Appendix Z: assessment of potential data-related interventions in digital advertising markets

Introduction

1. Many of the concerns we identified in digital advertising markets relate to data. In Chapter 8, we have summarised certain data-related interventions where we consider that the DMU should have the powers to intervene, if it finds that there are sufficient benefits to outweigh any costs of intervention.

2. In Appendix T we have summarised some criteria which have broad application across the assessment of data-related remedies. These criteria fall under the broad categories of:

   (a) efficiency;

   (b) privacy; and

   (c) competition.

3. In this appendix we provide more detail on our assessment of the data-related interventions in digital advertising markets summarised in Chapter 8 against these criteria. Although there is further work to do in this area, we highlight some particular examples of interventions where our assessment suggests that there is the strongest case for intervention against these criteria. As discussed in Chapter 10 of the report, we propose to consider some of these interventions further in joint work with the ICO following the completion of our study.

Data-related interventions

4. Consistent with our approach in Chapter 8, this appendix considers the following options for data-related interventions:

   (a) interventions to improve **transparency in the adtech supply chain**, particularly around fees and bid data for transaction identified by common transaction (or impression) IDs;

   (b) interventions to improve **transparency for ad verification**; and

   (c) interventions to address the advantages of SMS firms in access to data in targeting and attribution, including:

      (i) the **imposition of data silos,** either through regulation or through consent, using the concept of “purpose limitation”.

(ii) **mandated access to SMS firms' data for targeting and attribution**

(iii) measures to promote **data mobility**.

5. Finally, the appendix sets out some detail on our thinking on Personal Information Management Services (PIMS), a technology which could support some of the remedies designed to promote competition through more equal access to data, and in particular data mobility.

Data remedies – transparency in the adtech supply chain

6. Advertisers and publishers expressed a number of concerns about transparency within the adtech supply chain. As we discuss in Appendix M, the most notable of these are:

- Supply chain traceability/auditability – advertisers and publishers are typically unable to easily observe all the intermediaries that are involved in the buying and selling of inventory. Although they are aware of the parties that they contract with, they cannot always observe who these parties are transacting with. Many advertisers and publishers are also unable to access transaction-level data which they can use to effectively audit their supply chains.

- Fee transparency – there is a particular concern amongst both publishers and advertisers about visibility of fees across the supply chain.

- Access to bidding data – publishers have particular concerns related to their ability to observe who is bidding for their inventory and how much.

7. On the buy side, these issues make it difficult for advertisers to audit and manage their supply chains. For example, given that publishers decide which ad should be served based on bids net of SSP fees, visibility of these fees could make it easier for buyers to select the cheapest path to secure specific inventory and for DSPs to decide where to bid. The lack of transparency on the buy side over SSP fees can therefore affect buyers' decisions regarding which intermediaries to use and can have implications on competition between SSPs.

8. From a publisher perspective, one source of competitive pressure for intermediaries is the possibility of publishers signing direct deals with advertisers. Publishers would be in a better position to engage with advertisers if they knew which advertisers were interested in their inventory and to what extent they valued the inventory.

9. Greater transparency could also increase levels of confidence in the supply chain. One particular concern expressed by publishers in this regard is that intermediaries were taking high and unseen levels of fees and that this was reducing the revenue that publishers received from digital advertising.

Potential Remedies

10. We have identified three main options for improving transparency across the adtech supply chain:

- Within-contract fee transparency – whereby data on fees, at least at an aggregate level, are provided to contracted parties (eg an advertiser or media agency media agency would be able to see all fees levied by a DSP they have contracted with);
- Publication of average take rates and other fees and charges – whereby intermediaries publish their average fee or take rates;
- Provision of data, including fee data and bidding data, across the supply chain – whereby advertisers are able to have more transparency about what is happening on the sell side and publishers on the buy side. This could include sharing of aggerated data relating to individual advertisers' and publishers' transaction fees or sharing of non-aggregated impression-level bidding data with advertisers and publishers (which may necessitate the adoption of some form of common identifier such as a common transaction or impression ID).

11. There was strong support amongst advertisers and publishers for the potential adtech transparency interventions identified in our interim report. For example, one publisher submitted that it 'strongly support[s] all of these [transparency] interventions', which it believes 'would address many of the concerns surrounding Google's present ability to charge hidden fees and manipulate auctions to secure a disproportionately large share of ad sales at prices which are artificially low for publishers.'

12. However, whilst most adtech intermediaries generally supported greater transparency and pointed to improvements in levels of transparency across the industry as well as to various industry initiatives,[1] some were wary of too much transparency. As we discuss further below, some intermediaries considered that some transparency remedies, especially with regard to fee

[1] For example in 2018 a number of leading exchange signed up to a number of principles for a better programmatic market place, including a number around transparency: https://rubiconproject.com/insights/thought-leadership/principles-better-programmatic-marketplace-open-letter-advertisers-publishers/.

data, could potentially increase costs for adtech intermediaries as well as potentially distort competition by encouraging a race to the bottom. In addition, there are some concerns that remedies that require the provision of more information by adtech intermediaries about fees and bidding data could breach client confidentiality and, if these remedies were to mandate a common transaction or impression ID, facilitate the identification of individual users.

Within-contract transparency

13. Within-contract fee transparency would involve the provision of data on fees, at least at an aggregate level, to contracted parties. For example, an advertiser or media agency would be able to see all fees levied by a DSP they have contracted with, and a publisher would have visibility over the fees levied by an SSP with whom it has contracted.

14. Within-contract fee transparency is already common amongst intermediaries. Historically, one major exception to this seems to be Google Ads, which provides very little information to contracted parties on the take-rate that it earns for adtech intermediation.[2] However, even where there is some level of within-contract transparency, is not clear that it always covers all relevant fees, commissions or other elements of an intermediary's margin, or that it is provided at a sufficient level of granularity to be useful.

Publication of average take rates and other fees and charges

15. This would require intermediaries to publish data on the average amount of expenditure they retain in the form of fees, charges and commissions. A number of intermediaries already publish average fees or take rates.[3] One SSP submits that '[t]echnically and legally, there are no obstacles preventing [one SSP] from providing such data [on average fee or take rates] where the appropriate consent has been obtained'.

Stakeholder views

16. Whilst most adtech intermediaries generally supported publication of average fee rates, some were wary of too much transparency. For example, one

---

[2] Google tells us that it 'discloses price (CPC) and performance (conversions), which enables advertisers to compare alternatives and make decisions effectively'. It does not however, reveal the Google Ads take rate. This has sparked concern, amongst publishers in particular, that Google Ads is able to extract 'hidden fees' – see Appendix R for more discussion of this. However. Google recently published a blog post with some analysis of the Google Ads take rate: Google Ad Manager How our display buying platforms share revenue with publishers.
[3] For example, Google does so in relation to it Ad Sense product (see https://support.google.com/adsense/answer/180195?hl=en-GB) and Xandr has in the past published its average SSP fees.

vertically integrated intermediary submitted that, if fee transparency were to become a regulatory requirement, the focus would likely shift to the specific percentages of underlying fees rather than on net revenue and overall benefit to the publisher.

Provision of data, including fee data, across the supply chain

17. Provision of data, including fee data, across the supply chain would require supply-side intermediaries sharing data with buy-side intermediaries (and in turn with advertisers) and buy-side intermediaries sharing data with supply-side intermediaries (and in turn with publishers). This could include sharing of aggerated data relating to individual advertisers' and publishers' transaction fees or sharing of non-aggregated impression-level bidding data with advertisers and publishers (which may necessitate the adoption of some form of common identifier such as a common transaction or impression ID).

18. If provision of transaction-level data were to be most useful to advertisers and publishers, then it is likely that some form of common identifier would be required – such as a common transaction or impression ID – which allowed the identification of all activity related to a specific impression. Such an ID would be unique to an individual impression and would be included in all data files and bid requests relating to that impression. A key finding of a recent study on adtech fees by ISBA/PWC was that standardisation was urgently required to facilitate data sharing and drive transparency.[4] However, the privacy implications of the introduction of a common impression ID would need to be carefully considered.

19. A number of intermediaries have initiatives in place to provide greater visibility across the supply chain:

    - Xandr told us it has spent the last few years accelerating its Trust & Transparency initiative, by which it has been updating its seller contracts to enable it to share the costs charged to publishers with marketers and agencies purchasing ad inventory through Xandr's SSP. So far Xandr has obtained permission to confidentially share this information from publishers corresponding to approximately 60% of inventory in the UK.

    - Similarly, Index Exchange discloses take rates to buyers on the exchange when it has permission to do so. It has permission in its contracts with publishers to disclose approximately 35% of its

[4] ISBA Programmatic Supply Chain Transparency Study (2019).

publisher partner's take rates. Index Exchange is working towards receiving permission to share more take rates including outside the scope of contractual negotiations with a goal of reaching 100% publisher take rate disclosure.

- Another initiative to increase fee transparency is MediaMath's SOURCE project.

20. Google does not provide transparency across the supply chain. Outside the case of Google Ads – where, as noted above, fee or take rate data is not made available – Google submits that the 'publisher knows the SSP fee, and the advertiser knows the DSP fee',[5] but not that advertisers or publishers can see fees charged on inventory across the supply chain even where Google provides both DSP and SSP services. Google submits that this is in part due to confidentiality of contractual business arrangements with third parties. However, if, for example, a publisher using Google Ad Manager and an advertiser using DV360 wished to determine the fee charged across the supply chain when the advertiser buys inventory from the publisher and both Google's DSP and SSP services are involved, and they are comfortable disclosing this information to each other, they can simply share their individual fees to determine the total fee.

Stakeholder views

21. Advertisers and publishers felt perhaps the most useful move towards improving transparency within the adtech supply chain would be greater provision of transaction-level data and, importantly, that data should be provided in a manner that allows them to relatively easily combine it to obtain an overall market view across the entire supply chain. Advertisers and publishers felt perhaps the most useful move towards improving transparency within the adtech supply chain would be greater provision of transaction-level data and, importantly, that data should be provided in a manner that allows them to relatively easily combine it to obtain an overall market view across the entire supply chain. One publisher submitted:

> [Advertising intermediaries] should be required to share non-aggregate impression-level and bidding data with publishers. Such data should include on a per-impression basis the bids from all participating exchanges (including from header bidding) and

[5] Google tells us that it 'discloses price (CPC) and performance (conversions), which enables advertisers to compare alternatives and make decisions effectively'. It does not however, reveal the Google Ads take rate. This has sparked concern amongst, publishers in particular, that Google Ads is able to extract 'hidden fees' – see Appendix R for more discussion of this.

> the ultimate price at which the impression is sold. Importantly, the different types of data should be shared in a format allowing publishers to combine them. Access to that information would allow publishers to better monitor whether the ad server conducts auctions fairly, as well as to optimize their monetization strategy e.g. by measuring the incremental revenue brought by header bidding demand partners. In addition, proper access to bidding data would be expected to increase fee transparency and help detect hidden fees.

22. One intermediary submitted that before introducing potentially intrusive and costly measures to introduce end-to-end transparency within the supply chain, measures should be taken to encourage advertisers and publishers to better manage their supply chain using the information that is currently available to them. The intermediary also cited previous transparency measures for which advertisers had supported and encouraged the introduction, but had then not utilised them sufficiently once intermediaries had made costly investments to bring them into force. One example, they cited was the IAB Gold Standard,[6] which was introduced at significant cost but had not resulted in advertisers directing more expenditure towards IAB Gold Standard certified intermediaries.

23. A number of DSPs submitted that the introduction of a common impression ID would improve the efficiency of the adtech supply chain, as it would allow them to identify duplicate bid request. Being able to identify duplicate bid requests would enable them to avoid bidding for the same inventory on multiple occasions.

24. Publishers also had a specific concern with the inability to match data provided to them in various files by Google. They argued the that data on revenue earned from impressions could not be matched with data on who was bidding for those impressions and how much they were bidding. One publisher submitted:

> Google has taken multiple steps that make it more difficult for advertisers and publishers to run their own independent experiments (e.g. removing ability to export data out of Google Ads Data Hub on the advertiser side and removal of time stamp variables in data transfer files on the publisher side).

[6] The IAB Gold Standard seeks to improve brand safety and reduce fraud, see: https://www.iabuk.com/goldstandard.

25. Google considers that impression (or transaction) IDs would raise privacy concerns. It submitted:

> Imposing consistent transaction IDs raises potential privacy concerns by allowing advisers to join Google's secure bid data with other information in a way that would allow individual users to be identified. It would also allow various market participants along the intermediation chain to 'pool' user data without user consent.[7]

26. In addition, specifically in relation to its provision of data transfer files, Google submitted:

> We are constantly exploring ways to make our data files as useful as possible. But some large advertisers are sensitive about the disclosure of their bidding activity behaviour in previous auctions and contractually restrict us from disclosing that data. And, as noted above, bid data can be joined to other information in a way that allows individual users to be identified. Any attempt to 'improve' the quality of bid data which publishers receive needs to be balanced against the interests of these other stakeholders.[8]

Our Assessment

Within-contract transparency

27. We would consider it to be good practice that data on fees charged by adtech intermediaries, at least at an aggregate level, is provided to contracted parties. This should include all charges and deductions by an intermediary, not just the headline fees. This within-contract reporting should also include, for example, any buy-side fees or profits from arbitrage (such as post-auction bid shading[9]) accruing to an intermediary.

