

DATE: 07 FEBRUARY 2022

**MOVEMENT FOR AN OPEN WEB
RESPONSE TO CMA MOBILE ECOSYSTEMS
MARKET STUDY INTERIM REPORT**

INDEX:

I. INTRODUCTION AND SUMMARY 3

II. THE 4 OR 5 PROBLEMS AND EXTENT TO WHICH THE OPEN WEB CAN BE USED TO SUPPORT COMPETITION..... 6

III. THE BROWSER AS A TOOL IN THE HANDS OF THE END USER..... 12

IV. ISSUES TO BE ADDRESSED: CLAIMED BENEFITS 12

V. INCENTIVES IN MOBILE ECOSYSTEMS: IMPACT ON INVESTMENT IN THE OPEN WEB 13

VI. APPLE AND GOOGLE’S INCENTIVES TO INCREASE FUNCTIONALITY AND CONTROL OVER SUPPLY CHAIN AND ECOSYSTEM CAPABILITIES BY INCREASING FUNCTIONALITY IN THE BROWSERS AND SPURIOUS MISUSE OF SECURITY ARE COORDINATED 16

VII. CMA PROPOSALS AND QUESTIONS: MOW’S OBSERVATIONS ON REMEDIES AND THEIR EFFECTIVENESS 17

VIII. PRIVACY AND SECURITY AS NON-PRICE FACTORS OF COMPETITION AND THE NEED FOR INDEPENDENT SOURCES OF TRUTH, CERTIFICATION, AND VERIFICATION (PER CHAPTER 7) 22

IX. MOW PROPOSAL FOR BROWSERS: ESSENTIAL INPUTS THAT NEED TO BE TREATED AS SUCH AND OPERATE TO THE USERS’ INTERESTS THROUGH SYSTEMS THAT OPERATE UNDER FUNCTIONAL SEPARATION AND NON-DISCRIMINATORY INTEROPERABILITY 24

X. CMA CONCERNS TO BE INVESTIGATED..... 27

XI. OVERDUE NEED FOR EFFECTIVE REMEDIES AND ENFORCEMENT ACTION 27

I. INTRODUCTION AND SUMMARY

1. Movement for an Open Web (“MOW”) is a not-for-profit company limited by guarantee, set up with the object of safeguarding a competitive and open internet. Its members include a number of large and small online businesses, including analytics companies, digital advertisers, publishers, and broadcasters. MOW responds below to the CMA’s Mobile Ecosystems Market Study (the “Study”) Interim Report (the “Report”), published 14 December 2021.
2. In summary, MOW highlights the following points:
 - 2.1 The platforms have gone much further than the CMA has currently identified in abusing their market power over consumers and suppliers. Their respective dominance allows them to control end user data, shape demand and influence consumers to develop habits that prevent or restrict competition.¹ The report also overlooks the CMA’s previous findings on the importance of enabling end users to choose.²
 - 2.2 Further work on remedies³ is now needed to address accumulated benefit, for example the brand value and visibility of the platforms over their rivals. That accumulated benefit is derived from abuse. It continues to restrict entry. Cross promotion of alternatives can be used to address lack of visibility but needs to be tested for effectiveness and reach before being deployed.
 - 2.3 All alternative suppliers depend on browser and search gateways for data, and MOW

¹ This is achieved through promotional and marketing activity, and the use of behavioural economics, which is unaddressed by the CMA report. Some elements of presentational abuse are addressed in the CMA’s Final Report into Online Markets and Digital Advertising, where dark patterns and shaping behaviour to, for example obtain consumer consent is noted. However the systems go further, and involve continual and persistent cross promotion and promotion of owned products over rivals competing products, both a consumer level (see cross promotion of Chrome Sign In, and at business-to-business levels, see Google’s promotions of first party data systems to advertisers and its Customer Match program.

