, and exclusion of competitors.

Data protection law is inimical to internal data free-for-alls

9. The CMA's analysis incorrectly concludes vertically integrated platform's internal data free-for-alls are facilitated by the GDPR. The interim report suggests

[2] Article 29 Data Protection Working Party to Larry Page, 16 October 2012, pp 1-2.
[3] Andreas Mundt's statement in "Bundeskartellamt prohibits Facebook from combining user data from different sources", Bundeskartellamt, 7 February 2019 (URL: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html).
[4] "Online platforms and digital advertising: Market study interim report", Appendix E, paragraphs 34-35, 38, 40-41, 44, 47.
[5] Online platforms and digital advertising: Market study interim report", Appendix E, paragraph 50.
[6] "Online platforms and digital advertising: Market study interim report", Appendix E, paragraph 54.
[7] Thomas Eisenmann, Geoffrey Parker, and Marshall Van Alstyne, "Platform envelopment", working paper, Harvard Business School (URL: https://www.hbs.edu/faculty/Publication%20Files/07-104.pdf).

that companies that "offer a wide range of services [and] so can obtain consent only once, in contrast to a single service provider".[8]

10. Data protection law is inimical to internal data free-for-alls in vertically integrated platforms. Google and Facebook's data advantage arises from a lack of enforcement of data protection law by data protection authorities.

11. The bundling of consent in the manner described by the CMA infringes some or all of the GDPR requirements of transparency, fairness, accountability, and purpose limitation in data protection law.

12. Article 5(1)b states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes...".[9]

13. Recital 32 makes clear that consent should be granular, and not bundled: "…Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. …"[10]

14. Similarly, European data protection authorities state that:

> "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."[11]

15. Separate guidance from European data protection authorities make the point that a requests for consent under the GDPR are valid only if a person can foresee the purpose for which their data will be used: "A data subject should not be taken by surprise at the purpose of processing of their personal data".[12]

16. European courts have acted on this requirement that consent should be separate and specific.[13] The CMA interim report's statements about the bunding of consent

[8] paragraph 4.159, and 4.150-4.152. See also paragraph 4.143.
[9] The purpose limitation principle, Article 5(1)b of the GDPR.
[10] GDPR, Recital 32
[11] "Guidelines on consent under Regulation 2016/679", Article 29 Working Party, 10 April 2018, p. 10.
[12] "Guidelines on transparency under Regulation 2016/679", 11 April 2018, p. 24.
[13] Dutch-language Court of First Instance in Brussels, AR 2016/153/ A, Debeuckelaere v Facebook, 16 February 2018 (translated on 26 March 2018 by a sworn translator, acknowledged by the Court), p. 61. From the ruling: "'Specific' means that the expression of will must related to a specific instance

within vertically integrated platforms are therefore incorrect - unless data protection authorities fail to enforce the GDPR.

Consumer-led remedy

17. The GDPR contains the tools to establish a consumer-led remedy. Consumers will be able to functionally separate Google, for example, if data protection law is enforced in the following areas:

    a. purpose limitation, in GDPR Article 5(1)b;
    b. special category data, in GDPR Article 9; and
    c. ease of withdrawal, in GDPR Article 7.

<u>a. Purpose limitation</u>

18. Orla Lynksy and I wrote about the importance of purpose limitation in our submission to the CMA on its statement of scope for this study:

> "If undertakings are actually required to have a separate legal basis for each data processing operation they undertake, and this purpose must be legitimate and predictable, then this could lead to a 'soft' break-up of dominant digital firms."[14]

19. Preliminary analysis conducted by Brave indicates that Google has several hundred processing purposes that are conflated in a vast, internal data free-for-all. This is an infringement of Article 5(1)b, in addition to other GDPR principles. Google's internal data free-for-all should therefore be remedied by data protection enforcement.[15]

20. The Bundeskartellamt's Facebook decision of February 2019 goes some way in this direction. It refers to processing purposes, and requires the unbundling of data within the Facebook Group, though it focuses on the cross-use between subsidiaries of the Group rather than within subsidiaries too.[16] That Bundeskartellamt's Facebook decision is now before Germany's Federal Court, following suspension on appeal by Düsseldorf Higher Regional Court for reasons unrelated to the substance of these issues: the Bundeskartellamt may not have

---

or category of data processing and can thus not be obtained on the basis of a general authorisation for an open series of processing activities."