28. Within-contract transparency should help advertisers and media agencies to compare fees across DSPs and direct business towards lower cost DSPs and also allow publishers to compare costs across SSPs. This should facilitate increasing competition amongst DSPs and SSP, potentially leading to lower overall levels of fees.

29. This data should be provided at a sufficiently granular level for contracting parties to be able to observe the relative cost of supply routes for different

---

[7] Google's response to our consultation on the Interim Report, paragraph 100.
[8] Google's response to our consultation on the Interim Report, paragraph 100.
[9] Such as a DSP reducing the bid that it sends to an exchange after it has held an auction to determine the winning bid amongst buyers on its platform and the price that the winning buyer should pay.

types of transaction. The reported fee data could, for example, be split by: service type (eg technology fee, managed service fee, etc); purchase channel (open auction, private auctions, programmatic direct deal, etc); and type of inventory (video/other) and device (mobile/desktop-laptop). This degree of granularity is necessary so advertisers and publishers can compare 'like with like', as certain supply routes may be better and cheaper for certain types of transactions but not for others.

30. However, within-contract transparency does not solve one of the key issues of concern for advertisers and publishers, which is that they do not have visibility of fees across the supply chain.

Publication of average take rates and other fees and charges

31. Our view is that a move towards more widespread publication of data on average fee or take rates would improve the level of confidence amongst market participants, given the significant level of concern raised about fee transparency by advertisers and publishers. It would also give advertisers and publishers a starting reference point for assessing the cost of open display advertising.

32. However, publication of data on average fee or take rates may not significantly improve market participants' ability to actively manage their supply chains. The data on average fee or take rates is likely to be too aggregated, not specific to the individual participants and not easily comparable across intermediaries.

33. Any future work to facilitate the publication of average adtech fee or take rate should look to make the data as comparable and as useful as possible. This may limit the usefulness of the publication of a single aggregate or headline figure; instead, publication of a slightly more disaggregated view of average adtech fees and charges along the dimensions discussed in the section on within-contract fee transparency above may be more beneficial.

Provision of data, including fee data, across the supply chain

34. One option to improve transparency across the supply chain would be for DSPs to provide data to SSPs on aggregated fees charged by them on inventory purchased from those SSPs and, conversely, for SSPs to provide data to DSPs on fees charged by them on inventory sold to those DSPs. So, for example, an SSP would provide a DSP with data on the aggregate fees, split by relevant categories such as inventory type and advertisers, charged by the individual SSP in relation to the advertising inventory purchased by the DSP. DSPs could then share the information with advertisers. This

information could help DSPs and advertisers better manage their supply chains by directing the purchase of inventory towards the lowest cost supply routes and facilitate competition amongst intermediaries.

35. Fees are agreed in contracts between the intermediaries and the contracting party (normally for a DSP the contracting party would be an advertiser and for an SSP it would be a publisher). To reveal these fees to parties on the other side of the supply chain, the intermediary needs the permission of the party with whom it is contracting. This could potentially be a barrier to the widespread provision of information on fees across the supply chain. However, we do not consider this needs to be an insurmountable barrier. In this context, an SSP submitted that data privacy and confidentiality obligations also need not prove an obstacle to providing greater fee transparency. We consider that SSPs should look to provide transparency of fees to DSPs and vice versa, and that this data should be shared with advertisers or publishers within the constraints of privacy and confidentially, as a matter of good business practice.

36. In general, we consider that provision of more detailed transaction-level data to advertisers and publishers in a format that can relatively easily be combined across different files and intermediaries, including data on fees and bidding data, could, in principle, be highly beneficial to the ability of DSPs and SSPs, and of advertisers and publishers, to manage their supply chains. Visibility of these fees could make it easier for buyers and sellers to select the cheapest path to secure specific inventory and have implications on competition between intermediaries and overall adtech fees. Publishers, on the other hand, would be in a better position to engage with advertisers if they knew which advertisers were interested in their inventory and to what extent they valued the inventory; this would also put competitive pressure on adtech intermediaries. Finally, a common impression ID would help DSPs with identifying duplicate bid requests.

37. We acknowledge that there may be some genuine issues around confidentiality and privacy, especially in relation to a common impression ID, which need to be considered in more detail before any specific remedies regarding the provision of more transaction-level data to advertisers and publishers can be recommended. In addition, the introduction of a common impression ID may be costly for intermediaries and more work needs to be undertaken to assess the benefits of introducing this against the costs of doing so. Finally, we will need to carefully assess the implications of transparency for risk of collusion, as increased transparency on fees and bidding data may improve market participants' ability to monitor others' behaviour and improve the stability of coordination.

38. Whilst it is not intended that a common impression ID would be a strong identifier on its own for users or their devices (ie the ID is for the impression rather than the user), we acknowledge that it may be possible to use a common impression ID together with other data to identify users. However, any incremental privacy risks from a common impression ID must be assessed against the current status quo, where strong identification of and pooling of data about some users (potentially without user consent) is already routinely achieved by using cookies and mobile advertising IDs. In our view, a common impression ID would not require cross-site tracking of users and it would not materially increase the risks to privacy relative to the current situation, although this assessment may change if proposed changes to third-party cookies and other limitations on cross-site tracking within the web standards community are successful.[10]

Conclusion on adtech supply chain transparency remedies

39. We would consider it to be good practice that data on fees charged by ad tech intermediaries, at least at an aggregate level, is provided to contracted parties.[11] **A provision to require within contract fee transparency should therefore, we conclude, be included within the code applying to Google.**

40. Our view is that a move to more widespread publication of data on average fee or take rates could help bring a degree of confidence to market participants and could provide them with a starting point for assessing the scale of ad tech fees. **Facilitating the publication of more average adtech fee data, in our view, would be an appropriate role for the DMU to take on.**

41. We conclude that given the potential for it to have significant benefits the **DMU should have the power to introduce an impression ID** but that further work would need to be undertaken by the DMU to assess the cost and benefits and the extent of any privacy risks.

Data remedies – transparency for ad verification

42. For there to be effective competition between suppliers of advertising inventory, advertisers need to be able to make informed choices about the

[10] See Appendix G for a discussion of identifiers, cookies and mobile advertising IDs, and current proposals to limit cross-site tracking.
[11] However, we note that this should include all charges and deductions by an intermediary, not just the headline fees. This within contract reporting should also include, for-example, any buy-side fees or profits from arbitrage accruing to an intermediary.

inventory that they buy. Otherwise there is a risk that advertisers are overpaying for advertising inventory or purchasing poor quality inventory.

43. We indicated in our interim report that we were considering the case for specific interventions to address the concerns that digital advertising markets do not work well because there is insufficient transparency for advertisers and publishers. One of the measures we put forward was a requirement to provide sufficient data to allow for effective ad verification analysis. We suggested that there could be a rule which specified what data should be provided, at least by SMS platforms, to improve trust in the information which is provided on the effectiveness of different forms of digital advertising.

44. As set out in Appendix O, assessing and evaluating the quality of digital advertising is a complex and challenging process which involves a number of different stages, including verification.

Verification

45. Verification involves checking the viewability of the advert and the context in which it was displayed for brand safety purposes. It also has a role to play in safeguarding against ad fraud.

Viewability

46. Verification of viewability involves the authentication of the placing of an advert on a website, how much of it was viewable and how long it was viewable for. The fact that an advert was viewable does not guarantee that an advert was seen by a consumer, only that the advert had the opportunity to be seen. Viewability levels are taken into account when determining what advertisers pay for impressions delivered. Viewability is also a useful metric for the owners of websites in that it provides feedback to help them optimise the layout of the website and page experiences to increase the viewability levels of their ads.

Brand Safety

47. Brand safety involves ensuring that an advert does not appear alongside inappropriate content or content that is not in keeping with an advertiser's brand value.

Ad Fraud

48. Verification also encompasses checking for fraudulent activity. For instance, it is possible to verify IP addresses and check whether they are proxies or data

centres which are generating bot traffic. If advertisers cannot be sure that the advertising inventory they are buying is authentic or that the agents they are trading with are legitimate, then that lack of transparency will lead to a lack of trust in digital advertising and undermine the functioning of digital advertising markets.

49. Verification technology is primarily used by advertisers and DSPs but can also be deployed by publishers to help them better monetize their inventory.

Nature of Concerns

50. Although both Google and Facebook work with a number of 'approved' third-party verification providers, they restrict access to the underlying data on the advertising inventory they own and operate. In contrast, other display advertising platforms reported that they do allow advertisers to use third-party service providers to carry out independent verification on their advertising inventory.

51. Given a number of incidents of mis-reporting[12] and concerns about brand safety issues[13] on Facebook and Google respectively, advertisers expressed the desire to carry out their own, independent assessments. Without access to the underlying raw data and the ability to have full independent verification, advertisers and media agencies have the perception that Google and Facebook have the freedom, in effect, to 'mark their own homework'.

52. By restricting full and independent verification of the inventory that they own, Facebook and Google have engineered a degree of opacity into the buying and selling of their own advertising inventory. Advertisers have to rely on information provided by Google and Facebook. This could weaken competition or potentially result in advertisers over-paying for the advertising inventory supplied by Google and Facebook relative to other sources of supply. The buying and selling of display advertising is a complex process so that introducing additional restrictions on access to data adds to the 'friction' in terms of evaluating market outcomes.

---

[12] Marketingland.com, 'FAQ: Everything Facebook has admitted about its measurement errors.'
[13] For instance, in 2017, it was reported that a number of large UK advertisers had pulled their advertising from YouTube in response to concerns that their adverts were being shown alongside videos promoting extremist and terror groups. Source: The Independent, Banks join queue of advertisers ditching Google over extremist YouTube videos.

Stakeholder views

53. Both Facebook and Google have argued that the way in which they compile data for the purposes of verification, eg on the viewability of impressions on their inventory, meets industry standards and is subject to external audit. Google also argued that its approach to ad verification is driven by its obligations under the GDPR.

54. In its response to our interim report, Facebook welcomed proposals to improve standards in third-party verification in order to enable advertisers to effectively measure the success of their campaigns across different advertising media, including online and offline channels. At the same time, it considered that it was already operating in line with or above many of our policy proposals. Facebook re-iterated its position that it engaged with over 40 third-party measurement companies and entities worldwide to provide advertisers with independent metrics and comparisons, as well as third parties who perform regular checks on Facebook's ad viewability and other attention metrics. It also re-iterated that its measurement of impressions for ads on Facebook News Feed and Instagram was accredited by the Media Rating Council[14] and that in relation to visibility, the Facebook service and Instagram were certified for the Internet Advertising Bureau's UK Gold Standard[15], the latter being an initiative designed to reduce ad fraud, improve the experience of digital advertising, and increase brand safety.

55. Although Google did not respond in detail to the specific proposal about improving transparency in relation to verification, it did support our desire to increase trust and transparency. It pointed out that it had been an early adopter of the IAB's ads.txt initiative to combat ad fraud. It argued that an important question for the remainder of the Study would have been to determine which specific information ought to be provided and why it is important for competition.

56. Google argued that some degree of informational asymmetry might be unavoidable, for example where sharing would undermine efforts to fight ad spam and harmful ads. It stated that its approach to ad verification attribution was driven by its obligations under the GDPR and that any initiative to improve the ability of third parties to measure the performance of their ads should not conflict with the requirements of data protection legislation.

---

[14] The Media Ratings Council is an industry-funded organization whose purpose is to review and accredit audience rating services within the media industry and secure a measurement service that is valid, reliable and effective. http://mediaratingcouncil.org/.

[15] The Internet Advertising Bureau (IAB UK) is the industry body for digital advertising. It comprises some 1,200 members including media owners, agencies and brands. https://www.iabuk.com/.

57. In general, responses from other stakeholders (advertisers, publishers and adtech intermediaries) that addressed our specific proposals agreed with the concerns we identified and there was support for the proposal that Google and Facebook should provide access to sufficient data to allow for effective third-party ad verification.

58. For instance, Oracle argued that Google should not prevent third parties from collecting data directly from its owned properties, such that third parties are not simply measuring Google's curated data but can provide independent measurement and verification services. Beeswax told us fragmentation of measurement across digital properties was a hindrance. It argued that Google should be forced to allow third-party measurement and verification unless it can demonstrate rationale as to why this is not applicable or causes an undue burden.

59. More generally, a number of responses also indicated that a common standard for viewability metrics would also then allow like-for-like comparisons across platforms.

60. There were few detailed comments in stakeholder responses on the issue of transparency and ad fraud – most responses focused on the other transparency issues set out above. The response from JICWEBS reiterated its role in setting rigorous, transparent and objective trading standards for digital advertising in areas of brand safety, ad fraud and the viewability of ads. It also referred to its partnership with the US Trust and Accountability Group, which was founded five years ago to combat online fraud and piracy.

61. There was no challenge to the view we set out in our interim report that ad fraud was acknowledged to be an industry-wide challenge and that as such it was an issue which required industry-wide solutions to address it.