² Consumers need to be able to take an effective choice which means having alternatives to choose from at the point of making each decision. For instance consumers need a choice when considering sign into a browser, a website, or a system. They also need to have a choice over how their identity is used. Consumers collective decisions ultimately control the B2B decisions of the web properties they visit – and they can control how long their data is linked to them, and they should be afforded greater choice at each step of their journey. If consumer data it is not linked to their identity than business-to-business activity may be more easily facilitated. For example, a random ID as is used in SWAN see <https://swan.community/> enables people to reset it at any time –allowing consumers to exercise choice over suppliers. Whereas with Walled Gardens Google and Apple increasingly require multi-factor authentication linked to people’s identity to access functionality that does NOT require identity; thereby unnecessarily gathering more and more increasingly private data for their business use.

is concerned that the CMA assumes that choice and processing need to continue to be controlled by the browser owners, when there exists a choice mechanism from others and alternatives are available from rivals.

- 2.4 The Report also appears to accept that browser choice and competition is currently restricted for Google and Apple’s benefit (contrary to competitors and consumer’s interests). However, while the CMA accepts the need for unbundling and non-discriminatory behavioural obligations with relation to app stores (see pages 388-9), it does not then consider similar unbundling and non-discrimination obligations in relation to browsers. The CMA’s approach may thus be inconsistent, or the thinking at an early stage. MOW provides additional thoughts on remedies at data and browser level that encourage unbundling and non-discrimination at that level.
- 2.5 MOW agrees with much of the CMA’s analysis. However, while the “Open Web” is referred to multiple times, its capability to provide an effective alternative distribution platform for competing products and services needs to be further assessed. Remedies need to not only ensure that current abusive practices are brought to an end,⁴ but also that entry and expansion, especially by competitors using the Open Web, is properly supported.
- 2.6 MOW agrees that self-preferencing and discrimination are rife.⁵ However, ensuring non-discrimination is not simply about prohibitions or stricter enforcement, more flexible enforcement or codes of practice, and ex-ante investigations.⁶ Additional thought needs to be given to the incentives that exist in vertically integrated firms to continue to discriminate, and how their behaviour can be changed over time. MOW suggests the CMA consider greater use of data, operational, and functional separation remedies for browsers, in line with established practice and OECD studies, to change behaviour and ensure remedies work. CMA intervention should start with ensuring

⁴ As required by EU and UK competition law.

⁵ But, surprisingly, while the CMA lists many examples of anticompetitive activity it misses a major issue. Currently, Google and Apple also unfairly bundle their business-to-business functionality with their business-to-consumer software imposing unfair terms on consumers (by requiring their end devices to process data for the benefit of their businesses on preferential terms). This restricts competition by limiting the ability of rival business-to-business software to offer competing technology solutions to media owners or marketers

⁶ As contemplated for the DMU.

browsers operate independently and effectively as the user's agent, enabling access to a decentralised and competitive Open Web, as was intended at its creation.

2.7 The CMA also refers to the World Wide Web Consortium (“W3C”) as an independent standards making organisation. MOW raises concerns that the CMA's perception is different from the reality. [REDACTED]

[REDACTED] The European Commission has recently identified standards as a critical component⁸ for the future because interoperability and the ability to use individual components, access to API etc. are all dependant on an effective and properly independent standards making system. MOW believes the CMA needs to coordinate more closely with its international colleagues and notes that whilst the CMA has identified little wrong with the W3C, both the EU and the Department of Justice are concerned about its operation: *“Today, European experts and national standardisation bodies remain important players, but the geopolitical landscape has significantly shifted in recent years: other actors follow a much more assertive approach to international standardisation than the EU and have gained influence in international standardisation committees. The EU's objective is to shape international standards in line with its values and interests, but it is in strong competition to do so. The EU and its Member States must promote a more strategic approach to international standardisation activities, namely in the International Telecommunication Union (ITU), the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), but also in other relevant global partnerships, fora and consortia10”*⁹ (fn 10 includes: E.g., 3GPP, OneM2M, IETF, IEEE, W3C, OASIS, ECMA International, UN/CEFACT). MOW considers that the CMA needs to take a more strategic approach.

3. Overall, MOW is concerned that unless Apple and Google's incentives change, their anti-competitive behaviours will continue. The Report, while it identifies key issues, does not sufficiently address the question of incentives in changing behaviour which MOW submits should be the aim of remedies.

[REDACTED]

⁸ [DocsRoom - European Commission \(europa.eu\)](#)

⁹ See Section IV on page 5 of the “An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market” at [COM 2022 31 1 EN ACT part1 v5.pdf](#)

4. MOW sets out below how the Open Web can provide a platform for decentralised competition, and some approaches to improve the operational effectiveness of remedies, taking account of remedy design and how remedies to vertical integration have been applied in many other similar situations.