[14] paragraph 23, Ryan and Lynsky to CMA.

[15] Article 58 of the GDPR gives data protection authorities power to investigate companies' processing purposes.

[16] Purposes are explicitly mentioned in "Bundeskartellamt prohibits Facebook from combining user data from different sources Background information on the Bundeskartellamt's Facebook proceeding", Bundeskartellamt, 7 February 2019, p. 2 and 5.

provided an adequate justification for its action in antitrust law. However, if a data protection authority had enforced in the same way, but on grounds of data protection, it would have had a firm case in data protection law. In other words, Bundeskartellamt did exactly the right thing, but it may have presented the case using the wrong framing.

21. To reinforce a purpose limitation remedy against "privacy policy tying",[17] data protection authorities should also enforce two other requirements of EU data protection law: special category data and ease of withdrawal.

b. Special category data

22. Consent is not the only legal basis that Google claims. In many cases it appears that Google incorrectly categorises personal data to avoid the need to seek explicit consent.

23. Much of the personal data that Google combines and cross-uses is likely to be "special category data", the use of which is particularly protected in EU data protection law. The GDPR defines special category data as:

> "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[18]

The word "revealing" makes clear that this covers inferences drawn from the data.

24. Google can only process special category data if it has the "explicit consent" of the person concerned,[19] unless the data have been made public by the person concerned.[20] Enforcing the correct categorisation of data as special category data would stop Google from continuing to unlawfully use personal data for any purpose without asking for proper consent.

25. While enforcement of purpose limitation would stop Google from automatically combining and cross-using personal data, the accompanying enforcement of

[17] Daniele Condorelli and Jorge Padilla, "Harnessing Platform Envelopment Through Privacy Policy Tying", 14 December 2019 (URL: Condorelli, Daniele and Padilla, Jorge, Harnessing Platform Envelopment Through Privacy Policy Tying (December 14, 2019). Available at SSRN: https://ssrn.com/abstract=3504025 or http://dx.doi.org/10.2139/ssrn.3504025).
[18] GDPR, Article 9(1).
[19] GDPR, Article 9(2)a.
[20] GDPR, Article 9(2)e.

GDPR Article 9, which concerns special category data, would further stop Google from privacy policy tying.

c. Ease of withdrawal

26. EU data protection law now provides that "the data subject shall have the right to withdraw his or her consent at any time".[21] It also provides that "it shall be as easy to withdraw as to give consent".[22]

27. This is not currently enforced: it is far harder to withdraw one's consent from a vertically integrated platform than it is to give.[23]

28. The combination of purpose limitation, special category data, and ease of withdrawal is a consumer-led remedy. The advantage of vertically integrated platforms would be neutralised in two ways.

    a. First, consumers would not automatically be opted in to all services and offerings. As a result, each service would have to compete for users' data on its own merits. The vertically integrated platforms would lose their internal data free-for-all, and the overwhelming data advantage that it has afforded them so far.

    b. Second, consumers will have the power to decide what parts of which companies are permitted to use their personal data for what specific purposes.

29. Therefore, the CMA should prevail upon the ICO to urgently begin the enforcement of purpose limitation, special category data, and ease of withdrawal. If the ICO fails to do so, the CMA should investigate whether it can enforce in these areas itself, applying the Bundeskartellamt's experience.

30. Purpose limitation is almost entirely absent from the CMA's interim report. It is only discussed in the main report in any substance within a footnote (footnote 223), and in two paragraphs (144-145) of appendix E. Purpose limitation is also absent from the Fuhrman Review, the UK Competition & Market Authority's interim report, and the European Commission Competition Directorate General's "Competition Policy for the Digital Era" report. These reports all focus instead on other data protection concepts such as interoperability and portability. This is a mistake.

