PREISKEL & CO

MOVEMENT FOR AN OPEN WEB

Remedies to Platform Dominance: The control of data, Data Trusts and other models of decentralized data management and the need for data stewardship to complement remedies to bundling, self-preference and discrimination

Summary: sources of market power and the role of data in Online markets[1]

The Competition and Market Authority (CMA) Mobile Ecosystems Interim Report of December 2021 ("Interim Report") considers the issue of platform dominance with specific reference to mobile ecosystems and makes the following notable findings:

- that each of Apple and Google do not compete but are dominant with relation to their respective ecosystems; and
- their dominance has allowed them to impose restrictive terms and conditions in apps store guidelines, bundle products (such as apps and payment systems), user access to the Open Web, and allow each platform owner to promote their own products and discriminate against those of their rivals. These behavioural issues arise from market power and vertical integration throughout multiple supply chains since each platform owner has the economic incentive to discriminate against rivals and self-prefer own products – promoting themselves, limiting users' choices and distorting competition on the merits; and
- mechanisms to enable and increase consumer choice through browser unbundling, apps unbundling, banning restrictions in apps store guidelines, enabling Open Web apps to compete with native apps and other measures to address vertical integration issues are required.

The CMA is now seeking further views and considerations on remedies. Other jurisdictions are considering these issues in parallel in the context of proposed gatekeeper legislation.[2] MOW is publishing its views on these issues since they are manifestly significant and affect users in all jurisdictions.

The Interim Report seeks to address "the sources of Apple and Google's market power" with a view to taking action and to "reducing barriers to competition or otherwise opening up markets to competition".[3] Mobile browsers are seen as a source of market power.[4] Restrictions on the user being able to choose different browsers and browser engines are then discussed and remedies enabling consumer choice are

[1] See further Annex F CMA final report https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F in sum: data gives platforms a competitive advantage in the provision of digital advertising. Platforms provide targeting capabilities which allow advertisers to retarget their current customers and to target potential new customers. Detailed data on consumers' demographics, interests, preferences and behaviours is most valuable in terms of profiling consumers, predicting consumers' potential response to advertising and tailoring advertising messages. Platforms also provide verification and attribution services. Their ability to collect data, beyond their own consumer-facing services, from third-party sites and apps, and to combine it with analytics data to present a unified view of campaign performance to advertisers, is very important for digital advertising. Google has a competitive advantage in terms of being able to carry out attribution accurately for campaigns that advertisers run, at least in part, on their own 'walled garden' platforms. Restrictions on third-party access to granular analytics data on Google (and Facebook's) properties give Google (and Facebook) a competitive advantage in measuring advertising effectiveness. This finding has several implications for the role of data in digital advertising. Chapter 5 reviews the extent to which data, coupled with other barriers to entry and expansion, impedes effective competition between smaller platforms and Google and Facebook. Chapter 6 considers how platform's data advantages may lead to weaker competition and poor returns to consumers. Chapter 10 sets out the next steps the CMA in relation to data availability and data protection. In Appendix K the CMA reviewed the choices available to consumers to control their data and in Appendix X we evaluate potential interventions to allow consumers a choice over whether to receive personalized advertising. Appendix Z outlined remedies aimed at reducing or eliminating the competitive advantage that data confers to large platforms. No remedy to these issues has yet been put in place.

[2] See EU DMA, US Access and Interoperability and Australian proposals.

[3] Interim report Chapter 7 p 359

[4] Interim report Chapter 5 p 190.

canvassed.

MOW agrees with the approach and have made separate representations on them. However, the role of data and how the platforms capture, manage and misuse data for their own benefit is underexplored in the Interim Report. Consistency with previous analysis [5] and the duty to promote competition[6] suggests that data competition issues are highly relevant and need to be addressed now. They have not been addressed elsewhere.[7]

The Interim Report refers to the Privacy Sandbox case (at 5.210), but that cross reference refers only to one aspect of the case. Importantly the CMA's Decision incorporated by reference the CMA's June and December NIAC's cover the suite of changes that are being made by Google.[8] The issue of control over end user data and Google's data advantages and control over sign in is addressed, but the coordination between Google and Apple over sign-in policies and mutual control over data for their mutual benefit is not addressed at any point in any previous investigation. This means that Google and Apple can undermine access to data needed for interoperability or business to business measurement purposes and interfere with the provision of that data between end users' computers and competing businesses.

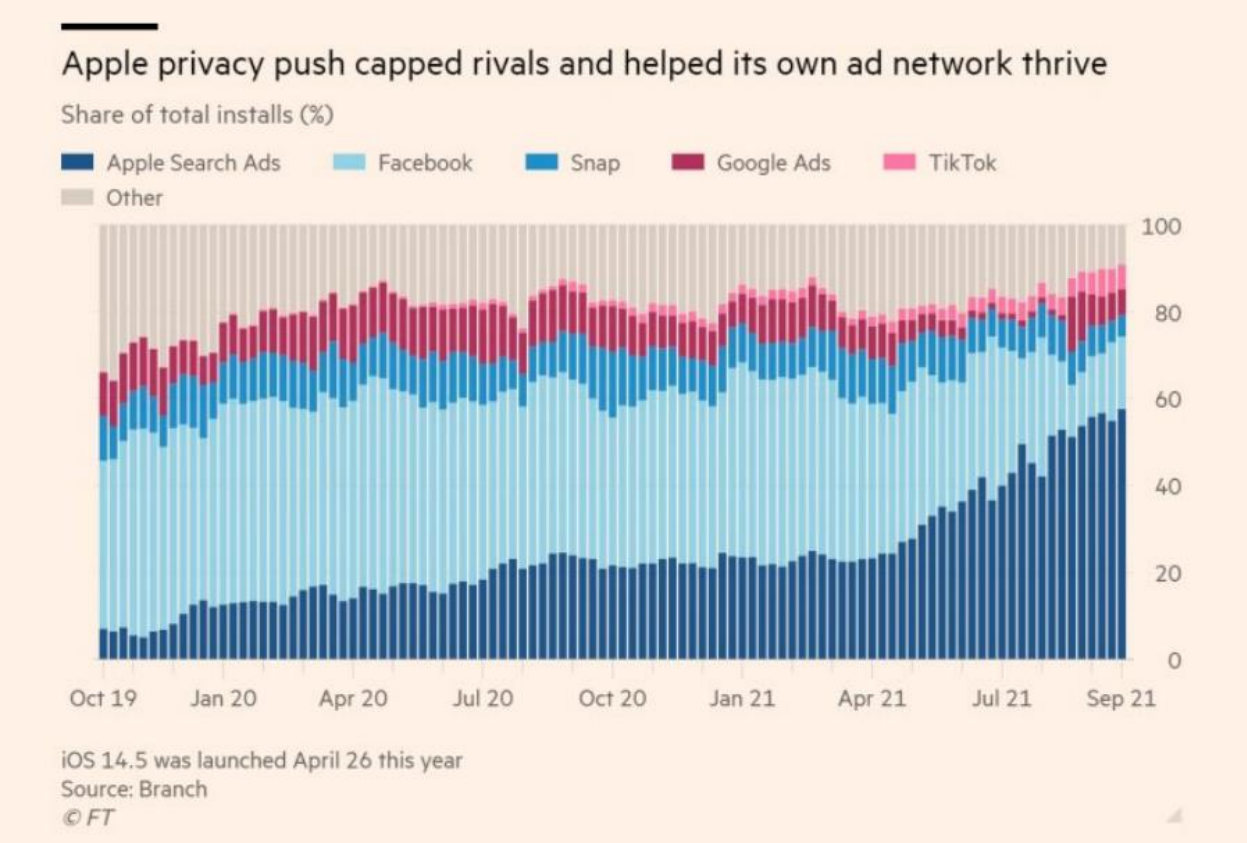
[redacted] Google and Apple are coordinating for mutual benefit.[9] A prominent and telling example is the discriminatory treatment Google Analytics cookies benefitted from under Apple ITP: [redacted] Apple's benefits from its self-preference and interference with interoperability and data include considerable financial benefits, as discussed by Patrick McGee of the Financial Times.[11] This also shows the growth in Apple's advertising business, which to date is not discussed or reviewed in the Mobile Ecosystems Investigation, but is the basis for funding the vast majority of internet businesses.