II. THE 4 OR 5 PROBLEMS AND EXTENT TO WHICH THE OPEN WEB CAN BE USED TO SUPPORT COMPETITION

5. The CMA invites comments on positive interventions (such as break up), fearing that the (very limited) benefits it has identified may be lost if intervention were to take place without care and attention.¹⁰
6. Most significantly, however, the CMA notes that the “*level of control exerted*” by Apple and Google in relation to operating systems, app stores, and browsers means that it is very difficult for another competing ecosystem to emerge. So, it recognises that market power exists over consumers, suppliers, and rivals. Competition from the Open Web is thus stifled.¹¹ How the Open Web could once again be a source of effective competitive constraint should now be in the spotlight.
7.
 3. The CMA identifies 4 types or themes of anticompetitive practices:
 - 7.1 Market power in the supply of mobile devices and operating systems: users don’t switch between systems.
 - 7.2 Market power in the distribution of mobile apps; Apple and Google control the distribution of native apps on their own apps’ stores.
 - 7.3 Market power in the supply of mobile browsers and browser engines from restrictions within iOS on browser engine choice, web standards and webpage compatibility, exclusive control over businesses’ payment systems for their consumer-facing services, consumer behaviour, and the role of pre-installation and default settings for browsers on mobile devices.
 - 7.4 Market power over app developers from controls over app stores that allow the platforms to set the rules of the game (and rig them in their own favour), restrict hardware and software functionality, change rules for own benefit, set opaque rules and

¹⁰ See Section IV below.

¹¹ Or other alternative distribution platforms such as Smart TVs

discriminatory preinstallation practices and design of app stores, ranking of results, exclusive control over businesses' payment systems for their own benefit. These are types of behavioural abuse that stem from a central structural control over both consumers and the members in each ecosystem.

8. There is perhaps a fifth area of concern that the CMA has previously identified which is highly relevant to mobile ecosystems and is unaddressed in the Report: control over end user sign-in data. The interventions noted by the CMA do not yet address this issue. This control happens in multiple ways, such as bundling of sign-in, restrictions on interoperability among media owners and their partners, or restricting the ability for businesses to collaborate absent interference by the gatekeeper. All lock in gatekeeper control over end users, from which market power, for example in advertising-funded search, is then derived. As discussed in Annex Z of the CMA's Online Platforms and Digital Advertising Market Study Final Report, control over end users and their data is central to platforms' market power and their ability to manage their ecosystems.
9. MOW notes that internet gatekeepers often confuse matters around user data. They raise privacy concerns. MOW agrees that legitimate concerns exist in relation to the collection and processing of identity-linked data, as addressed by data protection legislation, especially when it contains sensitive information. However, internet gatekeepers do not rely on distinctions recommended by the Information Commissioners Office and other data protection regulators. For example, they ignore the prospect for end user consent or control for use by rivals and how techniques to reduce risk can solve these issues. Using addressable identifiers not linked to identity is an important element. Using innocuous, non-sensitive information for legitimate business purposes is another.¹²
10. MOW agrees with the Report's observations that Apple and Google do not currently face competitive constraints in all areas of their activity from Open Web alternatives. The current position is the outcome of many years of unaddressed abuse. Recovery from that abuse will take time. The competition which survives differs at different levels in each ecosystem, and the depth of investment varies throughout the ecosystems. Nevertheless, a "competitive fringe"¹³ does still exist in many markets.