[21] GDPR, Article 7(3).
[22] GDPR, Article 7(3).
[23] "Online platforms and digital advertising: Market study interim report", paragraphs 4.109-4.110, 4.113, 4.124-1.127.

II. A functional "real-time bidding" (RTB) market requires two dimensions for enforcement: internal and external.

31. The CMA's interim report expresses a concern that robust enforcement of EU data protection law in the real-time bidding online advertising market would advantage Google.[24]

32. The CMA is incorrect in taking this view for two reasons.

    A. Google's hypothetical advantage would only be possible if the ICO enforces against the externaldata free-for-all among RTB companies, but does not enforce against Google's internaldata free-for-all;
    B. The external data free-for-all makes the RTB market dysfunctional and harmful;
    C. It may be possible to establish a better RTB market.

A. Google's hypothetical advantage would only be possible if the ICO enforces against the external data free-for-all among RTB companies, but does not enforce against Google's internal data free-for-all

33. From a competition perspective, the RTB market has two dimensions of data protection problems: external and internal.

EXTERNAL	INTERNAL
Data free-for-all among thousands of RTB companies. RTB bid request broadcasts are a massive, continuous data breach.	**Data free-for-all inside Google.** Tying, bundling, and combining and cross-using personal data internally gives an unfair ad targeting advantage.

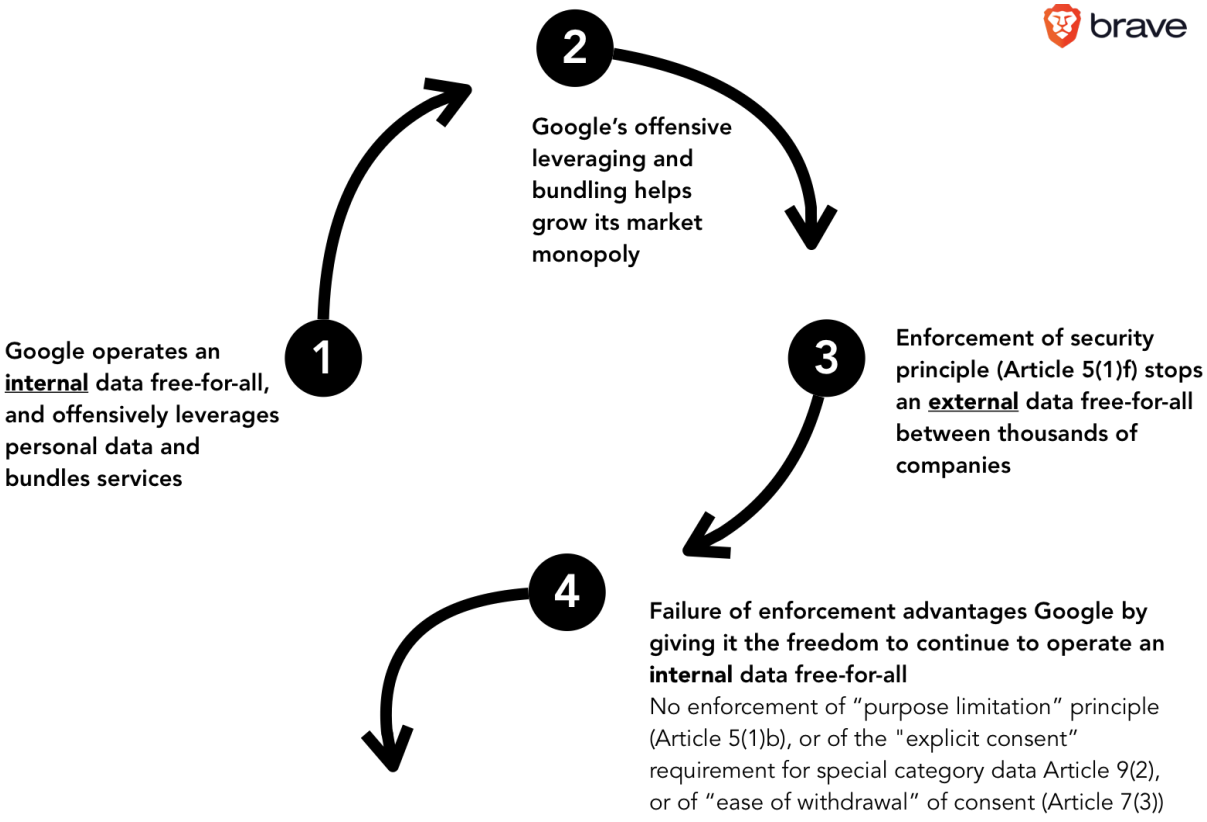
The CMA has considered only enforcement against external data protection infringements: Google's internaldata free-for-all would continue, while the