As discussed in the FT:

"Apple's advertising business has more than tripled its market share in the six months after it introduced privacy changes to iPhones that obstructed rivals, including Facebook, from targeting ads at consumers. The in-house business, called Search Ads, offers sponsored slots in the App Store that appear above search results. Users who search for "Snapchat", for example, might see TikTok as the first result on their screen.

Branch, which measures the effectiveness of mobile marketing, said Apple's in-house business is now responsible for 58 per cent of all iPhone app downloads that result from clicking on an advert. A year ago, its share was 17 per cent. It's like Apple Search Ads has gone from playing in the minor leagues to winning the World Series in the span of half a year," said Alex Bauer, head of product marketing at Branch."

[5] See para 13 page 8, para 4.57 page 165, para 6.46 page 321 and how they gather consumer data at para 4.28 p157 et seq and sign in as an issue box 4.1 p 156 and data capture in Annex F.
[6] UK Competition & Markets Authority, "Online platforms and digital advertising" (2020) https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf
[7] Also, associated with the capturing of data, at present the Interim Report does not yet cover the continuing and unremedied issues of "exploitative and unfair terms" imposed "On a Take It or Leave It" basis or "Sign-in". See for example CMA Online markets and Digital Advertising Final Report and CMA Decision concerning the Privacy Sandbox.
[8] https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes
[9] See [redacted] and https://movementforanopenweb.com/cma-investigation-of-apple-and-google-market-domination-is-long-overdue-and-is-something-weve-been-fighting-for/
[10] See [redacted]
[11] https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d?sharetype=blocked https://mobile.twitter.com/PatrickMcGee_/status/1449608262492459011



Coordination between companies of such scale as Google and Apple who are both in the online advertising business, and with so many rules affecting data collection not least in browsers, needs fuller investigation. Their individual dominance in each ecosystem stems in part from control over data and it is a core source of market power which now needs to be remedied.

When the CMA is considering the ways that the ecosystems may misuse browsers to strengthen their market positions[12] and remedies such as those discussed in Chapter 8 of the Interim Report, it should not investigate that issue in isolation from the role the platforms' browsers perform in capturing data from end users and how they interfere with the data needed by other online businesses.[13]

We expect that the Government's legislative response to this issue will at best be uncertain and at worst a distant prospect. Indeed, we consider it to be unreasonable for the CMA not to address the issue now. This can be done with the powers currently available to the CMA either in a market study or following a full Market Investigation. We call for a full market investigation for the full range of powers to be used and note that lack of use of its powers following a Market Investigation (that started in 2019) means that UK consumers need the CMA to build on its strong work from the past three years. There is however a risk of this influential work going to waste unless more is done to address the root causes of market power. Indeed, since so little has changed except for the pandemic accelerating the shift to online and increased power of

[12] See Interim Report section 5 and 5.203 et seq.

[13] [redacted]

the platforms [14] we believe the time has come for the CMA to step up and use its powers in the discharge of its public duty which, as above, is to *promote* competition.

In the following we discuss the issue of data trusts and data stewards as a mechanism for creating greater end user empowerment and as a vehicle for redressing to both behavioural and structural issues in the affected markets.

We consider that while all accept that data is critical for the development of online markets it is useful and important to separate out two basic categories of data: end user data and data used by businesses for business-to-business services. In the first category of end user data there is data that is private and personal and protected under data protection law. The second category includes such things as data used by online businesses to check and measure the effectiveness of different sales and marketing channels in promoting products for online commerce. The CMA has identified two different abuses with relation to data where some form of trust or stewardship could be useful as part of a remedy:

- exploitation of end user data;
- use and management of cross site measurement data (potentially through a shared, common or universal ID) [15] (business-to-business or B2B data). In this regard we appreciate the CMA statement concerning the common transaction ID that was contained in Annex Z of its Online Platforms and Digital Advertising Report when it observed:

  "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." [16]