Our Assessment

62. As set out above, verification is an important first step in a complex process by which advertisers are able to evaluate the quality and assess the effectiveness of the advertising inventory that they have purchased. Advertisers need to be able to assess the quality of the digital advertising they are buying and if they cannot do that, then that undermines the operation of effective competition in these markets. Given the history of mis-reporting and concerns about brand-safety in relation to Facebook and Google, it is important that advertisers are able to carry out verification for viewability and brand safety independently of Facebook and Google.

63. We understand that the data needed for verification for viewability involves information such as: the website on which the ad was served; whether the ad appeared on the screen; how much of the ad appeared on the screen; how long the ad appeared on the screen; and, if it was a video advert, whether the ad played, for how long it played, whether the sound was on etc. Similarly, for brand safety, the key information involves establishing which website an advert has been displayed on and what other content was on that website.

64. As a result, our view is that verification of viewability and brand safety does not necessarily need to involve the use of personal data.

65. We recognise that Google has argued that restricting third-party access both to its own targeting data and its own inventory (such as YouTube inventory) is the best way to maintain the privacy of user information and prevent it from being leaked to potentially malicious actors. However, as set out above verification for viewability and brand safety purposes should not need access to Google's targeting data.

66. Enabling third-party verification allows the performance of platforms to be properly evaluated and compared and this should help stimulate competition. In addition, as a matter of good business practice, it is important that advertisers should be able to verify that the inventory that they purchased has been delivered as contracted for, in particular in respect of viewability and brand safety.

67. As indicated above, ad fraud was generally acknowledged to be an industry-wide challenge and – at this stage - one that required industry-wide solutions to address it rather than regulatory intervention at this stage.

Conclusion on ad verification transparency

68. As a result, we recommend that Google and Facebook should give advertisers – or their agents – access to the tools or information necessary to carry out their own, independent verification for viewability and brand safety purposes of advertising purchased on the inventory owned and operated by Google and Facebook and that all sides work to secure the necessary contractual and consent arrangements to ensure that this is done in a way that is consistent with the requirements of GDPR. Since the concerns we have heard relate exclusively to Google and Facebook, we think that such a requirement should be implemented through the code.

Data remedies – access to data for targeting and attribution

69. We have found, for reasons that are explained in more detail in Chapters 3 and 5 and Appendices F, G and O, that user data is a source of market power for large platforms. The platforms are able to use data advantages both to entrench that market power and to leverage it into other markets.

70. In this section, we discuss remedies aimed at addressing the ability of Google and Facebook to leverage their market power through how they combine and use data across markets. In this study, we are particularly concerned about the use of data in digital advertising markets, although we expect that similar questions might arise in other markets where SMS firms are able to re-use data gathered from core user-facing activities. There are two approaches in which competitive advantages from sharing data could be addressed:

    (a) by applying rules which restrict sharing of data from markets where SMS firms have market power into more competitive adjacent markets, in order to promote competition in those adjacent markets; and

    (b) by applying rules which require SMS firms which share data from core markets into adjacent markets to also offer access to that data to third-party competitors, in order to promote competition in the adjacent markets.

71. Either of these remedy approaches could improve outcomes where the ability of SMS firms to share data obtained from user-facing markets is having a material adverse effect on competition in the adjacent markets. In this section we consider examples of digital advertising markets where stakeholders have told us that this is a particular concern, and discuss whether these remedies are likely to be appropriate.

72. The backdrop to interventions of this kind is the increasingly restrictive measures that browsers have taken to limit cross-site tracking, including Google's announcement that it intends to end support for third-party cookies by 2022. These are discussed in more detail in Appendix G. As set out in Chapter 5, these restrictions are likely to impact the digital advertising business model used by newspapers and other online publishers.

73. By contrast, large incumbent platforms with leading consumer-facing services like Google and Facebook are significantly less dependent on third-party cookies for delivery of high-performing targeted ads and continued advertising revenues, as they can continue to make use of targeting using first-party data and authenticated user data. This means that the adverse effects on

competition are likely to increase, unless alternative mechanisms for levelling the access to data between SMS platforms and their rivals are introduced.

74. In this section, we focus on two activities related to processing of data for commercial purposes that we have been told by many stakeholders are particularly important for the working of digital advertising markets, and where Google and Facebook have particular advantages:

(a) **Targeting and profiling.** The use of data for targeting of individuals for the purpose of maximising the value of digital advertising is a common characteristic of digital advertising markets, as discussed in Chapter 5 and Appendices F, G and M. In many cases, this data can be linked to an individual (ie it is personal data), particularly where different data on a particular user can be combined, for example location data and browsing data from different sessions, different contexts or devices. Google and Facebook have access to rich data sources for targeting and profiling.

(b) **Attribution.** The use of data for the purpose of effective attribution of conversion events to digital advertising spend is seen as essential to the willingness of advertisers to commit budget to digital advertising, as discussed in Appendices F and O. Currently, attribution involves matching of user interactions across multiple websites and apps where they may be exposed to ads, and linking this with their behaviour on the intended destination sites, apps, and in some cases, offline purchases. However, as detailed in Appendices M and O, Google and Facebook restrict advertisers and independent attribution providers' access to user-level ad exposure data on Google and Facebook's websites and apps, which prevents advertisers from using independent attribution providers to receive a unified view of campaign performance and to conduct multi-touch attribution, and makes it more difficult for advertisers to compare the performance of Google and Facebook's inventory and adtech services with those of independent rivals.

Stakeholder views on interventions for access to data for targeting and attribution

75. We noted in our interim report that Google currently has a competitive advantage over other platforms, publishers and adtech intermediaries in part because it had access to more data than any of its competitors, gathering data through its user-facing web services, Android, and its presence on many websites and app via advertising and analytics tags and SDKs.[16] We also

[16] Interim Report, Appendix M, paragraph 42.

noted that Facebook had access to significant volumes of user data, based on its own consumer-facing platform.[17]

76. The majority of our analysis in our interim report related to Google, due to its much larger position in intermediation in open display markets. We also noted that a number of concerns around the competitive advantage from access to user data were also relevant to competition across 'walled gardens' and publishers for advertising spend. Where that was the case, we expected that they might apply to both Google and Facebook.

77. We set out that under one potential approach Google could be required to either: a) provide access to relevant parts of its data around the actions of users which it gathered from its Google tags; or b) to allow rivals to access the relevant results or inferences about users that Google made using the underlying data.

78. We considered these options both for data used for targeting and for attribution. In principle, rivals would be able to use the information supplied to provide a more comparable service in respect of the performance of their digital advertising products.[18] We noted that some stakeholders had called for this form of data openness or access.

79. We noted that this form of mandated access to data would require careful design. It may involve establishing a price for the access that reflected the economic cost of the data to Google. It was likely that it would require some form of operational separation or accounting separation to ensure that a separate analytics business provided a comparable service to Google's own business and third parties.[19]

80. We stated that granting access to user data was likely to pose privacy concerns.[20] In nearly all cases, the data required for targeting and attribution are likely to include personal data.

81. We invited views as to whether mandating access to targeting and analytics data would be an effective intervention to promote competition in digital advertising services.[21]

---

[17] Interim Report, Appendix M, paragraph 43.
[18] Interim Report, Appendix M, paragraph 44.
[19] Interim Report, Appendix M, paragraph 45.
[20] Interim Report, Appendix M, paragraph 46.
[21] Interim Report, Appendix M, paragraph 47 and paragraph 48.

Stakeholder views against interventions

82. Google did not agree that any remedies requiring access to data were appropriate. Google told us that it was not the only platform with access to user data; for example, Facebook and Amazon have extensive user data that could be used for targeting purposes.

83. Regarding the potential intervention to mandate access to its analytics data, Google explained that there were privacy limitations on its ability to share data that it gathered from advertisers and publishers through its analytics tools. Google also noted that in most cases it was not in the legal position to share analytics data with either third parties or other Google services.

84. Google said that sharing data gathered from Google tags, including those associated with Google Analytics, raised serious privacy concerns as it exposes user data to all adtech recipients of the data.

Stakeholder views in favour of access to data for targeting

85. Some publishers and intermediaries supported opening access to Google's data. Oracle, Verizon Media and Beeswax provided examples of data which could be subject to access requirements and which would improve competition for digital advertising based on data for targeting. Potential types of data raised by these submissions included location data, where Google has an unmatchable advantage due to its position in search and Android.

86. Oracle told us that any data interventions should cover all data collected through any of Google's tracking technologies. Even in the most far-reaching scenario that we identified (ie a scenario in which competitors could gain access to data collected by Google tags and to data used for targeting purposes) Google would continue to have a competitive advantage from its access to all data in its possession, such as that from Android, whereas competitors would only have access to subsets of it. In particular, Oracle emphasised that value of location data to advertisers that Google has access to via Android. Advertisers would therefore continue to find it easier to turn to Google's one-stop-shop.

87. Oracle observed that we thought that such remedies would involve establishing a price for the access to the data that reflects the economic cost of the data to Google. That premise assumed, however, that the data belonged to Google whereas, in fact, it belonged to consumers. Google, in Oracle's view, should not be compensated for access to data that was not its data to begin with.

88. Oracle submitted that any (valid) concerns regarding privacy should be remediable, including providing access to data used for targeting purposes. Although it might prove challenging to ensure sufficient anonymisation of data before it being made available to third parties, that should not prevent us from addressing the competition concerns we had identified.[22]

89. Beeswax, a DSP, told us that Google had an advantage from the data it collected from its consumer products. Beeswax encouraged us to either make that data available to DSPs or make Google price its DSP services to advertisers at a market rate that reflected the use of that data.[23]

90. News UK told us that it was in favour of opening up access to Google's user data. It suggested that such a remedy should take the form of opening up targeting data to independent data management platforms (DMPs) such as Permutive, Lotame, Salesforce DMP and so on. That would allow publishers to target their audiences without having direct access to Google's data, but also without tying the data to a specific Google product.[24]

91. Verizon Media added that we ought to also recognise that search advertising data was useful to advertisers as a source of purchase intent. That, Verizon Media explained, made it some of the most valuable data in the advertising market as a whole.[25]

92. The Computer and Communications Industry Association (CCIA), an industry group which all the Big Tech firms are members of, told us that when discussing data we needed to systematically distinguish pre-existing data and data generated from use of the platform.[26]

Stakeholder views in favour of access to data for attribution

93. In respect of attribution, intermediaries and publishers also considered that an access remedy would be appropriate. Some stakeholders, including Oracle and Guardian Media Group, considered that access to the underlying data to allow third party attribution and measurement would be most appropriate, to allow an independent assessment of Google's reporting. Others, including DMG Media, supported access to Google's own attribution services.

---

[22] Oracle's response to our consultation on the Interim Report.
[23] Beeswax's response to our consultation on the Interim Report.
[24] News UK's response to our consultation on the Interim Report.
[25] Verizon Media's response to our consultation on the Interim Report.
[26] CCIA's response to our consultation on the Interim Report.

94. The Guardian Media Group told us that access to the underlying attribution data would be preferable to access to an interpretation of that data, enabling it to generate its own analysis based on the that data.[27]

95. Oracle, which owns verification firm Moat, told us that we should require Google to provide sufficient data to allow for effective ad verification and attribution analysis. Rather than aggregated data or insights, Google should, Oracle explained, make raw data available to advertisers or publishers such that they can reach their own conclusions as to the effectiveness of their ad campaigns. In addition, third parties should be able to collect the relevant data from Google properties directly, rather than simply measuring Google's curated data.[28]

96. Beeswax, a DSP, told us that its advertiser customers were able to deploy its tags for the purposes of measuring conversions without undue burden. Beeswax told us fragmentation of measurement was a hindrance and Google should be forced to allow third parties to measure and verify ads on its sites.[29]

97. DMG Media strongly supported mandating access to Google's attribution service, stating that with its user ID across Google products and sites Google was able to obtain a full picture of the user journey.[30]

98. The Telegraph Media Group told us that any proposal that involved removal of the underlying data would impact its ability to independently undertake analytics, fraud prevention, measurement etc. For publishers and advertisers, The Telegraph Media Group explained, data about their own readers, audiences and customers was central to their respective businesses. They should be able to choose independent intermediaries to serve their audiences without relying on Google's attributions.

99. News UK told us that the priority was that any future cookie replacement should allow third-party technology to offer attribution technologies on a level playing-field with Google.[31]

100. Verizon Media asked that we recognise there is a role for legitimate interests in permitting the use of personal data within programmatic advertising, for example when serving and measuring non-personalised ads, subject to a thorough analysis via a legitimate interests assessment.

---

[27] The Guardian Media Group's response to our consultation on the Interim Report.
[28] Oracle's response to our consultation on the Interim Report.
[29] Beeswax's response to our consultation on the Interim Report.
[30] DMG Media's response to our consultation on the Interim Report.
[31] News UK's response to our consultation on the Interim Report.