[24] "Online platforms and digital advertising: Market study interim report", paragraphs 4.150-4.152, 4.159. Also paragraph 5.228.

externaldata free-for-all involving thousands of RTB companies would end. This might allow Google to become an omni-DSP/SSP, wrapping the entire market within itself. This would end what the CMA believes is a vibrant and functional market.

34. The external data protection problem of RTB is that personal data are broadcast among thousands of companies, without security. This infringes Article 5(1)f, "security", of the GDPR. The issues have been raised before sixteen data protection authorities across the EU by Brave and its colleagues in formal GDPR complaints.[25]

Chart: Hypothetical scenario: external enforcement without internal enforcement.



35. However, this external dimension must not be considered in isolation. The remedy for the CMA's RTB hypothetical is the same as for the wider problem of data enabled monopolies: there should also be enforcement against Google's "internal" data free-for-all, which sustains this monopoly.

36. Indeed, irrespective of data protection authorities' enforcement in RTB, it is likely that Google's entrenchment will continue unless there is enforcement against Google's internaldata free-for-all. External enforcement to solve the vast RTB data breach may or may not merely accelerate this trend.

[25] See background at https://brave.com/rtb-updates/.

Chart: external and internal enforcement to address data protection problems and correct the market.

EXTERNAL	INTERNAL
Enforce GDPR Article 5(1)f ("security") against data free-for-all among all companies in the RTB market.	**Enforce GDPR Article 5(1)b ("purpose limitation") against data free-for-all inside Google. Also enforce Article 9(2) requirement for "explicit consent" for special category data, and Article 7(3) "ease of withdrawal"**

B. The external data free-for-all makes the RTB market dysfunctional and harmful

37. In a lawless market, it is inevitable that enforcement of the law may reward companies that can operate lawfully. This is analogous to the establishment of governance of the medical profession in the 19th century. One would not today lament the passing of the barber-surgeons of the middle ages. Practising medicine without a medical degree and a licence is illegal for good reason. It would not be reasonable or pragmatic for the CMA and the ICO to protect unlawful business practitioners in the open market merely because they may be unable to bring their business into compliance with the law.

i) Privacy harm

38. As Brave's evidence notes, Google RTB and IAB RTB systems broadcast what Internet users read, watch, and listen to online to thousands of companies, without protection of the data once broadcast.[26]

39. This data breach occurs hundreds of billions of times a day and can involve very sensitive information about people. As Brave recently reported, personal data about people seeking help for addiction, disability, and poverty on council websites across the UK is broadcast to thousands of companies in the RTB market.[27]

[26] See evidence at https://brave.com/rtb-evidence/.
[27] "Surveillance on UK council websites", Brave, 4 February 2020 (URL: https://brave.com/ukcouncilsreport/).

40. Once RTB data is broadcast to thousands of companies it becomes impossible to know or control how it will be used. The systematic data breach at the heart of RTB market exposes every person in the UK to mass profiling, and the attendant risks of manipulation and discrimination. These risks are profound. For example:

- An algorithm shortlisting job applicants may discriminate against a candidate,
- a product might be priced differently for a consumer, or
- a political issue campaign may micro-target a voter with disinformation.