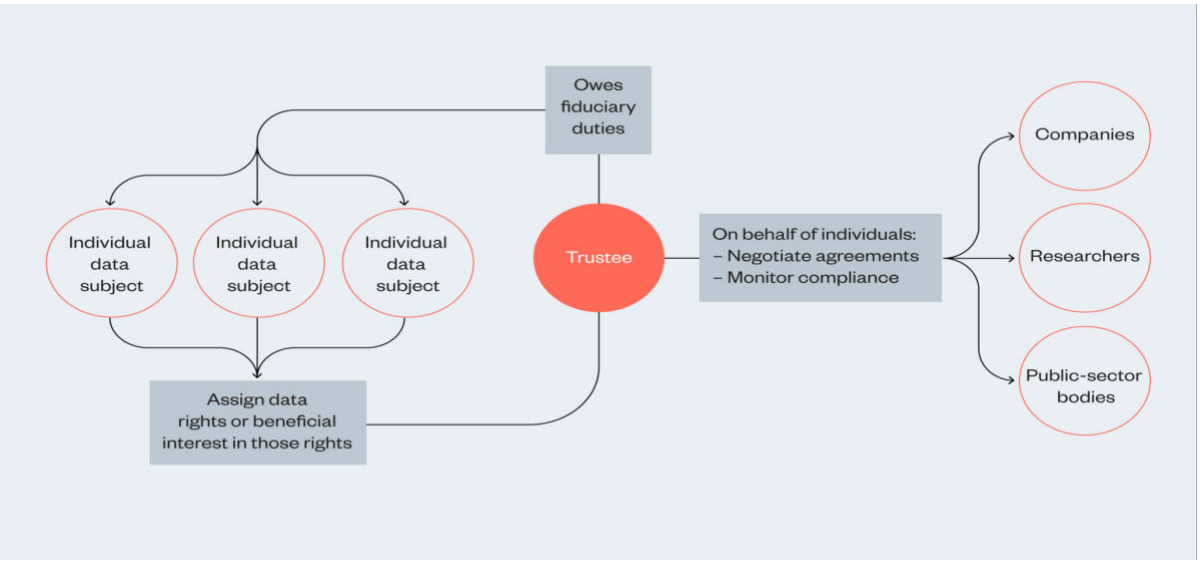
We provide an overview of data trusts[17] and stewards[18] and then review how a data trust remedy may help to enable and to promote competition. Certain issues with the use of trusts arise and we suggest that a decentralized network with a data steward that can help to manage a shared or common ID[19] is the most effective remedy. This is in line with the recent G7 Data Free Flow with Trust initiative.[20]

What is an end user Data Trust?

A "data trust" involves one party authorizing another party to make decisions about their rights, often over property.[21] This authorized agent becomes a "trustee" of that data owner's property, with a fiduciary duty

[14] See Para 7.76 et seq UK Competition & Markets Authority, "Online platforms and digital advertising" (2020)
[15] See CMA Online Platforms and Digital Advertising Annex Z and ISBA https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf
[16] See CMA decision on Privacy Sandbox and Appendix G for a discussion of identifiers, cookies and mobile advertising IDs, and proposals to limit cross-site tracking
[17] https://www.theatlantic.com/technology/archive/2014/08/what-if-people-could-subscribe-to-different-facebook-algorithms/378925/ and https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech
[18] See for example https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ and https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf
[19] As discussed by the CMA in Annex Z of its Digital Advertising and Online Markets Final Report
[20] that balances how to "facilitate data free flow with trust and drive benefits for our people, our businesses and our economies. We will do this while continuing to address challenges related to privacy, data protection, intellectual property rights, and security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2_Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf
[21] See Legal study on ownership and access to data - Publications https://theodi.org/article/what-is-a-data-trust. The Open Data Institute (ODI) was founded in 2012 "to connect, equip and inspire people around the world to innovate with data."

to act in the property owner's best interest:[22]



"Beneficiaries" should thus be distinguished from the originating owner as well as from the trustee. The mechanism involves a "settlor" and "trustee" – terms borrowed from trusts law. A data trust thus is the collection of rights holders or beneficial rights holders that collectively grant the trustee the authority to manage their rights or assign them to other beneficiaries and enable the trustee to supply such information to other parties to produce greater benefits for the collective benefit of the data settlors. The duties of the trustees as described in instructions and are imposed in equity under English common law.[23]

Use of End User Data Trusts to address Consumer Exploitation and Strengthen Competition?

The CMA has identified one competition issue of the monopolization of end user data via the browser, and the exploitation of end users by platforms not offering choice[24] and imposing unfair terms on end users. This is in part derived from the very considerable difference in bargaining power between the consumer and the trillion-dollar platforms. [25] This first abuse involves the capture of data from end users and their exploitation.

An end user data trust could be imagined as a remedy[26] to end user exploitation that could be set up to and for the benefit of end users, or categories of end users, aiming to trade with the major platforms on behalf

[22] Data trusts would provide a vehicle for individuals and groups creating a vehicle to state their aspirations for data use and mandate a trustee to pursue these aspirations. By connecting the aspiration to share data to structures that protect individual rights, data trusts could provide alternative forms of 'weak' democracy, or new mechanisms for holding those in power to account. Similarly, by enhancing consumer voices and collecting or pooling those voices with others in dominated markets they may promote competition.

[23] In 2004, Lillian Edwards proposed a data trust and a tax levied against profits earned by data controllers from misuse of private information. Many objections can be made to the use of trusts to share benefit from what may be the illegal obtaining of personal data, including the fact that government should not benefit from breach of the law nor can trusts legitimately be established for illegal purposes. The Edwards model proposing an early form of "data trust" also failed to distinguish between identifiers used for measuring the effectiveness of different channels of advertising, and personal information (since covered by data protection law such as the GDPR).

[24] Both in the Online markets Final Report and in its Privacy Sandbox Decision.

[25] The CMA should bear in mind the desirability of interpreting competition law in line with its consumer protection jurisdiction, e.g. s.62 of the Consumer Rights Act (invalidating anti-consumer unequal bargains unless prominent and clear, core terms (s.64).

[26] In October 2017, the UK government published its report on data-driven, automated feedback often referred to as "artificial intelligence (AI)". That paper recommended the creation of "data trust, to improve trust and ease around sharing data." These trusts were to provide a framework to facilitate secure exchange of information in a mutually beneficial way and to ensure a level playing field for all digital market participants. The trusts envisaged by the government was "not a legal entity or institution, but rather a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe and equitable way'. This paper is inspired by that report. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

of those end users and to obtain better terms from them to avoid "exploitation abuse". Indeed, the Ada Lovelace Foundation has suggested that:

> "Today's data environment is characterised by structural power imbalances. Those with access to large pools of data – often data about individuals – can leverage the value of aggregated data to create products and services that are foundational to many daily activities…."and
>
> "… By leveraging the negotiating power inherent in pooled data rights, the data trustee would become a more powerful voice in contract negotiations and be better placed to achieve favourable terms of data use than any single individual. In so doing, the role of the data trustee would be to empower the beneficiaries, widening their choices about data use beyond the 'accept or walk away' dichotomy presented by current governance structures."[27]

The following key issues arise with such trusts as remedies to the issue of platform market power:

- **Inequality of bargaining power, even with the trust:** Trusts have a major role to play in addressing high transaction costs preventing consumer sovereignty. That does not however mean that they would be in a strong bargaining position. No trust could ever expect to be able to trade on an equal bargaining position with the major platforms. Every trust is faced with a monopoly platform that is global and has almost limitless resources. There are no meaningful alternatives to the platforms for the services that they offer. Each platform is in such a position of 'ultra' or 'super' dominance that is entrenched and enduring and any trading partner will be at an enormous disadvantage. Trading terms can thus be imposed by the platforms on any data trust created to represent the interests of end users - which would suggest that the creation of the trust would fail to address this core issue of difference in market power and bargaining position, and without further intervention from competition authorities concerning the terms on which trusts would trade with the platforms, exploitation of the trust by the platforms would be the inevitable outcome.
- **Putting consumers first:** Each trust will, on accordance with its fiduciary duties, act in the interests of their beneficiaries/end users. [28] The short-term interests of end users could be expected to include receiving current services on the best available terms. Since the trusts would be dealing with one size fits all terms imposed by the platforms, and there are no meaningful alternatives, the trustees would find it difficult to either imagine or obtain other terms and would be duty bound to accept terms offered by the platforms, in the best interest of their beneficiaries. Again, unless the competition authorities were to intervene and address the issue of the terms of trade imposed by the platforms, a trust would not add much to a remedy.
- **Scale issues:** Practical barriers to entry for a new data trust in engaging with sufficient number of end users and in building scale for their activities in competition with the established platforms are likely to be legion. Lack of visibility, lack of funds for advertising, the need to advertise through online platforms that have no interest in promoting a competitor are just the start. Funding is unlikely to be forthcoming and the huge investments in intellectual property, systems and software that have been sunk by the established platforms are unlikely to be overcome in the short to medium term, if ever. The theory is thus unlikely to leave the drawing board.
- **Possible issues in abuse of trusts, e.g., monopolistic tying into browsers:** End user beneficiaries would benefit most from a trust that would promote competition. Such a trust would need to sponsor alternatives and enhance the market power of the competitive fringe of new entrants and under

[27] https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/#fnref-14

[28] Akin to the fiduciary duty for a trust, but slightly different (as the trust may legitimately profit provided this profit is based on consumer-friendly competition – the same reason why a bank cannot be a fiduciary regarding its accounts (the bank profits)).

scale businesses in the medium-term interests of both end users and new entrants. This type of trust would support the longer-term interests of society in benefitting from competitive markets. Such a trust might need to be coupled with other remedies to prevent the capture and bundling of data into the platforms' browser, and remedies designed to allow supply chain and ecosystem partners access to platform data used for cross site measurement and competitive effectiveness and assure non-discriminatory interoperability.

It is also legally and theoretically possible for 'mixed trusts' to be created whereby the trust structure can be used for the benefit of those that are adversely affected by platform abuse of dominance and misuse of data.

Two main issues can be foreseen with a 'mixed' trust of this type: firstly, the beneficiaries' interests are different, and the balancing of interest and decisions taken by trustees may lead in practice to differences about how that balance is to be achieved and hence to disputes and disagreement. Secondly, a data trust for end users can increase the social welfare of a community of users where control has been delegated to the trustee to act in the interest of the end users - this may involve control for data protection purposes residing with the trustee organization and the delegation of greater levels of control than end users are happy to consent to. Another practical issue is that the position of trustee involves decision making and control and systems and processes set up for that trustee may tend to centralize control in ways that prevent a more flexible business arrangements where more ad hoc networks of complimentary and different businesses may join and leave easily, which might facilitate more entry and expansion and be more amenable to contractual agreements.

Involvement of regulatory authorities and monitoring trustees to secure the interests of competition and promote competitive outcomes in the context of competition law remedies

Moreover, the debate about end user data overlooks the important role of business-to-business data-driven applications.[29] The CMA has recognized the importance of advertising data for business in selling products. Both online intermediaries and Google and Apple provide verification and attribution services which involve the use of data in business to business (B2B) applications. Their ability to collect data from third-party sites and apps, and to combine it with analytics data to present a unified view of campaign performance to advertisers, or other measurement and evaluation systems, is very important for digital advertising and other online systems' performance management. Indeed, without it, the success of one campaign or another or one channel or another can't easily be measured.

At present, however, these data flows are significantly distorted by market power.[30] Google has a competitive advantage in terms of being able to carry out assessments of advertising effectiveness throughout both Apple and Google's online ecosystems and accurately define attribution for campaigns

[29]Important to distinguish that the data that informs these business-to-business decisions is NOT related to businesses but involves how they are delivering value to their business customers. For example, paid advertising to consumers is a business decision, by a business, for the benefit of a business To be clear, these are the Data Protection Act-compliant uses by business, with business, of privacy-by-design data (e.g., data applying state of the art pseudonymization with no identity revelation risk, and the use of this data to optimize and advertising campaign).

[30] CMA Annex Z recognized: 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.

that advertisers run, at least in part, on their own 'walled garden' platforms: and its relationship with Apple, through which it pays apple $10-12bn per annum also provides it with additional data.[31]

Restrictions on third-party access to granular analytics data on the platforms give them a competitive advantage in measuring advertising effectiveness. This has several implications for the role of data in digital advertising. The CMA has identified that platforms such as Google and Meta (formerly Facebook) may misuse intermediary data that they gather about the effectiveness of different systems and processes, such as how effective different channels are in promoting products to end users. The CMA has decided in its Privacy Sandbox enforcement Decision that self-preference and discrimination against B2B rival ad tech providers is also an abuse of dominance.

Currently, the system adopted by Apple also gathers data and both Apple and Google use it for advertising and promotion of their products in their ecosystems. It is well established in multiple decisions[32] that that Google operates a self-preference business system. What is less well understood is that Apple takes substantially the same approach and has introduced browser restrictions (in its Intelligent Tracking Prevention or ITP project) that benefitted its own apps store promotions and pop ups.[33] The CMA's Mobile Ecosystems investigations is concerned with apps stores and apps. The extraordinary rise of Apple in the past 2-3 years in the business of apps advertising with Apple. This increase took place after Apple decided that users would be "opted out" of advertising tracking by default under its ITP and ATT changes. This left rivals such as Facebook, Google, Snap, Yahoo and Twitter "blind", in the sense that they had no data at B2B level.