101. Verizon Media also questioned the interpretation being made by some DPAs regarding what constituted valid consent where users were required to give this in order for their personal data to be used within digital advertising. Some DPAs, Verizon Media explained, believed that consent under GDPR could not be freely given if users were prevented from accessing content in the event that they did not consent, as they believed users would be subject to detriment in such circumstances. Verizon Media, however, asked us to acknowledge that nothing in GDPR prohibited publishers offering non-personalised advertising, and processing the associated personal data, as a condition of accessing a publisher's content. There was, Verizon Media explained, only an upside for users that consented as they obtained valuable content for free. If publishers were unable to place any data-related conditions on access, regardless of how reasonable those conditions were, publishers might be forced to charge consumers for access as they would have no alternative means of monetising their content.

102. IAB UK told us that consistency of data and reporting for advertisers was important but it would be preferable to achieve that via changes to existing industry standards. Any new requirements for platforms to provide additional information should therefore, IAB UK explained, be preceded by an examination of existing standards.[32]

103. Arete Research told us that Apple's introduction of intelligent tracking prevention (ITP) within its Safari browser led to a rise in fraud as third-party attribution firms were no longer able to utilise their (third-party) cookies.[33]

Stakeholder views in favour of data separation, enforcing stricter purpose limitation, and restricting the use of personal data in digital advertising

104. Other stakeholders considered that a more appropriate intervention to address Google's data advantages would be to limit Google's ability to share data between its different businesses. Brave, which is challenging Google's internal sharing of data,[34] supported a restriction on how Google is able to use its own data for personalised advertising. Other stakeholders including Guardian Media Group, Arete Research and Which? raised concerns about the sharing of data within Google and Facebook, and suggested approaches to limiting the use and re-use of data gathered for other purposes.

105. Oracle stated that Google should be prevented from making users' access to its dominant services conditional on extensive collection and combining of

---

[32] IAB UK's response to our consultation on the Interim Report.
[33] Arete Research's response to our consultation on the Interim Report.
[34] Described at https://brave.com/google-internal-data-free-for-all/

users' data, including third-party websites and apps using Google's ads services. In Oracle's view, Google coerced users to accept invasive data collection tactics, and preventing this would make competition in open display fairer.

106. Arete Research told us we needed to also focus on the sharing of data from distinct services within Big tech firms. Some platforms, Arete Research explained, had the ability to influence auction outcomes, since their aggregation of datasets allowed them a massive information asymmetry with smaller buyers or publishers. We should therefore be looking to restrict the opportunities of large platforms to exercise arbitrage, whereby they had an information asymmetry between what platforms see about the overall demand for inventory (ie on the buy side), and their ability to decide where to satisfy that demand (ie on the sell side), either with their own inventory or with that of third parties. For example, Arete said that Google was able to utilise exchange level data from AdX (ie AdX could see the bids from other DSPs and use that information to benefit its own DSP) to run more efficient auctions.[35]

107. The Guardian Media Group told us that enforcing key tenets of GDPR on Google and Facebook so that they didn't pool data about consumers from their different services and across third-party websites and apps to offer targeted advertising would create a more level playing field with the wider digital economy.[36]

108. Brave told us that another approach could be adopted to address the concerns we had raised. Instead of mandating access to data it stated that that there should be a ban on the broadcast of personal data within digital advertising. Brave explained that, contrary to some statements in our interim report, such data was not necessary for ad targeting, frequency capping, measurement, and so forth. Alternative methods had existed for some time to achieve that.[37]

109. Privacy International noted that the dominant players already held vast amounts of personal data across multiple services, and even then, they still seemed to be in a constant mission for more. It told us that it, however, seriously questioned whether any data-sharing (third-party access) remedies could ever adhere to strict data protection laws, even if effectively pseudonymised.[38]

---

[35] Arete Research's response to our consultation on the Interim Report.
[36] The Guardian Media Group's response to our consultation on the Interim Report.
[37] Brave's response to our consultation on the Interim Report.
[38] Privacy International's response to our consultation on the Interim Report.

110. Which? told us that consumers are likely to feel differently about the use of data collected in a first-party context and data collected in a third-party context. Any additional measures to enable competition by sharing consumers' personal data between multiple firms must, Which? submitted, be implemented in a way that would not result in negative impacts for consumers by increasing data privacy or data security risks.[39]

Assessment of the case for an intervention to address Google and Facebook's data advantage

111. Our understanding of the nature and problems of Google and Facebook's data advantage over other platforms, publishers and adtech providers is set out in Chapter 5. Some of the potential harms arising from this are discussed in Chapter 6. We summarise the relevant points below.

Summary of potentially problematic behaviour

112. Personalised advertising is targeted using data and profiles deployed by platforms, DSPs and, in some cases, by publishers.

113. Google and Facebook collect a wide range of high-quality data from their leading consumer-facing services and from third-party websites and apps that they have a tracking presence on. They do this through the linking of user access to consumer-facing services with the agreement to allow the data to be re-used for at least some purposes associated with digital advertising. This enables them to offer highly targeted advertising to advertisers and publishers. Rival publishers and adtech providers do not have comparable access to data for targeting.

114. Also, through its control over the leading web browser (Chrome) and mobile OS (Android), Google can also influence standards (such as support for third-party cookies) that affect rivals' ability to collect and use targeting data (eg users' browsing behaviour).

115. On attribution, Google and Facebook prevent advertisers and independent third-party measurement and attribution providers from accessing user-level data about ad exposures and interactions on their 'walled garden' properties. As advertisers benefit from unified measurement of campaign effectiveness across all impressions on multiple publishers (multi-touch attribution, unique reach, frequency capping etc.), this puts pressure on advertisers to rely on Google or Facebook for all of its adtech and analytics services.

---

[39] Which?'s response to our consultation on the Interim Report.

Summary of potential harms

116. We expect that as a result of this behaviour, the effectiveness of competition within adtech intermediation and digital advertising would be harmed. There are fewer rival adtech providers to Google, and the rivals that have remained in the market are less able to compete. Advertisers and publishers have fewer choices, resulting in higher prices and worse service (eg transparency) in adtech.

117. This has knock-on effects, such as reduced viability and returns on investment in content by publishers, higher marketing spend by advertisers which may be passed on to end-consumers, and reduced entry and innovation by new firms that rely on digital advertising to attract customers or to monetise their service.

118. Reduced viability of publishers and other services/content providers reliant on digital advertising mean that Google and Facebook also face fewer competitors on user-facing services, which result in worse service, more privacy-invasive data processing, and less innovation.

119. Advertisers are inhibited in their ability to have independent measurement and compare the relative performance between ads on Google and Facebook's inventory with other publishers' inventory, and between Google's DSP and rival DSPs. This further weakens competition and raises switching costs in digital advertising and in adtech intermediation.

120. On privacy, the status quo also delivers poor outcomes for those users whose preferences differ from the default choices presented to them by platforms and publishers. Platforms, most notably Google and Facebook, have extensive access to user-level data on content which they are readily able to join up.

Evidence of harm

121. The analysis in Chapter 5 sets out how Google and Facebook's data advantages contribute to their market power in relation to search advertising and adtech (Google) and display advertising (Facebook). This market power is manifested through the high revenues paid by advertisers to these platforms and evidence of wider harms.

122. The evidence that these harms exist is illustrated by Google and Facebook's persistently high share in the digital advertising markets where they operate, and the strong growth in their total digital advertising revenues.

    For example:

(a) Google and Facebook have by far the largest market shares in digital advertising in their respective markets. Google has over 90% of the search advertising market. Facebook's owned and operated platform has [50-60]% of the display advertising market.

(b) Google's position for key parts of the adtech stack is very strong – its share of supply of publisher ad serving is greater than 90%.

(c) Google's DSPs have [50-60]% of the open display market, the number of competitors in open display advertising has been reducing and there has been limited entry in recent years, despite the aggregate growth in digital advertising

(d) the largest firms in digital advertising, of which Google and Facebook are by far the most significant, are growing significantly faster than other platforms and publishers. According to the latest IAB UK and PwC digital adspend report the top five firms' advertising revenues in 2019 grew multiple times faster than for the rest of the market, with average growth at 15%.[40]

123. In addition, across digital advertising markets over recent years, the level of entry has reduced, while the level of concentration has increased.

124. In relation to attribution, media agencies told us that they had to largely abandon their independent attribution modelling for campaigns when they lost access to Google's user level data.

Conclusion on the case for an intervention to address Google and Facebook's data advantage

125. While Google and Facebook's use of data may have benefits in enhancing the value of digital advertising they offer, there are adverse effects that result from their advantages in data. In the next section we consider potential options for addressing these adverse effects, and whether the benefits of these options would be expected to outweigh any costs.

Remedy options for addressing data advantages of SMS platforms in targeting

126. To address these concerns, we have identified three forms of intervention, all of which could improve competition in digital advertising markets by providing more equal access to data for targeting and attribution for integrated platforms on the one hand and non-integrated publishers and advertisers on the other.

---

[40] Ad spend 2019 The official measure of the size of the UK digital advertising market, IAB UK

However, they differ in terms of their potential implications for effective targeting and attribution, and in their implications for data protection and privacy. The interventions are:

(a) data separation (or data silo) interventions, either by direct regulation or via enforcement of purpose limitation;

(b) user ID and data access interventions; and

(c) data mobility interventions.

127. In practice, these options are not mutually exclusive as the DMU may choose to use different interventions in different circumstances.

128. We first give an overview of the possible different types of intervention. We then set out in more detail how we would envisage each of these options working in practice. Finally, we assess them having regard to appropriate criteria, including the those set out in Appendix T of efficiency, privacy and competition, as well as other considerations such as feasibility and effectiveness.

Data silos imposed via regulation

129. Under a data silos intervention, Google and Facebook would be restricted in how they shared and re-used the data they collected within a single SMS business, product, or market, where there was evidence that this would have an adverse effect on competition. Restrictions could encompass the sharing of data from the core user-facing services and/or the related digital advertising. A regulatory body (the DMU) would determine what the individual businesses each were and the scope of any restriction, including what data is restricted and what restrictions are placed on how the data is used.

130. In order for this remedy to work, the DMU would need to have the power to prevent data sharing by SMS firms where it concludes that the adverse effects on competition, harm to privacy and harm to efficiency outweigh any efficiency benefits. The power could be applied in a flexible manner, as it would allow the DMU to prioritise intervention where it considered that to the benefits would be greatest and would most clearly outweigh the costs.

131. Data silos would prevent Google and Facebook from sharing their data within their corporate group, where the DMU had assessed that that sharing either had a material impact on competition and that any benefits from sharing would be outweighed by the adverse effects from this impact on competition.

Assessment

- *Efficiency: static and dynamic (including effects on competition)*

132. Under data silos, less data overall would be shared within the ecosystems of Google and Facebook, leading to a reduction in the efficiency, both static and dynamic, with which these platforms served their advertiser customers, and therefore a reduction in the value of digital advertising offered by Google and Facebook.

133. In terms of the static reduction in efficiency, advertisers advertising via Google and Facebook might not be able to base their targeting on such granular profiles of users, and be forced to rely on immediate contextual data / information plus rough location. Advertisers may no longer be able to overlay either their own first party or Google's search 'intent' data onto user profiles to make targeting even more granular. Furthermore, advertisers might not be able to take advantage of Facebook's lookalike audience targeting capabilities.

134. There would be likely to be a greater effect on the efficiency of digital advertising for advertisers arising from a reduction in the user data need for attribution than that for targeting. Attribution and measurement are considered particularly important in justifying spend by advertisers on digital advertising, and therefore the level of investment by publishers and other platforms which rely on digital advertising to fund their businesses.

135. Both Google and Facebook would also face a dynamic reduction in efficiency to the extent that they would face a reduced incentive to invest in new services in the absence of the ability to share user data across services. Any reduction in digital advertising revenues accruing to Google and Facebook from existing services might also lead to a reduction in their ability to act on their incentives to invest.

136. In the longer term, data silos for Google and Facebook may give publishers, other platforms and competing intermediaries in open display an increased incentive to invest. As other firms would face a more level-playing field in terms of access to user data to monetise digital advertising inventory, data silo measures may enhance competition in digital advertising, which may improve other publishers and platforms' relative bargaining position, and possibly lead to an increase in revenues and return on investment, resulting in additional content and new services of value to users or the prevention of loss of currently available content and services. If so, data silos might lead to an increase in dynamic efficiency for these stakeholders, particularly where the

data that had been combined was gathered from publishers or advertisers through the exercise of market power.

137. The balance of efficiency losses that would likely be incurred by Google and Facebook would need to be weighed against the potential gain in dynamic efficiency on the part of publishers, other platforms and intermediaries.

- *Privacy*

138. The principal effect on privacy of imposing data silos would be positive, as there would be less sharing of data by the SMS platforms across different purposes and beyond the services where users directly engage with the platform.

139. This privacy benefit could be partially offset to the extent that data silos could represent a reduction in consumer control, if some customers preferred to have their data shared, for example in order to receive the most relevant digital advertising, and the imposition of data silos were to prevent this sharing, or make it much more difficult.[41]

140. However, it is more likely that the DMU would find, based on the existing evidence, that most users preferred less rather than more sharing of the relevant data[42], but found it difficult to implement their preferences within the platforms' choice architecture. If so, the intervention would better align outcomes with most consumers' preferences and enhance consumers' privacy.

- *Feasibility and effectiveness*

141. Under this intervention, the DMU would have the power to impose data silos, conditional on having established the harm deriving from SMS platforms' internal data sharing.