41. The IAB and Google have no measures to remedy this. The recently released second version of the IAB's "transparency & consent framework" says only that the IAB "may adopt procedures for periodically reviewing and verifying a Vendor's[28] compliance".[29] In December, at the end of a six month grace period set by the ICO, the IAB merely proposed to establish an internal conversation about the problem, and provide non-binding suggestions to RTB companies.[30] Google's RTB system is no better, relying on self regulation on the part of the 2,000+ companies that receive its broadcasts.[31] Google has recently suggested that it may attempt to audit what these companies do with the trillions of personal data that it sends them, but in the absence of formal investigative powers this is an impossibility.

ii) Fraud

42. Aside from the data breach and the harms this directly causes, the RTB market is also dysfunctional. As the CMA notes, fraud[32] and opaque and high percentage fees[33] in the RTB market harms advertisers and legitimate publishers. We note that the fraud estimate in the CMAs interim report is rather lower than it ought to be.[34] The impact of ad fraud on legitimate publishers is not adequately

[28] "vendors" refers to the mass of companies that receive the data.
[29] Transparency & Consent Framework – Policies Version 2019-08-21.3, IAB Europe, p. 21.
[30] See analysis of IAB proposals at "Google and IAB's inadequate proposals to reform RTB", Brave Insights, 21 January 2020 (URL: https://brave.com/google-iab-reform/).
[31] "Authorized Buyers Program Guidelines", Google (URL: https://www.google.com/doubleclick/adxbuyer/guidelines/).
[32] "Online platforms and digital advertising: Market study interim report", paragraphs 5.127-5.130, 5.37, 5.122-5.135.
[33] As the CMA notes in "Online platforms and digital advertising: Market study interim report", paragraph 2.56, the estimates suggest that "intermediaries capture a significant portion of advertisers' expenditure". DSPs ranging from 8%-40%, and SSPs capturing 22%, paragraph 2.57.
[34] A useful range is $5.8B - $42B, using both "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

reflected. Business Insider discovered 25,000,000 fake ads offered (in a mere 15 minutes), using behavioural data to draw ad budgets away from Business Insider's genuine business.[35] As a result, Business Insider received less than $100 when an advertiser believed it had spent $40,000 to buy ads on BusinessInsider.com.

iii) Audience arbitrage

43. Also missing from the interim report is the harm of "audience arbitrage", in which legitimate publisher's audiences are commodified in the RTB system. This was a subject of my submission to the CMA with Orla Lynsksy,[36] and is a critical harm that should be evaluated.

44. Audience arbitrage allows a person identified on a high quality website to be targeted for advertising at a lower cost on a low quality website. The publisher of Recode explained how this works:

> "I was seated at a dinner next to a major advertising executive. He complimented me on our new site's quality... I asked him if that meant he'd be placing ads on our fledgling site. He said yes, he'd do that for a little while. And then, after the cookies he placed on Recode helped him to track our desirable audience around the web, his agency would begin removing the ads and placing them on cheaper sites our readers also happened to visit. In other words, our quality journalism was, to him, nothing more than a lead generator for target-rich readers, and would ultimately benefit sites that might care less about quality."[37]

By exposing their readers to third-party identification, publishers surrender the exclusive relationship with their audience.