Since April 2021, data on how users were responding to ads, once real-time and granular, is now delayed by up to 72 hours and only available in aggregate. By contrast, Apple offers detailed information to anyone signing up to its ads service and should investigate the following:

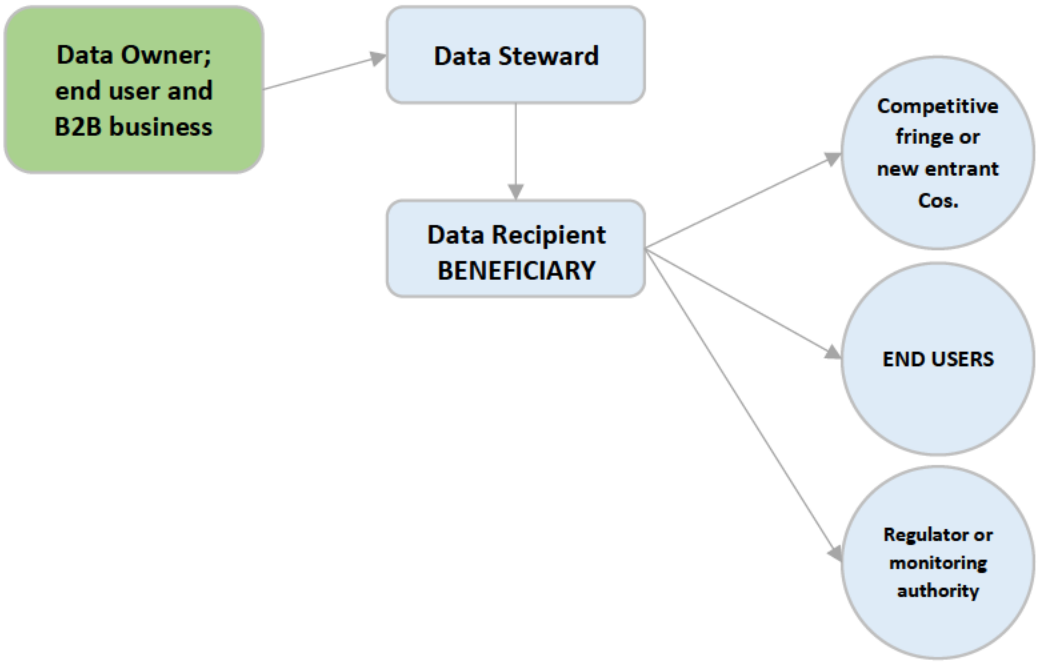
[31] See [redacted] https://support.google.com/admanager/answer/7560930?hl=en

[32] See EU Commission CASE AT.39740 Google Search (Shopping), EU Commission CASE AT.40099 Google Android and the CMA Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals.

[33] See for example Apple's ITP abuse and its ATT advertising preferential arrangements that have generated increased benefits for Apple. See [redacted] Patrick McGee's article at https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d?sharetype=blocked.

We suggest that these harms should be prohibited and policed through access and interoperability conditions together with measures taken to address both unbundling and non-discrimination as outlined in the Interim Report. However, if access, interoperability, unbundling and non-discrimination remedies are to work well, we believe that the root of the problem requires both the prevention of consumer exploitation, the prevention of B2B business benefit only for the platforms and the promotion of competition via entry and expansion of the existing competitive fringe.[34]

The promotion of competition objective that is contained in the CMA's markets regime[35] can be supported by the creation of data stewards over a shared or common ID that would enable entry and expansion. End users could sign up on standardized contracts on fair reasonable and non-discriminatory terms so that consumers can exercise meaningful choice and that safe, interoperable data access can then take place. End users (individuals) could also be parties to a stewardship agreement alongside those competitors that are designated by the competition authorities to promote competition. This is outlined in the diagram below:



Examples of these data stewardship organizations could include combinations of Personal Information Management Systems (PIMs), Digital Wallets and other Privacy Enhancing Technology (PET)[36] that could

[34] The limitations of consent as a model for data governance has been widely canvassed. Many terms and conditions are lengthy and difficult to understand, and individuals might not have the ability, knowledge or time to adequately review data access agreements; for many, interest in consent and control is sparked only after they have become aware of data misuse; and the processes for an individual to enact their data rights – or receive redress for data misuse – can be lengthy and inaccessible. See https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/#fnref-8 See further: British Academy, techUK and Royal Society (2018). Data ownership, rights and controls: seminar report. [online] The British Academy. Available at: www.thebritishacademy.ac.uk/publications/data-ownership-rights-controls-seminar-report

[35] Enterprise and Regulatory Reform Act 2013 s.25(3)

[36] There are 2 families of PETs (See https://research.aimultiple.com/privacy-enhancing-technologies/). Those that require an organization to send data to a centralized gatekeeper that controls the processing (e.g., Multi-party Computation, Differential Privacy, and Federated Learning) e.g., Apple's Child Sexual Assault Material scanning of people's local devices relies on these BUT Apple explicitly states it can re-identify any customer with its technology "CSAM Detection enables Apple to accurately identify and report iCloud users who store known Child Sexual Abuse Material (CSAM) in their iCloud Photos accounts." https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf

all operate on access and interoperability agreements overseen by competition authorities and to protect sensitive, directly identifiable personal data, and provide consumers with enhanced control over which organizations can receive their personal information.

There is a significant role for competition law to play here. Absent guidance, there may be risks in advocating a cross-party agreement, and an unpredictable enforcement risk may discourage innovation in the consumer interest, simply because there is thought (incorrectly) to be a risk under Chapter 1 from such interactions. There is also a role for a legal device to make it clear that such network rules bind third parties, just as shareholders are bound to their fellow shareholders, regardless of contractual privity, by a statutory device.[37] This would give network rules real teeth, and strongly enable innovation.

We do not, however, advocate centralized institutions. These do exist and do manage the collective data in centralized organizations can be found in the UK government-funded Open Data Initiative's Sharing Cities Programme, that means sensors in public buildings and parking lots can be used to inform retrofit investments and vehicle navigation, in the public interest.[38] Another is the e-bikes loan scheme where individuals' journeys were monitored by GPS to help inform city planning and locate collection points more effectively.[39]

It is important to note as described above that no amount of centralization of control will even up the bargaining power of end users or competing companies with the platforms. Indeed, the network effects at the heart of concerns with platforms would, if anything, be amplified by a centralized model.

Instead, the competitive fringe needs amplification and could be identified by competition authorities, with intervention taken to support expansion and new entry through access to data from the platforms and regulated interoperability. We suggest that networks of companies that would be simple and quick to join (and leave) is to be preferred. As with other regulation designed to create competition, such as EU telecommunications laws, alternative networks would need to be promoted, and interoperability agreements subject to regulatory oversight, but the success or otherwise of one or more specific competitor or networks of competitors would be left to the market (and end users) to decide.