¹² See for example SWAN.Community

¹³ As described in Case T-201/04 *Microsoft Corp, v Commission*

11. The issue for the CMA to address in the next six months is to develop a framework for remedies to that abuse which can foster both investment, innovation and competition. A better and more detailed understanding of the existing capabilities of business activities by market and market segment using the Open Web is needed. That assessment would aim to understand those businesses that operate using Open Web functionality and their individual and collective capacity to provide competitive pressure to the platforms. Looking ahead at what can be done to encourage investment over time will also be needed.
12. The underlying investment in the mobile and fixed communications infrastructure used by mobile ecosystems and the Open Web, based on a series of standards and protocols that overlay heavy and historic investment in communications systems, is vast. So, when considering how Open Web-based alternatives can add competitive pressure, it can be recognised that much of the cost of entry, even globally, is likely to be from applications that run on top of existing infrastructure; they can rely on these existing investments. Entry may be easier as a result.¹⁴ However, one, risk is to expect entry absent restrictions. Existing capability and new entry may also need to be nurtured and supported during the transition period in which Apple and Google's restrictive practices are brought effectively to an end. For example, unbundling of apps from payments systems may not be sufficient. Unbundling of browsers from platforms may not be sufficient. Banning restrictions may not be sufficient. In addition, to address accumulated brand value and lack of visibility, promotion or cross promotion of alternative browsers, web apps, technical services, products and solutions may also be needed.
13. Because Apple and Google's businesses include all levels of the ecosystem, and at each step they rely on dominance in adjacent markets to promote their own components and their own products over others, the CMA examination needs to look into what would be needed to promote healthy competition at each level and in each market segment, which could, with time, provide effective competitive constraints. Simply banning restrictions will not create entry and could destabilise existing investment and supply. Also, the withdrawal of the list of restrictions currently identified would not do enough to address the accumulated bargaining power vis-à-vis ecosystem partners and vis-à-vis consumers, nor address recognition and visibility and brand value that has accumulated as a benefit, following so many years of illegal activity, to Google and Apple.

¹⁴ The system of worldwide regulation, operating under the WTO telecoms package, provides for both regulation to restrain telecommunications players and promotes competition from alternative providers. This can enable "timely likely and sufficient" entry in each segment or area of the market

14. The platforms have gone much further than the CMA has currently identified in shaping demand and influencing consumers to develop habits that prevent or restrict competition. The CMA should further investigate:

14.1 Promotion, cross promotion and marketing and sales strategies.¹⁵ See for example Google and Apple’s proposals to further promote themselves as payment services suppliers in their browsers,¹⁶ their cross promotion of sign in to their products to enable each platform to obtain end user data and their misuse and promotion of the idea of “First Party Good/Third Party Bad” when considering data and the many sales, marketing, advertising, and influencing of consumer opinion with relation to first party data and collections of first party domain information, much of which may be privacy invading, such as Google’s Customer Match program.¹⁷ Importantly, promotion remedies have been tried in the past; see Browser Choice Screen remedies and API publication in the *Microsoft* and *Google* cases,¹⁸ but their limited effectiveness probably stems from their limited visibility and promotion to end users to ensure that effective choice actually takes place.

14.2 Misuse of standards and interactions at W3C.¹⁹ The European Commission has recently highlighted the importance of standards and standards making: “*A particular critical situation relates to internet standardisation to promote a free, open, accessible, inclusive and secure global internet. In recent years, international standardisation on internet protocols has become increasingly politicised, at the risk of limiting the evolution of the global open internet and hampering the digitisation process across the world.*”²⁰ The European Commission noted the importance of the W3C in this regard,

¹⁵ See EU commission decisions in *Microsoft* and *Google Search* and *Google Android*.

¹⁶ W3C payments issue, attached as Annex 1

¹⁷ Privacy Security and Safety. Here, the CMA has called out Apple and Google as often being “in the position of acting in a quasi- regulatory capacity in relation to users’ security, privacy, and online safety.” In many cases they opt to make decisions on behalf of consumers. However, it is not always clear if these numerous choices – ranging from restrictions on browser functionality to policies that affect targeted advertising – are in all cases made fully in the interests of consumers. For example, in many cases it seems decisions made on the grounds of protecting users’ security and privacy would also serve to give an advantage to first-party apps, or otherwise limit consumer choice of Open Web alternatives

¹⁸ See Case T-201/04 *Microsoft Corp, v Commission* and Case AT.39740 — *Google Search (Shopping)*

²⁰ See page 6 of the “An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market” at [COM 2022 31 1 EN ACT part1 v5.pdf](#)