142. A risk to the effectiveness of this remedy would be if the DMU was unable to effectively enforce data silos. As discussed in Appendix E, Google and Facebook have wide ecosystems, and several routes exist by which data can be shared within their ecosystems. In order to implement a remedy which only restricted the sharing of data that had an overall adverse effect on consumers taking into account the trade-offs between efficiency, privacy and competition,

[41] It is likely that there would still be some ways for customers to express a willingness to have their data shared, for example to be consistent with GDPR data portability requirements.
[42] See Appendix L for a discussion of consumers' attitudes towards personalised advertising.

the DMU would need to have confidence that it could design a restriction that could be made effective within these complex ecosystems.

143. More generally, the DMU may face a challenge in coming to decisions when determining the scope of the products, services, or markets within which data silos are to be enforced. This is because the value of various benefits and costs considered under the heads of efficiency, privacy and competition are difficult to robustly measure individually, let alone in combination. There therefore might be a difficulty in assessing which data sharing practices were in fact sufficiently harmful to warrant a ban on sharing. Inevitably the assessment would involve the need by the DMU to exercise judgement in determining the scope and applicability of the series of restrictions that such a measure would entail.

144. For a data silos separation remedy to be effective, the DMU would need the power to monitor the internal separation of data by the SMS firms. This would include access to reporting by SMS firms on the flows of data within the firm and independent audit of the arrangements which SMS firms put in place to comply with the remedy.

Conclusion on data silos imposed via regulation

145. A data silos remedy should reduce some of the unmatchable advantages that Google and Facebook have, thereby resulting in more investment and innovation in digital advertising and the content and services financed by digital advertising more broadly.

146. The main risk to the effectiveness of the remedy in driving increased benefits to consumers would arise from any reduction in revenues earned by Google and Facebook stemming from the loss of use of any unique user data that led to a reduction in the value to users of the services they provided. This may have the greatest effect in respect to attribution data, as we understand that the ability to perform effective attribution is particularly important in promoting the use of digital advertising over other media.

Enforced purpose limitation

147. As discussed in Chapter 4 and Appendix G, Google and Facebook currently share data across activities within a common ecosystem. This practice is under review by the DPAs, and some parties such as Brave have suggested it is not consistent with GDPR.

148. Under this approach, regulators would mandate SMS firms to revise their legal bases for processing personal data, and to redesign their data

processing activities so that adequate purpose limitation is observed. We envisage that regulatory action may require SMS firms to use consent as the appropriate lawful basis for processing data to personalise advertising. Where relevant, the DMU could also require SMS firms to pre-submit proposed designs for consent flows and interfaces, so that these can be tested with users and to ensure that they comply with 'fairness by design' principles (outlined in Chapter 4 and Appendix Y), before being deployed for UK users with the regulator's approval. Regulators would ensure that, where consent is the appropriate lawful basis for data processing, consumers would be presented with a genuine choice, and that consents across multiple separate purposes or services are not inappropriately bundled together.

149. Under this remedy, a 'fair by design' consent flow may involve purpose limitation observed 'upfront' in the initial choice presented to consumers (instead of bundling consents across purposes and services upfront, and then offering settings and controls to users to adjust subsequently to opt out of personalised advertising). Purpose limitation would be monitored and enforced by the appropriate regulator.

150. As required by data protection law, the default arrangement will be that no data from user-facing services would be used for profiling and targeting of digital advertising. In the absence of valid user consent to do so, SMS firms will not be allowed to share data across different purposes and services within their ecosystem.

151. The effect of a requirement to obtain more granular consents for sharing of data within an ecosystem would depend on the design of the consent mechanism. More granular consents may result in more users choosing to limit SMS firms from sharing data from SMS user-facing services for use the delivery and measurement of digital advertising.

152. Under current legislation, we expect that the DMU and the ICO would need to work together with SMS firms to design and implement any appropriate separation of data.

Assessment

- *Static and dynamic efficiency (including effects on competition)*

153. We currently expect that if this remedy was implemented in the way envisaged by Brave and other stakeholders, then it would be likely to result in a significant reduction in the data shared by Google and Facebook from their user-facing businesses into digital advertising. There should therefore be

efficiency and competition effects which may be similar to the data silos approach described above.

154. To the extent that their users would not be prepared to share the data, then there would therefore potentially be a reduction in the effectiveness of targeting and attribution and a corresponding loss in the value of advertising. If so, Google and Facebook might have less incentive to invest in user-facing services. However, such losses would be the direct result of the freely expressed wishes of their users.

155. A transparent link between the granting of consent for use of user data for a particular purpose and the benefits of data sharing might could in principle promote competition based on the granting of consent for individual purposes. Competition for the use of user data between different user-facing services is currently played out at the level of the platform, so overall this could, if implemented effectively, increase the intensity of competition on the basis of privacy. This would need to be weighed against the increased burden on the consumer of additional consent requirements, potentially leading to consent fatigue.

156. A further point of difference with the approach of data silos imposed via regulation is that individual consumers may be expected to make decisions about SMS firms' processing of their personal data without taking into account the benefits and costs of their decisions on others and society in general (ie externalities), whereas a regulator is able to do so when designing data silos.

- *Privacy*

157. This remedy would increase the control that users had over the use of their user data. Those users who wish to share their data will be readily able to do so, albeit potentially through the process of granularly opting to a series of consent statements. Such a granular approach could also incentivise Google and Facebook to spell out more clearly the benefits to individual users of them giving consent for each purpose.

158. However, this remedy would place burdens on individual consumers to exercise their data protection rights effectively, and make granular decisions that they may not be well-placed to do so. We hope that these frictions could be minimised through appropriate design of the consent interfaces (in line with a 'Fairness by Design' duty on SMS firms), but it remains to be seen (ideally through user testing) whether the consumers are able and willing to meaningfully engage.

- *Feasibility and effectiveness*

159. A requirement to maintain purpose limitation over certain data would not be a complex intervention for a regulator with sufficient powers to implement. In practice the regulator would need to engage closely with the Google and Facebook to ensure that the relevant consent statements give the user effective control.

160. The DMU and/or the ICO would face a challenge in designing appropriately separate purposes. If purposes are too granular, this may increase the burden on users to make many choices, increasing the 'hassle costs' of using SMS services and resulting in 'consent fatigue'. Conversely, if purposes are defined too broadly, this may reduce the ambition and potential effectiveness of the intervention.

161. In principle, the case for which purposes should be subject to the intervention could be based on similar reasoning as for data silos imposed by regulation. The DMU could define and enforce separate purposes where the benefits of imposing separation would have a positive effect on competition and privacy that could outweigh any loss of efficiencies. As with the data silos remedy, we recognise that designing separate purposes would require the regulator to exercise judgement in determining the scope and applicability of the series of restrictions that such a measure would entail.

162. As for the data silos imposed by regulation remedy, for a purpose separation remedy to be effective, the DMU and/or the ICO would need the power to monitor the internal separation of data by the SMS firms. This would include access to reporting by SMS firms on the flows of data within the firm and independent audit of the arrangements which SMS firms put in place to comply with the remedy.

Conclusion on enforced purpose limitation

163. Overall such an intervention should level the playing field between the large platforms and rival platforms, publishers and intermediaries in open display. It would also give consumers greater control over how their data is used. The competitive effects should be broadly comparable to those under the option described above of data silos imposed by the DMU, except that there would be an added burden on consumers relative to the data silos intervention.

164. We discuss our proposals for further work with the ICO in Chapter 10.

Mandated data access interventions based on user ID

165. In this remedy, the DMU would require SMS firms, in this case Google and Facebook, to offer access to rivals in adjacent markets to specified data sources on an agreed basis, potentially without requiring users to make choices or give consent. This could take the form of access to relatively low-level, 'raw' observed data about their users, or to higher-level information derived by Google and Facebook (eg various characteristics about users or profiles). Either form of data access would allow third parties active in adjacent markets to compete more effectively in the market for display advertising. We note that this type of intervention, which we invited views on in our interim report, received strong support from a number of market participants.

166. This form of intervention has parallels with potential access remedy to user search queries data, discussed in Appendix V on interventions to address market power in general search. However, an important difference to the click and query intervention is that it would constitute personal data. It could also potentially include, for instance, data or information derived from data on videos watched on YouTube, location data from usage of Google Maps, or information about users' attributes derived from their interactions on Facebook. Furthermore, the data may be made available to a wider range of entities, such as adtech providers (such as DMPs), advertisers and publishers. Access could be provided using standardised open APIs provided by Google and Facebook.

167. In practice, the DMU will need to carefully consider exactly which data should be made available in this way, and to make an assessment on a case by case basis taking into account the particular characteristics of the data (including privacy concerns), and the context and capabilities of the market participants that will gain access to the data, such as their ability to adequately protect it, to use it for other unintended purposes, or to circumvent any privacy protections such as anonymisation (if any such protections were feasible in the first place). The DMU may wish to consider allow access only to a limited set of data or insights that provide the highest benefit to other market participants, such as purchase intent data or location data.

168. For this data to be useful for targeting of personalised advertising, there would need to a common user ID, which would enable the recipients of the data made available to associate it with identifiable individual users, browsers or devices.

169. A common user ID intervention would involve the DMU mandating the creation of a secure common digital ID that market participants could use to

assign to their own data for targeting and attribution purposes. This is a form of interoperability intervention, as it involves establishing and ensuring adherence to a common standard.

170. A desired outcome of this intervention would be that advertisers have a wider range of firms which can provide personalised advertising targeted using insights on users derived from their use of SMS services, improving competition in digital advertising.

171. This would be a proactive intervention which would require a regulator to oversee both the set-up of arrangements and its operation in practice. It would require ongoing regulatory oversight, both to ensure that the remedy was effective, and also to ensure that the access to data was being provided in a way that is consistent with data protection requirements. There would therefore need to be new regulatory controls on firms which operate in digital advertising markets to address these risks, and restrictions on firms which do not comply with these controls.

Assessment

- *Efficiency: static and dynamic (including effects on competition)*

172. Data access remedies would be likely to increase static efficiency as data is made more widely available and put to valuable use in helping firms to better understand their customers and to better target advertising.[43] It would also enhance competition in the supply of display advertising, as more adtech providers are able to use these data to deliver effective advertising in competition with Google and Facebook.

173. The extent of the efficiency improvements are likely to be linked to the gap between the data available to Google and Facebook's comparators. In addition, the scale of efficiency benefits will depend on whether more sharing of data promotes new and innovative ways to use data, or results in more commoditisation, with all intermediaries having comparable data and reduced incentives to innovate to obtain valuable data.

174. This remedy could also harm dynamic efficiency if it undermines Google and Facebook's incentives to invest in collecting relevant user data and analysing it for insights on users, as these data and insights will then be shared with their competitors. The DMU may need to establish a fair price for the access

[43] It may also have some benefits to innovation, if the data were made available for purposes other than targeting and attribution of personalised advertising, as the data may be or used in unforeseen ways that uncover new insights or to deliver new or better services.

that reflected the economic cost of collecting and processing the data to Google and Facebook.

- *Privacy*

175. There are potentially many difficulties with this intervention in respect of its effect on privacy. There are likely to be serious privacy concerns through the exposure of users' data through APIs which allow third parties to access that data. Users will expect that data about their activities on one platform are not shared with third parties. There is a significant risk that any remedy which implies more sharing of data for targeting and profiling will be at odds with users' interests in respect of both consumer control over data and privacy. Much of the data used for targeting and profiling (browsing data, location data) may be sensitive to the user. This intervention would also reinforce the use of personal data to target advertising, which in itself may be a cause for privacy concerns for individuals.

176. This is also the case with proposals to develop a common user ID, which could be used to enable cross-site tracking, and reinforce the practice of widespread broadcasting of personal data to market participants. We describe in Appendix G that personal data are linked to individuals using a variety of imperfect means including cookie matching.

177. An argument could however be made that, relative to the current market, a market based on access to data under authorised access agreements overseen by the DMU would be better and provide greater certainty. The personal data and insights about individual's activities on Google and Facebook are already available to advertisers and other market participants, albeit indirectly, as Google and Facebook are able to deliver targeted advertising on their behalf using these data and insights. Similarly, consumers are already routinely tracked across many websites, apps, and physical locations, and their activities are linked together (albeit imperfectly) and widely shared with market participants. If it is accepted that some form of data sharing is likely to continue, then these interventions could promote more effective competition for firms which use personal data for digital advertising.

- *Feasibility and effectiveness*

178. In respect of technical feasibility, secure data sharing between market participants already happens at scale. The CMA's experience with Open Banking demonstrates that, with regulatory support, data sharing can be made to happen in a way that protects individuals' interests. However, the sensitivity, scale and variety of data and recipients under this intervention will be several orders of magnitude greater than for Open Banking.

179. There is also a gap between the capability of regulators and firms to oversee a secure mechanism for the sharing of data. However, from our experience from Open Banking and other initiatives which require regulatory oversight, it is possible that industry-led initiatives could develop if the incentives are there to do so. These could include regulatory approval for secure authentication measures, and the requirement for large firms to participate.