It is to be emphasized that alternative networks could operate in decentralized ways, with support from competition authorities allowing collectives to operate together to address market power and flexibly and in their different ways preserve and promoting innovation, avoiding the risks of becoming centralized managers, or become entrenched in a trust-based system that could well be less innovative.

The potential role of data stewardship to promote competition and safe use of the internet outside of a formal trust

While data protection law obliges meaningful consent to be obtained, dominant B2C internet providers do not provide people with choice to keep their identity distinct from this software (e.g., logging into Gmail automatically logs consumers into Chrome). In contrast, in a competitive market, people would be able to navigate online without tied data collection practices as condition of access as they must do when accessing

Those that enable an organization to rely on privacy-by-design interoperable identifiers to choose which partners will process the data (e.g., pseudonymized, "Random IDs" OR "data masking" like de-identification) e.g., Apple's Privacy Policy (see News + Siri, rely on this) "Apple News delivers content based on your interests, but it isn't connected to your identity. So, Apple doesn't know what you've read. close More about Apple News. Many news sources keep track of your identity and create a profile of you. Apple News delivers personalized content without knowing who you are. The content you read is associated with a random identifier, not your Apple ID." https://www.apple.com/privacy/

[37] In *Globalink Telecommunications Ltd v Wilmbury Ltd & Ors* [2002] EWHC 1988 (QB)), Justice Stanley Burnton said: "The Articles of Association of a company are as a result of statute a contract between the members of a company and the company in relation to their membership."

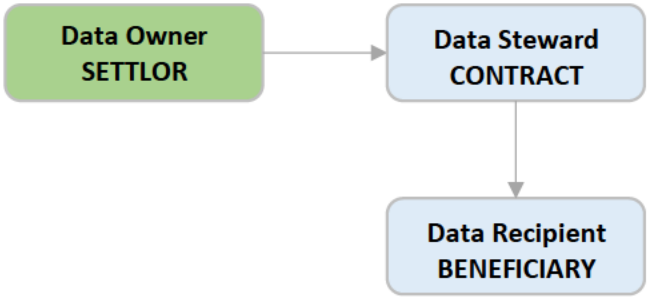
[38] https://www.sharingcities.eu/sharingcities/resources

[39] https://www.bikebiz.com/smart-cycling-project-launched-in-manchester-and-dublin

many Google and Apple services at present (indeed, the UK ICO has noted that conditioning excessive data collection in this way may well breach data protection law (especially, data minimization duties). [40]

Independent technology and ad tech providers need only truly anonymized or pseudonymous IDs, ("Random IDs" in the parlance of Apple's privacy policy, which are not linked to identity)[41] to supply access to the ad-funded properties which are the prevailing business model of the Open Web.

If a stewardship relationship could be established, whereby the steward is obliged by contract to operate to and for the benefit of other beneficiaries that each abide by a contractual use which restricts specific data processing, that could reduce the privacy risks to end users and create a collective system. That collective system could be set up among the current competitive fringe with the express purpose of promoting competition as part of a competition law remedy,[42] and much could be done to redress the market power of the platforms and create greater benefits for end users.[43] A simplified view is provided below:



We are suggesting here that the central idea of stewardship of assets for the beneficiaries can be combined with contractual arrangements between end users and businesses that promote competition, thereby securing a role for the market in setting remedies that will enable entry and competition, over time, in competition with the prevailing platforms. As above, a legal device would be needed to deem the contract binding on all, much as companies' articles are deemed to bind successive shareholders regardless of privity.

Examples of these forms of data stewardship arrangements are regulatory and technology frameworks that help facilitate exchanges of non-sensitive information by eliminating unnecessary friction.

Practical issues for data stewards

A motivating principle behind establishing a stewardship system is to manage a set of benefits among the data owners, both those originating the data and those creating databases and add additional technology and measurement systems and processes that increase the value of that data.

The steward could be required to operate according to a set of principles. We outline some practical issues and potential answers below:

[40] AdTech Opinion of 25 November 2021, p. 28
[41] https://www.apple.com/privacy/ (see in particular Apple's use of Random IDs to operate their ad-funded News and Siri services).
[42] "Constructive trusts," also called "implied trusts," can also be found to exist by courts and created via conduct rather than established by a settlor. As researchers Bianca Wylie and Sean McDonald wrote in 2018: Fiduciary data trusts aren't organizations; they're contracts that give a trustee, or a group of trustees, authority to make decisions about how an asset — say, data — can be used on behalf of a group of people." It is important to highlight that the data trust increases the social welfare of the community of users, rather than focusing on increasing the control of each distinct user who by definition has delegated control to the trust framework.
[43] https://www.cigionline.org/articles/what-data-trust

- Q: What is the purpose of the steward? A: to ensure compliance with privacy laws and promote competition.
- Q: What are the duties the data steward has with regard to the data? A: ensure compliance with data protection laws.
- Q: What is the decision-making process associated with distributing the data to beneficiaries or benefits back to data owners? A: determined under contracts between the members: a not-for-profit organization might be used as a vehicle for decision making among members.
- Q: How is the data trust funded? A: by members either by way of subscription like a buyer's club or from advertising.
- Q: What mechanisms incentivize efficiency of operating the data trust? A: not for profit organization would have to operate to a published and transparent profit and loss account and report to members.
- Q: Should any data owner's rights be violated what is the appropriate recourse for that individual to seek redress? A: the steward could insure against this risk and take action on behalf of all when the eventuality arises.

Key success criteria for the establishment of an effective decentralized digital market steward would include:

- Standard contractual clauses used by all participants that govern that appropriate and prohibited uses of personal data, such as assurance that:
    - personal data shared will not undergo unauthorized re-identification;
    - personal data will not be joined with sensitive information;
    - people have the right to opt-into personalized marketing and easily opt back out again on any digital property that uses their personal information;
    - people have the right to reset their pseudonymous, random identifier at any time, and absent manual intervention this identifier will automatically reset to a new identifier; and
- Transparent, no-cost access to an accountable audit trail for organizations involved when matching content to people based on their data; and
- Multiple participants with different commercial models and additional features to support competition whilst operating to common rules for transparency and data sharing.

The roles in online advertising and competitive markets

A common misconception is who decides on the things people see online. The CMA found in 2020 that the things people see online are largely decided by the major platforms. Facebook and Google between them control approximately 80% of all online advertising.[44] However, the internet is not merely a "pull" of sending only the content expressly requested by a consumer.