- [REDACTED]
- [REDACTED]
- 14.3 Their individual and joint strategy of cynically playing on consumer concerns and fears over privacy (see the recently unredacted Texas AG litigation) to mislead consumers to join their walled gardens and keep them from using the Open Web.²²
- 14.4 The importance of addressing power over consumers and visibility in the design of remedies. The CMA’s current approach and outline of remedies falls short in its thinking about the importance of promotion, sales, marketing, and advertising. Attracting attention is vital if competing alternatives are to thrive.²³
- 14.5 Collections of consumers and demand aggregation may be a feature of enduring remedies. Data trusts and mechanisms to build data trusts should now be part of the CMA’s further examination of what is needed to truly remedy the position that it has identified.²⁴
- 14.6 Look more closely at the Intelligent Tracking Prevention (“ITP”) project, of which App Tracking Transparency or ATT is a subset. ITP operates in much the same way as the Google Privacy Sandbox – each element of which is questionable. See, for example, the Gnatcatcher IP cloaking proposal which the CMA accept is problematic but where Apple introduced a similar proposal, which has not been investigated, and which is now the subject of an EU commission complaint.²⁵ MOW provides further details in Annex 2 to this Submission.

15. The CMA could thus consider the extent to which:

- 15.1 It needs a mechanism to catch and consider further constraints and restraints on competition that it has not yet identified.

[REDACTED]

²² See CMA online gambling enquiry and Richard James, Claire O’Malley and Richard Tunney, October 2016, ‘Understanding the psychology of mobile gambling: a behavioural synthesis’, British journal of Psychology, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5516195/> article which considered how mobile phone use interacts with psychological processes relevant to gambling,

²³ See EU Commission investigation into possible anticompetitive conduct by Google in the online advertising technology sector at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143

[REDACTED]

²⁵ <https://medium.com/enrique-dans/why-telecoms-companies-are-angry-about-apples-private-relay-23157090dcab>

- 15.2 Demand aggregation systems and data trusts can be used to level up the bargaining position and power that the platforms hold over consumers.
 - 15.3 The Open Web can provide a competing platform with competing functionality (e.g., to enable other app stores to provide alternatives to the Google and Apple app stores, or how competing browser functionality can be sustainably developed).
 - 15.4 How such alternatives can be promoted, advertised, and sold when Google and Apple continue to operate their browsers as the windows on the web, for their own benefit and continually cross promote their own products.
 - 15.5 How the use of the Open Web can enable use of data centres or cloud computing platforms which could potentially enable higher computer processing at lower cost²⁶ for equivalent computer resource use but would be impeded by browser owners preferring their own internal systems and end device level computer processing.
 - 15.6 The extent to which higher levels of security are available from Open Web and cloud computing alternatives to those that are available within end user devices and walled gardens.²⁷
 - 15.7 The extent to which computer and communications infrastructure is used by both business-to-business and business-to-consumer industries, including the mobile ecosystems, and how common elements can represent common costs to functionally equivalent services which could be available to provide a timely, likely and sufficient alternatives to constrain the platforms' market power.
16. MOW would suggest that the CMA's focus can be on effective remedies in the next stage of the Study which requires greater understanding of Open Web functionality. This is both to examine how the Open Web's architecture can and does support alternatives and rivals such as web apps that compete with Google and Apple apps and app stores, but also to investigate why the shift of computing power from desktop to data centre that has taken place generally, with its increase in functionality, security, and cost savings available from cloud computing have not been passed onto consumers by the platforms' via their "Walled Gardens".

²⁶ <https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/>

²⁷ See Microsoft Azure shared security, which is applied to all on the Azure platform at <https://aws.amazon.com/ecs/features/> and Amazon ECS ability to share the cost of security across multiple servers and processing applications <https://aws.amazon.com/ecs/features/>

III. THE BROWSER AS A TOOL IN THE HANDS OF THE END USER

17. The underlying architecture of the web was designed to allow users to explore the web. In turn, businesses could set up and supply them freely. The web was designed to be decentralized. One design feature is that the browser, as a foundation, was expressed by the W3C to be the “User’s Agent”.²⁸ As such, the browser should act in the user’s interest and operate as the user’s window on the web it should operate fully independently of Google and Apple and not serve to support their downstream and adjacent market businesses.
18. However, the top two browsers, which are dominant in their respective operating system and ecosystems, are controlled in the platforms’ interest.²⁹ No longer is it a tool in the hands of each end user; it has become each platform’s agent. Its purpose is very different from its design. It now must gather information for the system it is part of, operating seamlessly with that system, and benefit the owners of that system. It depends on that system for upgrades. To keep up with functionality in websites worldwide it is sustained by platform dollars.
19. The outcome is browser dependence on platforms and the business interests of the platforms. It still functions as a tool in the hands of each end user, but that function is for the benefit of the commercial interests it serves, not the end user.
20. When considering the opening up of Apple and Google’s platforms to increased browser competition much can be gained but, equally, there is a risk that Apple’s Safari/WebKit could be displaced by Google’s Chrome/Blink. Since duopoly to monopoly is not an improvement in competition, consideration of controls on both existing platforms is needed as well as the ending of existing constraints. For example, if the role of the browser as the user’s agent could be restored, incentives for upgrades and software and device functionality could then operate to the benefit of the consumer. Simply enabling impartial open access to the Open Web, would address a lot of the issues identified by the CMA.