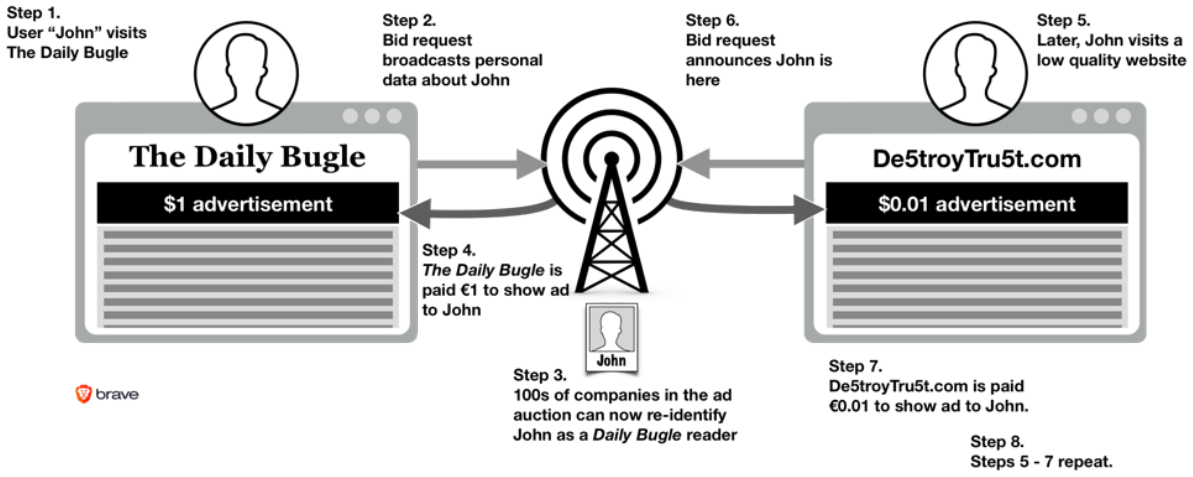
-advertisers) for a global estimate, and the lower figure from the Association of National Advertisers estimates that at least $5.8 billion of their spend is stolen by ad fraud, in "2018-2019 Bot baseline: fraud in digital advertising", Association of National Advertisers (URL: https://www.ana.net/getfile/25093). The divergence of these estimates demonstrates that authorities figures do not exist. The scale of ad fraud is large, but unquantified.

[35] See "Domain Spoofing Costs Business Insider 10M Fake Impressions -- in 15 Minutes," Adage, 30 October 2017 (URL: https://adage.com/article/digital/business-insider-york-times-shed-details-ad-industry-s-biggest-problem/311081)

[36] Ryan and Lynsky to CMA, paragraphs 41-42.

[37] "Mossberg: Lousy ads are ruining the online experience", The Verge, 30 January 2017 (URL: https://www.theverge.com/2017/1/18/14304276/walt-mossberg-online-ads-bad-business).

Chart: audience arbitrage



C. It may be possible to establish a better RTB market.

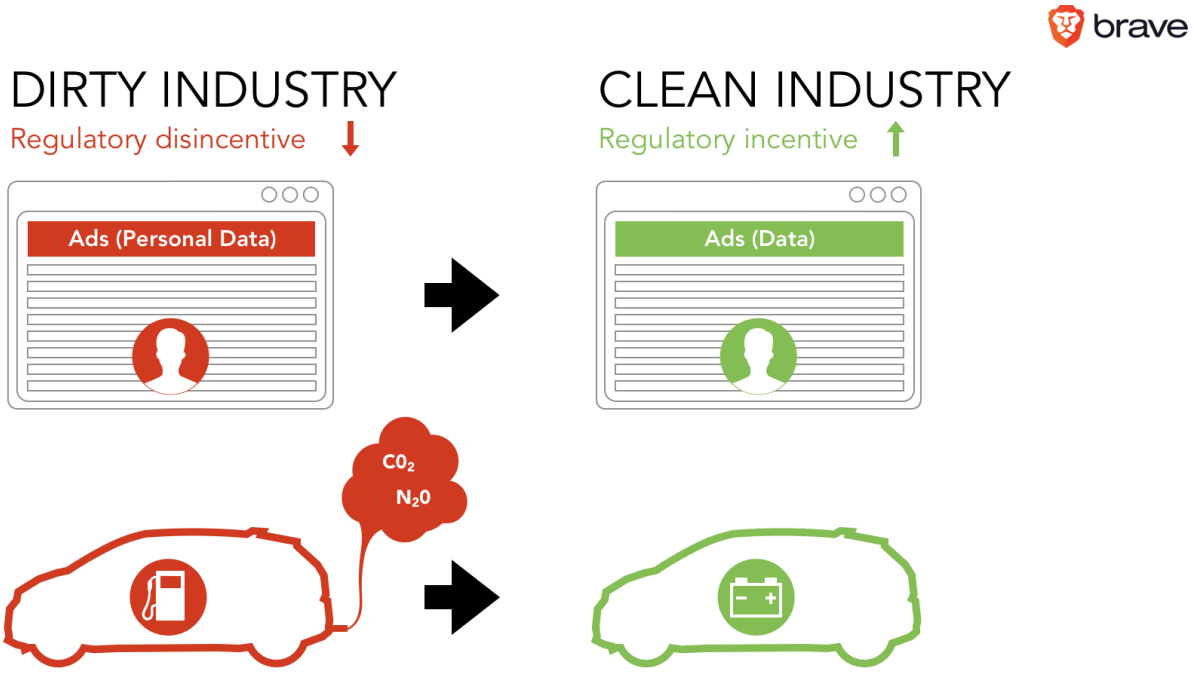
45. The broadcast of personal data is not necessary for ad targeting, frequency capping, measurement, and so forth, contrary to some statements in the CMA's interim report. Alternative methods have existed for some time to achieve this.[38]