Advertising is clearly needed as consumers don't know what they may be interested in and may not be certain about what they want. Advertising including the broader promotion of products for end use is thus vital to all trade and commerce. Benefits to the consumer include (i) free content such as videos that provide users with a taster or idea or of an experience and (ii) learning about a new product (holiday, car, shoes you don't yet know about, etc.).

Advertising is a "cost", but the ideal case is where the ad is most valuable to the advertiser by also being relevant to the user, both in the short and longer term. While marketers may hope the people who see their

[44]See CMA Final Report paragraph 5.362 and Annex F paragraph 53.

adverts will notice them, engage with them, and ideally remember the message long enough to inform them about the benefits of the brand, the primary goal of advertising is often not in response to people's requests for content – but to inform and promote what *might* be of interest and use.

The promotion of goods and services through the different forms of advertising is managed by intermediaries, marketers, who seek to identify groups of similarly situated users. Those users may not be potential purchasers in the sense of being one step away from being a buyer[45] but are identified by their likelihood or propensity to take an interest in a product and be somewhere on a shopping journey.[46] The immediate "customer" of advertising is thus the marketer, not an individual. The marketer's interest is to ensure efficiency in expenditure: consumers benefit from this operating efficiently.

Confusion of "Consent-Over-The-Control-Of-Personal-Data" and "Consent-to-Advertising"

Any consent-based approach to specific advertising begins with an assumption that the consumer knows what they want. A world where consumers know what they want is one where the individual can decide what content to receive or from whom to receive it. Such an assumption would create an anticompetitive "Catch-22" whereby consumers would only be exposed to advertising from brands they already know with limited ability for new market entrants to ever gain market share. Advertising that supports and promotes competitive markets is thus about the promotion of things consumers may or may not want and may or may not be interested in – informed by what others may have decided and what others have found useful.

Display advertising is less distorted by the dominant platforms and is vital for the Open Web. It relies on sponsored creatives to fund people's access to digital properties. With Display, advertising solutions rely on interests of an audience based on current context, geography and predicted interests combined with the amount a marketer is willing to pay to people that match these targeting dimensions. Yet the matching of content is a necessary but insufficient portion of how digital advertising functions. The real-time optimization is what supports all ad-funded digital properties. This optimization process requires a feedback loop of accurate information provided in a timely basis.

Importantly this optimization process does not need to link people's identity to the prior exposures across publishers that generate success events for marketers, and for most online properties they do not. Google and some other large online platforms such as Facebook being key exceptions to the rule.

Distinguishing competitively important "Data" for measuring advertising effectiveness from "Personal Data"

As the CMA is aware data used in programmatic advertising is vital for measuring the effectiveness of different online channels and promotional systems. It consists of identifiers (often called "keys") and information linked to these identifiers (often called "values" or "attributes"). The identifiers can be a city-code, a URL, or related to the user of the web-enabled application. We should bear in mind that information associated with content exposure or user interaction is not an identifier, such as the time an advert is displayed or when a user clicks. However, the identifiers are useful to controlling the frequency of exposure (i.e. reducing the number of displays to the same device), measuring the total audience reached (i.e. unique identifiers exposed to the same creative), and attributing value on marketers' properties back to media owners' properties (i.e. understanding which engagement tactics, even when only contextual targeting is

[45] And the CMA has previously noted in Online platforms and digital advertising market study that users search among as many as 9 different alternatives before deciding what to buy.
[46] See CMA Online platforms and digital advertising market study.

used, drive more value and hence deserve larger budget allocation or warrant paying higher prices going forward).

These identifiers and the information linked to them are both "personal data." However, data protection regulations incentivize businesses to rely on privacy-by-design techniques that keep the keys distinct from people's identity such as relying on pseudonymous and de-identified identifiers rather than those directly linked or linkable by the recipient to people identity. We note that data protection laws do not require technical impossibility of relinking to identity for a pseudonymous or de-identified identifier to be considered distinct from identity-linked data, as appropriate measures that can be either business process or technical in nature are explicitly referenced. Indeed, a responsibly run data trust has a major role to play in improving data collection practices, and in entrenching privacy by design, and it would be very unfortunate if data protection law were interpreted in a way that impeded this improvement from getting to the consumer.

As the CMA has noted in its Privacy Sandbox Decision, truly anonymized data is not personal data in any sense.[47] Yet Google's Privacy Sandbox relies on collecting people's personal data across different web properties as inputs to feed the business-to-business advertising uses cases involved in digital advertising. While the outputted data may in some circumstances be classed "anonymous," Google's B2B Ad Systems, which include Privacy Sandbox, process the same forms of input personal data as rival ad tech providers. This is the reality: as of today, there is widespread tied data collection, and intervention is required to enable innovation in currently foreclosed data management systems. The alternative is simply large-scale data collection: business as usual for the big platforms.

Use of Identifiers (IDs) for ads in programmatic advertising and intermediary ad tech businesses

All businesses need to promote their products. Competitive markets would not function without the promotion of the products consumers have yet to experience and have yet to decide that they want. A common misconception is that advertisers are interested in "surveillance" and taking personal data – as intermediaries they are interested in which channel to market is working better than others in driving visibility of adverts so that end users see them as well as in the effectiveness of channels in driving sales.

It is important to note that advertising identifiers enable these intermediary marketers to look at the competing alternative ways to reach the end customer. Marketers focus their limited media budgets, measure which channel to market is working, and optimize their budgets to improve their return on ad spend (ROAS or Return on Investment ROI- which is the basis on which the industry is paid).

To understand the relative value of two digital channels to market and pay the relevant channel for assisting in a sale, the marketer needs to know which outlet drives more traffic, customers and sales ("attribution"). Attribution is required even when engagement relies solely on contextual targeting (such as advertising in a page about "travel". Attribution requires a common identifier for the ad that links its exposure on each publisher's property to the subsequent visit and purchase. The information required for efficient and effective Display Advertising thus relies on using non-sensitive information linked to pseudonymous, random identifiers for identifying ads, not end users.

The ability of digital systems to provide such specific feedback and show how online channels increase visibility and drive increased sales is the main reason for the growth of programmatic advertising.[48]

[47] See paragraph 4.47 of the CMA Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals.
[48] High scale data and access to aggregate data from multiple sources also improves the confidence of predictions. When the mechanism is impaired, by restricting data used for interoperability or if a major platform owner interferes and feeds in less accurate data, less granular data or less timely data, the algorithms struggle to estimate the appropriate pricing resulting in less effective return on ad spend.