IV. ISSUES TO BE ADDRESSED: CLAIMED BENEFITS

21. MOW agrees with the CMA that there are two separate mobile ecosystems that do not compete with each other: one operated by Apple, powered by the iOS operating system, the other operated by Google, powered by Android.³⁰ Both ecosystems operate “key gateways” to both

²⁸ See W3C Web Platform Design Principles paragraph 1.1 at <https://www.w3.org/TR/design-principles/>

²⁹ Also, given that Microsoft’s Edge is now powered by Google’s Chromium project, Google is in an unparalleled position over control at browser level in desktops as well as mobile.

³⁰ P. 6 paragraph 5.

app stores and internet services.³¹ The CMA identifies some purported benefits of this including free services, ease and convenience of use of products offered over an integrated platform, the availability of product guarantees, and improved trust and confidence that comes from well-known brands allowing (some) smaller brands to access consumers using their distribution systems.

22. The CMA needs to reconsider these claimed benefits. These benefits are not only available from current platform businesses. Free services are available when funded by advertising. Apple does not provide much in the way of free services. Many others in online advertising offer users services that are ad-funded and free at the point of use. The CMA cannot therefore reasonably think free is a unique property of the current providers, and a benefit that needs to be retained. Likewise, product guarantees are available in open markets (and hardly a major justification for the consumer detriments from competitive constraints also listed). Similarly, any benefits of vertical integration such as ease of use (aka Quality of Experience “QOE”), are likely overstated.
23. While vertical integration may improve efficiency in other markets where consumers pay for products and incentivise suppliers to compete for their sales, it is highly questionable that vertical integration provides any benefit at all where each tech platform is “ecosystem dominant”. By definition, no competitive constraint forces the delivery of the benefits of vertical integration to end users. In ad-funded markets which are free at the point of use the benefits of vertical integration are more likely to have been captured as increased profits by the platform(s). QOE benefits can be achieved through operational and technical non-discrimination remedies.

V. INCENTIVES IN MOBILE ECOSYSTEMS: IMPACT ON INVESTMENT IN THE OPEN WEB

24. The CMA notes three key incentives to innovate in features, functionality, and performance of mobile devices: competitive pressure from their rivals, to get customers to upgrade and/or replace their current devices, and to increase revenue generating opportunities in the ecosystem.

³¹ P. 6 paragraph 6 “Apple’s browser, Safari (over 90%) and Google’s browser, Chrome (75%) have very strong shares of browser usage in their respective mobile ecosystems and are generally pre-installed for use when a user first turns on the device. As Apple operates the only browser ‘engine’ that runs on iOS and as Google operates the main browser engine on Android devices, each is in a position to determine the functionality and standards that will apply not only to their own browsers, but to competing browsers and, in turn, to web apps