46. Surprisingly, the interim report appears to lack a market scenario in which personal data are generally unavailable for advertising targeting (including to Facebook, Google, or any other players) as a result of both internal and external enforcement of EU data protection law.

47. It may well be that advertising targeted with personal data is more lucrative than advertising targeted with non-personal data today, though the revenue may go to intermediaries, rather than publishers. However this has little bearing on what the value of non-personal data will be in the market once data protection has been internally and externally enforced. (One would not walk into a car showroom today and compare the current price of electric cars to their petrol equivalents predict the value that electric vehicles will have after a carbon regulation is introduced.)

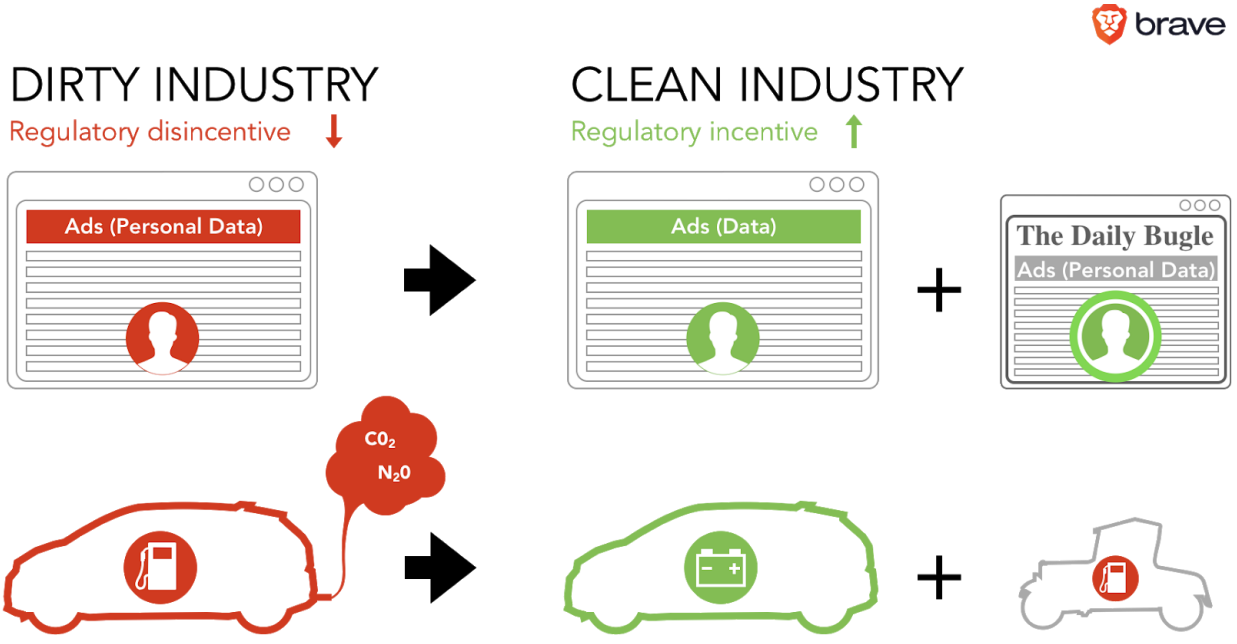
Image: The car showroom analogy of the future advertising data market