180. The development of a common user ID to be applied when sharing data would be technically feasible, and there are already a number of initiatives in the adtech industry to create a common user ID, such as DigiTrust (by IAB), the Advertising ID Consortium, ID5 and The Trade Desk's Unified ID.[44] However, we understand that Google has not joined these initiatives, which limits their usefulness given Google's market position in adtech. It is not clear how a common user ID would work in a future scenario where third-party cookies are no longer supported by most major browsers, and browsers continue to pursue vigorously anti-circumvention measures that close off technical alternatives that recreate the functionality of third-party cookies.

181. Existing data protection laws may place some limits on what can be implemented by the DMU pursuing this kind of intervention. However, we note that regulatory intervention (eg through order making powers or legislative requirements) could, in principle, provide a legitimate basis for processing. Therefore, the current parameters of GDPR and PECR do not necessarily create a decisive constraint on which interventions are possible.

Access to data for attribution

182. Unlike many publishers, Google and Facebook do not share user-level data with third parties on the activity of their users on their respective platforms. As discussed in Chapter 5 and Appendix O this prevents both advertisers and independent measurement and attribution adtech providers from undertaking unified measurement of campaign effectiveness across all impressions on multiple publishers (multi-touch attribution, unique reach, frequency capping, etc), where advertisers spend at least part of their budget on Google and Facebook's owned and operated inventory.

183. There are strong efficiency and competition reasons why advertising customers should be able to independently measure and assess the value and effectiveness of advertising services that they buy, and to be able to compare the value across different providers of inventory and different supply paths.

---

[44] See, for instance, Clearcode 'Identity in AdTech: Unravelling The ID Problem'.

184. Google and Facebook appear to recognise the importance of advertisers being able to measure the effects of their ad spending. Instead of permitting third parties to directly collect data about users (eg using tags and SDKs) who are shown ads on Google and Facebook's own properties, Google and Facebook now both offer 'data clean rooms' to advertisers in which they can scrutinise user-level data for measurement and attribution purposes, although advertiser may need to invest in the technical skill and capability to do so. However, this 'data clean room' approach does not address the concern that advertisers may wish to use independent attribution providers to conduct measurement, instead of relying on data that has been curated and made available by Google and Facebook.

185. However, in respect of privacy, allowing third-parties to collect granular user-level data about users' exposure to ads for attribution would also likely allow them to collect similar data (eg about users' browsing history) used for targeting, and so similar privacy implications are likely to apply. This is a particular concern if advertisers are able to obtain information on the context in which their ads are shown or information about the characteristics of the user (eg for audience verification), which can be linked to individuals. In these circumstances, someone obtaining access to ad exposure information would in principle be able to also use it to build profiles for the purpose of targeting. The same user tracking technology is used to achieve both targeting and attribution.[45]

186. As Google and Facebook already provide access to user-level data in data rooms to approved third parties for use in attribution, an alternative approach to access to data for attribution could be that the DMU were able monitor these arrangements. This could include a requirement on Google and Facebook to allow the DMU to audit the arrangements and ensure that the data made available in these data rooms are reliable and not overreported.

Conclusion on mandated access to data and information

187. Overall, we think that the case for implementing data access interventions supported by a common user ID to promote competition is likely to be strongest where the data is necessary to overcome barriers to entry and expansion. At present, the privacy and data protection risks of data access

[45] We note that there is an active debate within the web standards community about whether privacy-preserving click-through attribution may be possible (see Appendix G for more details). The key idea is that it may be possible to advertisers to receive information that *someone* that clicked on an ad ended up converting, without knowing which specific individual did so. However, these proposals for privacy-preserving attribution have yet to be implemented by major browsers or websites. Also, whilst such technologies may preserve some ability to attribute conversions, not all forms of attribution may be possible (eg view-through attribution, or multi-touch attribution) or possible to the same extent (eg click-through attribution over a long period of time, or analysis of conversion data against users' characteristics).

remedies are significant, and would need to be carefully managed. An interim arrangement where the DMU oversees a regulated form of access to attribution data by Google and Facebook may be a more feasible medium-term alternative.

Data mobility

188. The Report of the Digital Competition Expert Panel (the Furman Review)[46] recommended that its proposed Digital Market Unit should pursue personal data mobility and systems with open standards. It said that that personal data mobility would 'give consumers greater control of their personal data so they can choose for it to be moved or shared between the digital platform currently holding it and alternative new services.'

189. This remedy would be a user-led form of data sharing that would allow consumers to share the data that platforms hold on them with other platforms. The DMU would mandate that SMS platforms made user data available to third parties upon the user's request, via commonplace APIs and formats. This would allow consumers to effectively exercise their right to data portability, and move or share their personal data between the digital platform currently holding it and alternative new services.

190. Personal Information Management Services (PIMS) could facilitate the operationalisation of this remedy, by providing individuals with tools to manage their relationships with firms that control data about them.

191. As for the data access remedy, one of the desired outcomes for a data mobility remedy as applied in digital advertising markets would be to enable a wider range of firms to access users' data for digital advertising purposes, which would enhance competition and innovation.[47]

192. Similarly to the data access remedy, a data mobility remedy would include an obligation for large platforms to make user data available to other service providers. However, data mobility aims to shift the power to initiate the sharing of data towards the user: the obligation would only operate when explicitly sought by a user and with the user's consent, for a specific subset of data.

193. As an example use case, a user could instruct Google or Facebook to make data on their own interactions with the platforms available to a news publisher, which can use it to improve their service by personalising content and

---

[46] Report of the Digital Competition Expert Panel.
[47] Appendix W explores data mobility in more detail, including in its relationship with other concepts like platform and content interoperability. It also outlines the Data Transfer Project, an existing platform-led data mobility effort designed to facilitate direct transfer of data between multiple online platforms.

advertising. This access would be continuous and in real time, so that the publisher could rely on time-sensitive information (eg purchase intent).

194. In terms of 'what' data such remedy would include, data mobility could encompass the data that can be used for targeting and attribution to achieve any competition benefits in digital advertising. This could be in the form of raw user data, such as browsing and search history, or could be information derived by Google or Facebook.

Assessment

- *Efficiency (static and dynamic) and competition*

195. Increased data mobility can stimulate both competition and innovation. Similar to the data access remedy, it would enhance static efficiency by making data more widely available to be used by other service providers in the ecosystem to improve their offering and compete with SMS platforms. If costs associated to transferring data between services are reduced, novel business ideas that exploit or combine different sources of data can become feasible and compete with services offered by dominant platforms.

196. The greatest difference between the effect of an intervention based on data mobility and an intervention based on access to data is likely to be the breadth of data which becomes available to actual or potential entrants or existing competitors. The extent of data shared under a data mobility remedy will be limited to those users which participate in the relevant scheme. As discussed in the section on PIMS below, there are currently commercial barriers to encouraging users to sign up to PIMS. These would need to be overcome to a sufficient extent to allow third parties to have access to enough users via PIMS to make competition using that data viable.

- *Privacy*

197. Compared to the data access remedy, data mobility raises fewer privacy concerns. The sharing of data would only happen on the consumer's request and with the consumer's consent, rather than operating in the background. At the same time, the fact that this remedy is user-led might lead to less data being shared from large platforms to competitors, given that users might not always find it advisable to authorise their data to be used. In this sense, the static efficiency gains might be smaller than for a data access remedy.

198. It is unlikely that this remedy can be implemented without devolving some functionality to a trusted third party that can act on behalf of the consumer. PIMS could fill this role, by orchestrating the transfer of data and enforcing

users' consent and preferences. PIMS could also provide users with unified interfaces that allow them to keep track of all data mobility relationships that they have initiated.

199. Data mobility has been suggested as a viable solution for the sharing of data that is less time sensitive, such as what is stored in a user's account (eg pictures and social media posts). This is for example the case for the Data Transfer Project, a data mobility effort led by large platforms. To engender significant efficiency improvements in targeting and attribution, where data can depreciate quickly (eg browsing history, purchase intent, or location data), a data mobility remedy would need to involve exchanging data in real time. To our knowledge, this type of user-initiated live data transfer has no precedents in adtech, and its development would need to be closely overseen by the DMU to ensure that transfer of data is timely enough to allow rivals to SMS platforms to actually compete.

200. A potentially significant drawback of a data mobility remedy relates to the granularity of user consent it requires. Suppose a user visiting a news publisher's website trusts that publisher enough to initiate a data mobility request to Google, instructing the latter to make their recent search history and browsing behaviour available to the publisher. To effectively serve personalised ads, the publisher would need to share the user's data downstream with advertisers and/or DSPs. From a privacy point of view, this step would require a further data sharing request to be initiated by the user. This risks introducing significant frictions on the user side, who might be encouraged to deny access to actors in the stack they are unfamiliar with, effectively nullifying the competitive benefits of data being shared. Alternatively, the original request to share data from Google to the publisher could also include the publisher's adtech partners, similarly to how consent management platforms currently operate but with the difference that Google's data would be made available to all participants.

- *Feasibility and effectiveness*

201. It is apparent from the discussion in this section that this remedy is not likely to be effective today. The take-up of secure, user-led technologies such as PIMS is very low. However, a mandated data mobility requirement could support the development of PIMS as a commercial product. Therefore, if there were a DMU with powers to impose mandated data mobility, and also provide regulatory oversight of the development of PIMS, this could be an opportunity for the future. We discuss in more detail in the section below the conditions which might be required for PIMS to be implemented at scale, in addition to mandated data mobility.

202. To be effective, a data mobility remedy should make it easy for users to obtain and transfer their data. Many online platforms already allow users to download a copy of their data, including Google[48] and Facebook[49]. However, downloading one's data to upload it to another service is a laborious process, and can be time consuming for large quantities of data. If this manual process was the only way in which data mobility was operationalised, widespread adoption would be unlikely.

203. A more efficient approach to data mobility would rely on APIs. Many platforms, including Google and Facebook, maintain a set of APIs to allow developers to interact with the platform's services and integrate them into new services.[50] The main advantage of APIs is that they can provide access to data automatically, in real time, and via commonly accepted protocols and data formats. An effective data mobility remedy would mandate platforms to provide APIs to enable access to data, where they do not already exist.

204. Consumers would not be able to directly interact with APIs, but could do so via their PIMS), which could facilitate data mobility by directly interfacing with APIs provided by platforms, thus streamlining and automating user data mobility requests. The user would be able to instruct a platform to share data with another service, on a one-off or ongoing basis, and the user's PIMS would orchestrate this data transfer in a seamless fashion.

205. Some stakeholders have put forward the view that data mobility relies on the availability of defined standards regulating how APIs should be implemented. Until platforms are compelled to comply with standards via regulation, it has been suggested that they will have little incentive to push any initiative through.[51] On the other hand, there is a risk that the process of developing and approving standards will be lengthy and cumbersome. Highly detailed standards might not be required to enable third parties like PIMS providers to successfully interface with platforms' services, and might actually end up being too prescriptive. It might be easier and less intrusive to simply mandate that platforms' open APIs comply with commonly accepted industry specifications in terms of authentication, data format and encoding, and documentation.[52]

---

[48] Google Download Your Data (formerly known as Google Takeout) is a centralised page for Google users to import and export their data in many (but not all) Google services.
[49] Facebook, Accessing and Downloading Your Information, accessed 07/05/2020.
[50] Appendix J in this report presents an overview of Facebook APIs. Google maintains several APIs for its wide range of services – a list is available here.
[51] This point has been raised by Ctrl-Shift in their response to our consultation on the Interim Report.
[52] As an example of commonly accepted open API standards, see the OpenAPI Initiative.

Conclusions on data mobility

206. Data mobility supported by PIMS could be an effective way to balance the benefits from data sharing against privacy concerns. It would require the development of new commercial models by which users sign up to PIMS, or any other services which allow them to port their data using data mobility. We provide a more detailed discussion of the possible advantages and drawbacks of PIMS, as well as obstacles to their widespread adoption, to the final section of this appendix.

207. We provide overall recommendations for powers for the DMU to impose these remedies in the section below.

Our assessment – targeting and profile data

208. We have assessed in this section four different options which could address the data advantage that Google and Facebook have over their competitors. The case for these interventions will be strongest where there is the greatest difference between the data available to the SMS firms and their competitors, which will therefore deliver benefits in terms of better working of competition.

209. The options for intervention described above would all address this competitive advantage and level the playing field. The benefits of all the options will therefore be likely to become greater in the future if rivals to Google are no longer be able to utilise third-party cookies to join user data from different sources. We therefore expect that the DMU would be more likely to intervene if Google phases out third-party cookies as planned, and continues to use its own data in profiling for digital advertising.

210. We have summarised in Table Z.1 below some important considerations in comparing these options, having regard to the criteria described in Appendix T.