Thus, programmatic advertising relies on non-sensitive data linked to pseudonymous identifiers to improve engagement, measurement and optimization. For example, a tech business helping a travel company advertise to people most likely to purchase a foreign holiday which creates an algorithm to predict when people are likely to buy does not need personal data. It may find that advertising sunny places to people in the dark days of winter is successful. However, if a platform changes its browser to limit the functionality of one type of cookie or another (as is being done by both Apple and Google) then measuring effectiveness of advertising channels will mess up the marketer's ability to assess competitive advantage and anticompetitive abuse will have taken place.[49]

It should also be noted that a responsible identifier system is necessary to allow certain rights to be exercised, e.g., the right to erasure. If there are data troves linked to users, then the only way for these to be reset is via some type of identifier to allow that to happen.

How would stewardship and contractual mechanisms work?

Data-sharing agreements among system members could be created with a very clear purpose in mind, and the rules and documents could be made public to increase transparency. A data contract will be needed to be established to govern how data will be processed. The governance framework could contain provisions around who will be permitted access to data, for what purpose and under what circumstances. The governance arrangements will include mechanisms for appropriate auditing and ensuring that data users have adequate remedies if compliance fails.

The stakeholders could establish a company limited by guarantee (CLG) to document the process and manage the framework for responsible, interoperable data sharing with its members being participating schools – both state and private, academies, further education bodies and data providers.

Per the above, advertising is B2B processing of data primarily for business purposes – the various supply chain functions and entities are not known to consumers and frankly they have no interest in being informed about how the proverbial sausage is made. Thus, the agreements on restrictions on use are set up by the steward to govern the B2B supply chains, some of which are controlled by buyers and others by sellers.

So long as the agreements are protecting people's human rights as outlined in data protection regulations and European law, then the stewardship agreements could provide people more choice and value than gatekeepers with whom they have no alternatives.

Why would a stewardship model be more likely to work when an end user data trust would not?

The issues that would mean a data trust is likely to fail concerning end user data trust being used to create an equality of bargaining power with Google and Apple. This issue is not the aim of a common ID steward model as outlined here. By comparison, each business that uses the common ID is free to operate independently and to compete independently and succeed on its own merits. Each will have an aligned economic incentive to promote their own products and services, and while the online media market participants are much smaller than Google or Apple, they can be expected to promote their alternatives individually and collectively to advertisers and publishers.

We expect that advertisers and publishers would welcome the opportunity to by-pass Google and Apple. Indeed, they sought to do so through the creation of the header bidding system that was, al be it briefly,

[49] The recent disclosure of Google's strategy to substitute its own advertising solutions for the competitive open market, by bundling these B2B offerings with their dominant B2C consumer software, begins with impairing rivals' access to interoperability identifiers and any information linked to them.

successful in enabling an alternative system to thrive. It was also effective in bringing prices for online advertising down while it lasted. This is a real-world example of the opportunity for innovation that a data steward model may allow the market to repeat.

Further, a data stewardship model that removes the ambiguity concerning compliance with privacy laws and people's reasonable expectations of digital services will guarantee people's privacy rights and advertisers and publishers adherence to laws removing uncertainty, and also encourage investment on new value adding features and services.[50] People will become familiar with the data stewardship model and have consistent expectations as they traverse multiple digital services. Google and Apple might also wish to adopt the data stewardship model.
Also, a stewardship model operates at the level of B2B activity and is intended to enable the coordination of technical systems that would help advertisers to individually identify the most effective and successful channels to market. As such, it would improve their separate ability to meet end user needs. Since advertising operates on a model of delivery of increased returns on investment, a stewardship model that supports a shared or common ID would increase the intensity of the competitive fringe. Increased competition of that remaining competitive fringe with the main platforms of Google and Apple, would necessarily be designed to promote competition where, today, competition is increasingly difficult.

The difficulties that are faced by competitors arise from the actions of Apple and Google: under either their restrictive practices known as ITP or Privacy Sandbox respectively. Each of ITP and Privacy Sandbox involves the gatekeepers in misusing their dominant market positions and blocking or interfering with the competing activities of other publishers, advertisers and intermediaries, for their own benefit.

Seen in this context, a stewardship model can be viewed as a necessary part of a remedy that supports access and interoperability in the context of online advertising. This is necessary since the prevailing business model operating in online mobile ecosystems is advertising. Without some form of common ID or a mechanism for a common ID to be used by competitors, even if unbundling or other access and interoperability obligations were imposed as remedies on the platforms, they will continue to dominate their mobile ecosystems.

Recommendation

Data Trusts, as described above with relation to end users are unlikely to be useful or helpful to enable competition in digital advertising markets. However, stewardship agreements could be used among digital marketers and ad tech intermediaries as part of an access and interoperability remedy that is designed to amplify the effectiveness of the competitive fringe in competing with the major platforms. This could be considered a best practice as regards data collection and will enhance competition with the more invasive, tied data collection practices.

We suggest the CMA consider a contractual framework among ad tech businesses and the sharing of common ID data could be created as part of an access and interoperability remedy. Previous access regimes have been used as remedies to similar issues of vertical integration and foreclosure but have not needed to address the particular characteristics of the advertising markets.

The CMA could further consult on the terms and conditions of data sharing that supports competitive, decentralized market actors, and would be a positive step forward in returning a level playing field to digital markets.

[50] Rather than having talented people spending days reviewing proposals privacy will be solved and they can deploy people and capital on other innovation.

We think that mobile ecosystems have been dominated for so long that such a framework would be needed to not only supplement prohibitions on exploitative terms, unbundling and non-discrimination remedies but also to ensure that healthy privacy compliant competition is developed.

Our focus is on a truly anonymized data that would support the promotion of advertising competition across digital markets. The benefits of such a model would be easier data interoperability, which improves efficiency and reduces waste – thus providing greater value to marketers, media owners, and most importantly people who access digital properties. This framework would create an environment for innovation and would enable the UK to provide a model example for other digital economies. It would introduce a pathway for competition over data protection quality, not unlike a Fairtrade certification scheme, which also addresses ethical issues in complex supply chains.

Nascent versions of these data stewardship systems exist in the form of SWAN.community[51] and Prebid.[52] Further explanation of such organisations can be arranged, but the purpose of this paper is to outline how these types of system can be used as part of the remedies available to the CMA and as matters to be further explored in promoting competition.

[51] https://swan.community/
[52] https://prebid.org/