[38] See Sean Blachfield, "Frequency capping and ad campaign measurement under GDPR", 7 November 2017 (URL: https://www.linkedin.com/pulse/frequency-capping-ad-campaign-measurement-under-gdpr-sean-blanchfield/).



48. In a future open market where data protection enforcement against the external data free-for-all stops the broadcasting of personal data among a large number of market participants, the price of advertising targeted with non-personal data should rise if demand is reasonably consistent. In general, non-personal data would be the only available means of satisfying demand.

49. The same would be apply to "walled garden" platforms too if their internal data free-for-alls are addressed. Moreover, trusted publishers will be in a strong position to use first party personal data. This will allow them to operate a premium niche that may help sustain legitimate media.



Recommendations

50. Accordingly, we propose several recommendations for action by the Competition & Markets Authority. We invite the CMA to consider these, and to call upon us if Brave can contribute further to these deliberations.

    a. Purpose limitation as a means to address the platforms' monopoly-sustaining internaldata free-for-alls is not adequately discussed in the CMA's interim report. Platforms are bundling their services, and offensively leveraging personal data. This allows them to create a monopoly in the market. Enforcement of purpose limitation can allow the market of users to directly impose functional separation of platform's data. The CMA should examine this remedy in substantial detail. As the Bundeskartellamt Dusseldorf Court decision shows, this remedy is best applied under the auspices of data protection law, and presumably under the auspices of a data protection authority. Therefore, the CMA should discuss how the purpose limitation remedy should be applied with the ICO.

    b. The CMA should put the purpose limitation remedy on the agenda of its counterparts across the EU, who should use the EDPS Clearing House meeting in Spring 2020 to organise collaboration with their respective national data protection authorities.

    c. The CMA should also put the purpose limitation remedy on the agenda of the European Commission DG Competition and the Californian Department of Justice. It is significant that "purpose specification" is included in the Californian Attorney General's rulemaking on the California Consumer Protection Act (CCPA),[39] and will be also in the follow up legislation (CPRA) due for referendum in November 2020.[40]

    d. Contrary to its CMA's interim report's apparent call for caution in data protection enforcement against the externalRTB data free-for-all, [41] the CMA should instead prevail upon the ICO to act. The Information Commissioner has been reluctant to use her powers to enforce against the external data free-for-all in the RTB system. Enforcement of Article 5(1)f "security" is necessary to end the UK's largest ever data breach, and will also have positive market effects, correcting harms to legitimate publishers and to the UK

[39] CCPA, §999.305 (a)(3).
[40] CPREA, §3 (B)(2).
[41] "Online platforms and digital advertising: Market study interim report", paragraphs 4.150-4.152, 4.159. Also paragraph 5.228.

consumer.

e. The CMA should prevail upon the ICO to cooperate closely with the Irish and Belgian data protection authorities so that it can maximise the effectiveness of its enforcement against internal and externaldata free-for-alls in the digital advertising market.[42]

Faithfully

Dr Johnny Ryan FRHistS
Chief Policy & Industry Relations Officer
Brave

[42] The Irish Data Protection Commission is the lead authority under the GDPR for Google, and the Belgian Data Protection Commission is the lead authority under the GDPR for the IAB. It is Google and the IAB that control what data are permitted to be used in the RTB system. The "one stop shop" mechanism in the GDPR gives the ICO's Irish and Belgian counterparts the authority to develop the initial regulatory responses to the RTB system's external data free-for-all in the European market, which must then be confirmed by the European Data Protection Board.