Table Z.1: Summary of assessment of intervention options to address Google and Facebook's data advantages

Type of measure / criteria	Ease of implementation	Impact on competition and innovation	Impact on static efficiency / value of digital advertising	Impact on privacy
Data silos	Easy to implement but likely to need monitoring and audit to be effective	Should promote competition by levelling the playing field – offset by less data available for digital advertising	Mixed – negative from less data, offset by positive if more effective competition	Positive – regulator determines extent of sharing
Enforced purpose limitation	Easy to implement for regulator. Likely to increase burdens on consumer and consent fatigue			Positive – user determines extent of sharing
Mandated data access (based on common user ID)	Difficult to implement as would require common user IDs. May be more manageable for certain types of data – eg regulated product for certain types of attribution data	Positive for digital advertising as innovation and competition dampened by advantage of large platforms. Could support innovation in user content if makes monetisation more effective	Positive direct effect from more valuable digital advertising	Potentially negative as relies on more sharing of data. Could be offset by greater regulatory oversight than under status quo of current data sharing across Google and Facebook and implemented for limited data sets
Data mobility	Difficult to implement as would require: • widespread take-up of PIMS. • regulatory oversight of access to ensure that it is limited to approved data and suitable measures are in place	Positive if can be made effective, and could potentially support development of innovative services based on PIMS and data mobility in other markets	Positive direct effect from more valuable digital advertising	Broadly positive – If implemented via PIMS, it could enhance privacy and be based on consent. Some risk, however, that widespread and easy rollout would result in users being 'nudged' into sharing data

Source: CMA analysis.

211. This summary of the different options illustrates that DMU would need to trade off the potential harm from balancing measures which improve privacy but may reduce the value of digital advertising, against those which are likely to have the opposite effect. However, all the options should make competition work better in digital advertising, and all the options would at least provide some additional oversight about the sharing of data, by comparison with the current market.

212. **We recommend that the DMU should have powers to make each of these interventions, where it concludes that the adverse effects on competition outweigh any efficiency benefits.**

Conclusion

213. **We recommend that the DMU should have powers to impose remedies to address the data advantages that SMS firms have in targeting of digital advertising.** These powers would be limited to where there is sufficient evidence that the benefits outweigh the costs, having regard to the DMU's broader objectives, including consumer control and the technical feasibility of the remedies.

214. Following this study, and alongside the work of the Digital Markets Taskforce, we intend to work with the ICO on the future direction of work, including how consumer control, the incentive to invest and competition can both be considered in assessing what is appropriate in respect of sharing of data, within both the SMS platforms and the open display advertising market.

Personal Information Management Services

215. In this appendix, we have presented remedy options aimed at addressing data advantages of SMS platforms. We have considered and weighed their implications for efficiency, privacy, and competition. Beyond the merit of these interventions, questions remain about how to effectively implement them in the current ecosystem of online platforms and digital advertising.

216. Personal Information Management Services (abbreviated as PIMS) have been proposed as a tool to give individuals more control over how their personal data is collected and processed online. They enable individuals to manage their relationship with the entities that can access this data.[53]

217. We believe that PIMS have the potential to provide the infrastructure needed to operationalise data-related remedies. PIMS could be used to facilitate a data mobility remedy, by streamlining the process of integrating and transferring data across services on the user's behalf. They could also be instrumental for the enhanced purpose limitation remedy, by allowing users to specify and manage consents with the various firms that control the user's data.

218. An important feature of PIMS is centralised consent management. Consumers can oversee in a single interface which entities are authorised to process their data and for which purposes. This enables them to more effectively exercise

[53] We use the acronym 'PIMS' to encompass several other analogous or similar concepts, such as personal information management *systems*, personal data management systems (PDMS), personal data stores (PDS), data facilitators, and data trusts.

their data protection rights such as data portability, purpose limitation, rectification, and erasure.

219. Other potential benefits of PIMS can be to improve the quality of data available to online service providers to develop new integrated services. Furthermore, by supporting data portability and reduce switching costs for consumers, they can stimulate innovation.

220. The most common form of PIMS is that of a centralised infrastructure, where the consumer's Personal Data Store (PDS) sits at the centre of a series of services interconnected by APIs. Each service must obtain consent from the consumer, mediated by the Personal Information Manager itself, to process any of the consumer's data.

221. PIMS rely on well-developed technologies and are technically viable. The main obstacle to their adoption is likely to be their commercial viability. As a multi-sided platform, they rely on incentives for adoption being present on all sides. No application of PIMS is yet operational that enables provision of online advertising.

222. A PIMS-based ecosystem has the potential to create additional concerns. PIM providers might at least initially be under-resourced, and not able to provide levels of data security that are comparable to those by dominant platforms, creating the risk of a single point of failure for data privacy. From a competition perspective, there is a risk that network effects might cause any market for PIMS to be concentrated, engendering new competitive gateways.

223. If the Digital Markets Unit were provided with the necessary powers to implement the data-related remedies outlined in this appendix, and coordinated closely with the ICO to provide proactive enforcement of data protection law, PIMS might emerge as a viable solution to address privacy and competition issues in digital advertising.

224. In this section, we start by describing a stylised PIMS ecosystem. We then outline the main advantages of PIMS, and their potential for operationalising the proposed data-related remedies in this appendix. We proceed by examining the technical and commercial viability of PIMS from the perspective of consumers, advertisers, and publishers. Finally, we present a set of ancillary measures that are required or desirable to enable a market for PIMS to emerge.

Outline of a PIMS model

225. For the purposes of describing a general PIMS model, it's useful to identify the main actors that feature in a simplified digital advertising ecosystem.

- The *consumer* is an internet user who wants to access online services.
- The PIMS, which is authorised to act on behalf of the consumer and mediate her relationship with data controllers and data seekers.
- *Data controllers* are organisations that control data about the consumer, which the consumer provided directly or generated by interacting with their services. Data controllers could be providers of online services: for example, a news website providing news content that records the consumer's reading habits, or a social media platform that aggregates content from the consumer's friends and pages. They could also be advertisers: for example, an online store that logs the consumer's visits and purchases.
- *Data seekers* are organisations who are interested in processing data about the consumer that they do not control. For example, they could be advertisers wishing to serve personalised ads to the consumer.

226. A common PIMS model is that of a centralised, multi-sided platform, where the PIMS acts as an intermediary for the consumer's data relationships. In a sense, the PIMS acts as an infrastructure layer, on top of which additional services can be built by third parties through the APIs that the PIMS offers. The consumer can instruct businesses controlling their data to share that data with the PIMS in real time. The consumer's data is stored in a secure location (sometimes known as *personal data store*, PDS) – which could be on the cloud or on a private server/device – owned by the consumer themselves. In principle, any type of data can be included in the PDS: demographics, browsing activity, purchase history, but also social media posts, financial transactions, and health data.

227. The PIMS manages access to the data on behalf of the consumer.[54] The consumer can instruct the intermediary to allow named parties, or parties meeting pre-specified criteria, to access subsets of her data. The consumer is also able to specify for which purposes and for which period of time the data would be made available. Information on all these permissions can be centralised into a 'consent dashboard', where the consumer can oversee, amend, or revoke consents.

[54] The GDPR does not make specific provision about the ability to appoint someone to act for you when dealing with an organisation that is processing your personal data (except for the ability to appoint a specialist body for the purposes of making complaints). However, in its guidance to individuals on complaints about media organisations, the ICO states that it is possible to appoint someone to act on your behalf to exercise your rights under data protection law, and that it most circumstances it would expect organisations to allow you to exercise your data protection rights, or raise data protection concerns, through a properly appointed representative.

228. The PIMS could also be responsible for orchestrating exchanges of user data. As an example, a news publisher might want to access a user's social media data in order to recommend content to the user based on her interests. The publisher would in this case be required to obtain consent (via the PIMS) to access social media data in the user's data store, for the specified purpose of providing personalised content recommendations.

229. Another case is the use of data for digital advertising. An advertiser (or a DSP on an advertiser's behalf) wishes to display ads on a publisher's website, targeted to users with certain characteristics. In this case, the advertiser could seek to obtain consent to access the data store for users visiting the publisher's website. Alternatively, the targeting could take place entirely on the publisher's side, without the advertiser having sight of the data.

230. Centralised PIM solutions are already available, although they vary in their degree of adoption. Some examples are.

- Solid, which stands for social linked data, is a proposed set of conventions and tools for building decentralized Web applications, based on personal data stores.[55]

- Hub of All Things (HAT) has developed open source 'HAT microservers' which allow users to store their data in the cloud and make it available to third parties in a private way.[56]

- Digi.me offers a decentralised architecture where users can aggregate data from multiple sources and share it privately with apps and other service providers.[57]

231. It is unlikely that PIMS would be compatible with obtaining data for us in the real time bidding (RTB) ecosystem, at least in its current form. In the RTB paradigm, consent is often elicited in a blanket fashion by the publisher for multiple adtech providers upon acceptance of cookies by the user. Impressions can then be auctioned among this set of adtech providers by propagating user data through bid requests. This appears hard to reconcile with the granular type of consent implied by PIMS.

232. However, it's possible to envisage real time auctions taking place *within* the personal data store in a privacy-preserving way, extracting inferences on the data without any data leaving the store. This is similar in spirit to some of the client-side privacy-enhancing technology (PETs) proposals outlined in

---

[55] See how Solid works, getting started with Solid, and GitHub page for Solid.
[56] See What is the HAT, and *Homo Databundus: Correcting the Market for Identity Data*.
[57] See What is Digi.me.

Appendix G. Indeed, development and deployment of client-side PETs allowing for on-device targeting and attribution might reduce the need for data to be transmitted in the ecosystem at all.

233. None of these solutions has yet been implemented in the realm of digital advertising. However, by substantially acting as private APIs for users, these platforms could facilitate an ecosystem in which developers can create applications and interfaces that leverage user data, and may quickly expand in scope to encompass digital advertising if they became widespread.

234. Decentralised models alternative to the centralised PIM exist. One example is Tide, where the data controller retains the data itself, but cedes the cryptographic key needed to access it to the consumer. Through Tide's software, the consumer would be able to manage which controllers can obtain a one-time access key to gain sight of their data.

Potential benefits of PIMS

Operationalising data-related remedies

235. As detailed throughout this appendix, PIMS can be instrumental in operationalising data-related remedies related to data access for targeting and attribution.

236. The data mobility remedy concerns mandatory access to raw data held by SMS platforms about users. This would entail user data, which is often personal, being made available to competitors if requested by the user. PIMS can allow data controlled by one party to be accessed by a third party (i) in a secure way, (ii) with the awareness of the user, and (iii) if needed, integrating it with any standardised identification layer, such as a Digital ID.

237. Another proposed approach, which we termed purpose limitation, would mandate SMS platforms to obtain more granular consent from the user for processing the same data across multiple purposes – in contrast to the broad privacy policy terms where consent is obtained for many purposes at once. If these granular purposes are sufficiently standardised across multiple SMS firms (or across the wider ecosystem), then PIMS may be well placed to help consumers to effectively exercise their data protection rights by enabling centralised consent management: users may be able to oversee and manage the purposes for which they have consented their data to be processed, effectively enabling the remedy to be user driven.

238. It is less clear whether the proposed data silos remedy, whereby sharing of data across different services provided by SMS platforms would be prohibited, can be effectively supported by a PIMS-type solution.

Centralised consent management

239. Currently, the main model for communicating data protection information to users has been notice and consent. Typically, users are presented with privacy policies and are asked to accept or reject them. As detailed in Chapter 4 and Appendix K, this notice and consent model imposes excessive transaction costs on consumers, by putting on them an unrealistic burden to engage with privacy policies multiple times a day. Furthermore, once consent is given, it is often difficult to withdraw it and amend its scope by exercising GDPR rights such as access, rectification, and erasure. These rights need to be exercised separately for each data controller, with time-consuming ad-hoc procedures.

240. The main benefit of PIMS could be to provide consumers with tools to tackle some of these issues via centralised consent management. Consumers could have access to unified interfaces to keep track of controllers and processors of their data, what data each of them has, for which purposes data is being used, and manage consents for such data. This can help minimise consent fatigue and empower consumers to make more consistent, comprehensive, confident and informed choices.

241. More broadly, a centralised consent tool can facilitate the exercise of rights under GDPR and data protection legislation. Requests for access, data portability, restriction of processing to certain purposes, rectification, and erasure could be managed by the PIM, which would operationalise them in a delegated manner. A consumer could manage this type of request towards a single controller, or against multiple data controllers at the same time.

Other benefits

242. PIMS could also unlock some secondary benefits.

- They can operationalise the principle of data portability enshrined in GDPR, and enable consumers to make fuller use of data mobility across platforms, in turn benefiting competition and innovation;

- They can unlock value for the entire ecosystem, by providing secure and consensual access to high-quality data from multiple sources which can be used to develop better products and services;

- They can provide value to consumers by offering additional functionality, such as secure data storage, avoidance of repeated consent popups, and seamless private authentication.

Practicability of PIMS

243. Despite similar intermediated models existing since the 1990s, PIMS have never managed to achieve widespread adoption. Some responses to our interim report have highlighted that no viable business model seems to have reached substantial scale yet, despite recurring interest in this type of solution through the years.[58] In this section, we examine the practicability of PIMS from a technical and commercial perspective.

Technical viability

244. A potential PIMS ecosystem would mostly be based on consolidated technologies like encryption, APIs, secure authentication, and secure data storage – whether on the cloud or on users' devices. None of the responses to our interim report consultation raised any doubts about the technical feasibility of PIMS. Similar technologies are already being used in open banking, where confidentiality and security are paramount. This suggests that that PIMS could rely on approaches that are familiar and commonplace in the industry.

245. Some proposed implementations of PIMS incorporate other technologies – particularly decentralised approaches such as edge computing and blockchain. These technologies do not form a core part of the simplest PIMS model. While their viability is less clear, they might significantly expand the scope and applicability of PIMS. This type of additional functionality could be one of the bases for competition between different PIMS providers.

246. In summary, we do not see major technical hurdles to the viability of PIMS. It is more likely that the practicability of PIMS will hinge on their commercial viability, rather than their technical feasibility.

Commercial viability

247. To achieve widespread adoption, PIMS would need to overcome the 'chicken-and-egg' problem that typically faces multi-sided platforms. Network effects imply that consumers will find it convenient to adopt a PIMS if they are able to use it across many services, and service providers will only adapt their

---

[58] See for example the responses to our consultation on the Interim report by Developers Alliance, DMG Media, and Verizon.

infrastructure to PIMS if they expect facing significant demand from the user side. It is thus useful to consider, for each main actor in a possible PIMS ecosystem for digital advertising, where the creation of additional value might stem from, and where obstacles to adoption are likely to arise.

Consumer-side value creation

248. For PIMS to reach widespread adoption, it is vital that they create value from the perspective of the consumer. There is a range of potential value creation proposals that might encourage consumers to adopt a PIMS.

249. Firstly, a PIMS ecosystem where the ability to track consumers is also curtailed can facilitate *privacy* in a broad sense. Data provided or generated by the consumer resides more clearly under the control of the consumer herself.

250. Using centralised consent management tools provided by PIMS, the consumer can keep track of controllers and processors of her data, what data each controller or processor can use and for which purposes, and manage consents for this data. This aspect is central to the potential value of PIMS, for multiple reasons:

- It can provide a unified interface, with a comprehensive view of what data is being processed and for which purposes, enabling the consumer to make decisions of varying granularity about what processing to allow;
- It can help prevent consent fatigue, by providing default privacy-oriented consent choices for newly encountered services – for example, defaulting to denying data to publishers that are only seldom accessed by the user;
- It can provide periodic reminders for users to review their preferences and relationships with data controllers and processors, updating and actualising their privacy choices;
- It can make it easier for users to withdraw consent and exercise their other data protection rights (such as subject access requests and erasure requests).

251. Another important set of advantages pertains to enhanced features of the online user experience that can be unlocked by PIMS:

- *Avoidance of consent popups*: The PIMS can manage default or automatic consent (acceptance or denial) upon accessing new websites of services.

- *Secure data storage*: Data about the user from multiple services, some of which might be personal, is backed up and stored securely in a centralised location.

- *Ease of switching*: The need to manually transfer data from one service to another can be eliminated, enabling more seamless exercise of data portability rights;

- *Better value from services*: The possibility of securely and privately pooling insights from multiple data sources can enable service providers to develop and offer new services, delivering increased value to the consumer;

- *Private authentication*: A PIMS can allow users to sign up (and sign in) to participating providers' services in a faster, more seamless, and private way.[59]

252. Finally, PIMS may facilitate a more formal value exchange involving the consumer. This could involve consumer-side monetisation, with flows of micropayments from publishers and platforms to consumers in exchange for access to their data.[60]

253. While plausibly helping adoption, these monetary incentives might end up being quite small. Furthermore, there are reasons why monetisation of user data might not be desirable. Besides conflicting with the position that privacy is a human right,[61] allowing consumers to reap direct monetary benefits from interactions with ad-funded content might induce moral hazard dynamics: users might be incentivised to engage with ads not out of interest or relevance, but purely to be compensated. Regardless of these concerns, monetisation does not appear to be a prominent feature in the existing PIMS initiatives we have examined.

254. Alternatively, PIMS may facilitate the flow of non-monetary value – such as additional services, convenience, or rewards – from publishers to consumers. This type of value exchange between publisher and consumer seems more desirable. It can incentivise consumers to share their data with publishers and services that they value, rather than monetising ads regardless of where they appear.

---

[59] For an example of this function, see Sign in with Apple.
[60] For example, see UBDI.
[61] As noted by Privacy International in their response to our consultation on the Interim Report: 'it is essential that personal data is not regarded / framed as a mere economic asset'.

Consumer-side obstacles

255. Alongside these potential incentives, there are relevant obstacles that might hinder adoption of PIMS by consumers. Firstly, the attractiveness of a centralised platform where consumers can review and update their data access settings hinges fundamentally on their capability and willingness to engage with these settings. Consumers' lack of knowledge and inertia are likely to be the biggest barriers to the adoption of PIMS.

256. PIMS may provide an opportunity for users to examine their consent choices in a more 'ideal' condition, when they are not impatient to access a website or app, and potentially a mechanism to enforce that choice and control their own future behaviour. However, proposals to centralise consent management do not fundamentally shift the burden away from users to make potentially difficult abstract choices about the relative value of privacy protection versus access to online services.

257. If not designed for maximum ease of use, PIMS might end up introducing further frictions in the consent management process, rather than relieving them. Consumers might not be interested in changing their ways of consuming content, especially if it requires further effort in understanding and operating a new platform.[62] This might be particularly true for vulnerable consumers, like children and elderly people. For this reason, it seems important that a PIMS ecosystem is accompanied by privacy-oriented defaults as an ancillary measure.[63] We will touch upon defaults in the 'Ancillary measures' section below.

258. Finally, a prerequisite for adoption of PIMS is consumer trust in the security of their data. Regardless of a PIMS provider's technical arrangements to store and access data securely, consumers might not trust a less-known entity to keep their data secure from leaks or malicious attacks – at least compared to how much they trust large platforms like Facebook and Google. As detailed in the 'Ancillary measures' section below, a system of accreditation for PIM providers could help ease this concern.

Advertiser-side value creation

259. In a PIMS ecosystem, advertisers would be able – with consent – to leverage data coming directly from the consumer's data store, a univocal, up-to-date, and cohesive source of data, potentially covering a broader set of information about the consumer. This increased data quality can enable the provision of

[62] This point has been raised in the responses to our consultation on the Interim Report by DMG Media.
[63] See Horizon's response to our consultation on the Interim Report.

more relevant and timely advertising, increasing value not only for advertisers but throughout the ecosystem, including consumers and publishers.

260. Further potential advantages to advertisers are:

- Preserving a complete and auditable consent trail, where each impression can be linked to consumer consent – either directly from the user, or delegated to the PIM;
- Reducing aspects of the need to store personal data on consumers, thereby reducing liabilities deriving from data breaches and security threats.

Advertiser-side obstacles

261. The main obstacle for adoption of PIMS on the part of advertisers is the availability of 'outside options' to obtain analogous or similar data on consumers. Advertisers will refrain from paying to access data from a PIM if they can obtain it at a lower cost and without valid consent from other sources, chiefly large 'walled gardens' or data management platforms.

262. This issue appears particularly challenging from a technical side, as it would require the PIMS provider to be able to exclude firms that have not obtained consent for accessing the relevant data. Without additional safeguards, this type of data is non-excludable – eg it can be easily copied and sold by whoever first accessed it with consent.

263. A workable solution for this issue is likely to not be technical, but rather regulatory. A remedy which limited some forms of data sharing to cases where user data is managed by a PIMS could be one option to give platforms and publishers the incentive to encourage users to sign up to PIMS.

Publisher-side value creation

264. Similarly to advertisers, publishers can also benefit from increased data quality available from PIMS. Better quality data can lead to more relevant advertising, which can in turn result in increased publisher revenue.

265. There are also some opportunities for PIMS to create value for publishers more specifically. A common complaint from publishers is that first-party data on their unique audiences' interactions with their services is collected by large platforms like Google and Facebook via analytics and tracking tools, and subsequently reused for targeting purposes on other websites. More information on the 'commoditisation' of publisher data is available in Appendix S and Appendix G. In a PIMS ecosystem, the ability to reuse data for

targeting without valid consent would be curtailed – thereby potentially mitigating the devaluation it implies for publisher inventory.

266. Furthermore, access to more detailed and better quality data about their user base can allow publishers to offer new types of service. Private authentication can enhance publishers' ability to offer tiered access to their content, allowing users to choose between subscription models versus ad-supported versions of the same pages.

PIMS-side obstacles

267. Finally, we touch upon some barriers that PIMS providers themselves might face upon establishing a market for their services. Firstly, while the technologies underlying PIMS are at a relatively mature stage of development, any new provider will incur substantial upfront costs in setting up their infrastructure. Some of the ancillary measures detailed below (such as accreditation) can be used to stimulate sufficient investment in this area to overcome initial fixed costs.

268. Some responses to our consultation also cited a risk that emerging PIMS providers might not be able to successfully match the data quality and depth of large platforms like Google and Facebook.64 As for the previous point, if supporting remedies like mandated data mobility were in place, this would have a consequential effect on the ability of PIMS providers to be viable in providing competitive services either themselves, or through commercial agreements with publishers or intermediaries.

Ancillary measures

269. Despite the significant potential advantages outlined so far, PIMS have not yet been able to reach widespread adoption. There is currently no full-fledged market for this type of solution, despite several proposals being piloted and made available. We discuss below a set of ancillary measures which could counteract some of the obstacles to adoption that we have detailed in the previous section.

Authentication

270. An important component of PIMS is authentication. It's essential to ensure that the person authorising the sharing of a consumer's data was the

[64] See the response by the Competition Law Forum to our consultation on the Interim Report.

consumer itself. PIMS would therefore require a secure authentication process.

271. It might also be necessary to provide participating consumers with a single 'Digital ID' that they could use to identify themselves with multiple providers. We examine the implications of a Digital ID earlier in this appendix, when discussing the data access remedy.

Defaults

272. PIMS would introduce a further level of intermediation for consumers accessing online content. Even if PIMS interfaces were successfully designed for maximum ease of use, they might still be too complex for some consumers – particularly vulnerable ones like children and the elderly. It might be necessary for PIMS to come equipped with sensible default settings, whereby a consumer who is not able or willing to engage with customising their PIMS is not subject to more exploitation of their data than if they did not have a PIMS.

Accreditation

273. An accreditation system could be envisaged for PIMS providers, similar to the Open Banking setting, where each provider's accreditation details would be made available to counterparties. This would imply a process of risk-based scrutiny by a regulator (possibly the Digital Markets Unit) to ensure that organisations entering the ecosystem were fit and proper and that their procedures and systems, including security, were adequate. It would also imply a register or directory where the accreditation credentials of third parties could be inspected, including by consumers and data controllers.

274. Alternatively, a regulator like the DMU could simply formulate and implement a set of standards that PIMS providers need to comply with, and leave the audit process to third parties.

275. The advantages of an accreditation system would not be limited to the enforcement of data security standards. It would also provide a trustworthiness signal for consumers, potentially increasing their willingness to adopt a PIMS from a provider that would otherwise be relatively unknown. However, setting up and administering an accreditation system is likely to be a burdensome process, and it risks slowing down the pace of innovation among PIMS providers.

Digital literacy

276. Consumers who are better informed about data collection practices and the trade-offs inherent in accessing online content 'for free' might be more willing to adopt PIMS as a means of managing their online presence and controlling their data. Multiple parties responding to our interim report have highlighted the usefulness of public information campaigns focused on digital literacy.[65]

Potential for raising new concerns

277. Despite the many advantages, a PIMS ecosystem might have drawbacks. A first concern is about data security. SMS platforms are able to invest significant resources in keeping the data they control safe from leakage or malicious breaches. Nascent PIMS might have limited funding to maintain strong data security for their data stores, both at rest and during transmission, at least compared to dominant platforms.

278. In addition, a centralised data store might end up containing potentially very sensitive data from many products and services. This risks casting data stores as single points of failure for data breaches.[66]

279. Our experience with Open Banking seems to indicate that this sort of infrastructural security concerns can be dealt with successfully via robust accreditation procedures. Furthermore, Ctrl-Shift drew our attention to their report on the results so far of their Data Mobility Infrastructure Sandbox project. Their report's primary conclusion was that the end-to-end process of personal data sharing can be made safe.[67]

280. From a competitive perspective, an additional layer of intermediation in consumers' online activities has the potential to engender further competitive gateways. As a multi-sided platforms, PIMS providers will experience cross-side network effects, where consumers value a PIMS that is supported by many publishers and advertisers, and publishers and advertisers are more likely to support a PIMS with a large number of single-homing consumers. This familiar dynamic increases the likelihood that very few firms (perhaps even just one or two) will emerge as 'winners' and take most of the market,

---

[65] In their response to the consultation on the interim report, the Advertising Association underlines Ofcom's statutory duty to promote digital literacy, and calls for 'both government and industry to invest more effort into media literacy programmes'. Snap suggest that Ofcom should be resourced to provide 'expanded and improved media literacy training for all citizens'.
[66] This point was raised by DMG Media in their response to our consultation on the interim report.
[67] Data Mobility Infrastructure Sandbox, p5.

similarly to the evolution of other markets in which digital platforms are active.[68]

281. A separate concern is the possibility that existing incumbent online platforms could act as strong competitors in nascent PIMS markets, given their large 'installed base' of customers.

[68] This point was raised by the Developers Alliance in their response to our consultation on the interim report.