- 24.1 The CMA notes that Google and Apple do not compete directly, their business models are different, they collaborate in many ways and their products are not price competitive. Direct “head-to-head” competition is thus not currently an important driver of innovation. This is consistent with EU Commission findings.³²
- 24.2 The CMA sees that most users buying a new smartphone are replacing an old one and manufacturers thus have an incentive to innovate to avoid the constraint of the existing device in consumers’ pockets.
- 24.3 Ecosystem incentives. One example is of Android manufacturers receiving a share of the Google advertising and Play revenues. Innovation to increase the usage of Android mobile devices (e.g., in terms of engagement or time spent) or increase the offerings available through apps also generate revenue and incentives for suppliers.
25. The CMA should also investigate and gather evidence about:
- 25.1 Google and Apple collect and control end users by controlling their data at the start of a user’s journey online when they sign in. This data is a cornerstone of the system of control and market power of both businesses. This was recognised in Annex Z of the CMA Online Platforms and Digital Advertising Final Report. The CMA should not overlook its relevance in this investigation. The interventions and actions previously identified should be implemented.
- 25.2 The fact that incentives exist within the platforms to control systems and functionality that would otherwise compete in the Open Web (as exemplified by Google’s Privacy Sandbox that seeks to further embed functionality in the browser that exists in the Open Web such as WebID proposal that disintermediates website sign-in).
- 25.3 Open Web functionality can be substituted by functionality on the device or within a controlled, extended, and cloud-based platform of computer servers (i.e., the platforms’ own cloud service and servers in its Walled Garden³³).
- 25.4 This incentive seeks to reduce or eliminate Open Web alternatives and functionality and suppress innovation over the Open Web by pulling functionality into the platform’s ecosystem. Preventing users from leaving also prevents choice and prevents

³² See case AT.40099 Google Android

³³ See Annex 2.

alternatives from arising that would then compete more effectively. These aim to avoid competitive threats and disintermediation.

- 25.5 Apple and Google have incentives to maximise profitability. Vertical integration in the circumstances that the CMA has described of no head-to-head competition can also be seen as a situation where no incentive exists to pass cost savings, or innovation benefits, through to end users exists.³⁴ In a world of free services this is likely to most adversely affect end users in the form of innovation rents, where Apple and Google gain the benefit of innovation for themselves and pass on only that which they choose to pass on. Hence, if they can generate efficiency benefits in terms of lower utilisation of computer resources in handsets or cost savings, such as from increased use of cloud computing, which can keep the benefits. They have no incentive to pass those costs savings on to end users or shop around for the best and cheapest source of supply.
26. Where the CMA discusses incentives to innovate, MOW has further questions. The platforms also have incentives to drive users to buy ever more expensive handsets (with the latest operating system). For example, Apple's explicit public strategy is to increase the volume of sales of services and to reduce the extent to which its business is dependent on the sales of (risky) handsets. While device sales still predominate it needs to include as much functionality as possible in both its devices and walled garden that increase the sales of more, higher capacity and higher functionality devices.
27. This incentive may be contrary to overall computational efficiency and detrimental to the innovation that would exist to support end users' needs in competitive markets. Examples that the CMA should also investigate include:
- 27.1 browser bloat – the amount of computing power needed in end user devices to run browsers has considerably increased over time with impacts on device requirements.
- 27.2 memory and power limitations – Apple has been found to have broken the law in France³⁵ for its management of power practices. These practices will have impaired functionality in circumstances where Apple substitutes new products for old, increasing

³⁴ Indeed, at P 174 the CMA's assessment of Apple's waterbed effect model suggest that iPhone prices and profits have remained high and are not being reduced to encourage uptake or use of apps- which also suggests lack of direct competition and limited incentive to upgrade efficiently.

³⁵ <https://www.bbc.co.uk/news/technology-51413724>

its sale of new products. The CMA should check on whether this (recent) practice took place in the UK and whether software upgrades are also being used to restrict or reduce their battery power in the interests of the supplier of “new products for old.”

- 27.3 system and admin storage bloat – the mechanisms through which increasing amounts of software is using up memory and storage “on-device” and how that is managed appears to be used by supplier systems to “encourage” users to store more on cloud-based solutions for a fee (see Apple’s online storage fees for basic memory).
- 27.4 whether users are really buying new products because old products stop working well after a few years; and why they do so. The solid-state functionality of most devices means that they do not wear out as would a mechanical device. Their loss of functionality may be driven by the way software “upgrades” are imposed on end users by the platforms in their own interest. The CMA states that users buy a new device because it is better than the device in their pocket, but does not ask why the device in the pocket is outmoded. MOW thinks the CMA should check with consumers, do market research, and gather evidence from technical experts about whether a new device is needed because the functioning of the older device is becoming impaired, and whether that impairment is contributed to Apple or Google’s operational practices.
28. When seen in the context of an overall strategy of creating walled gardens, Apple and Google’s strategies are both monopolistic, self-interested, and exploitative of end users and computing and engineering functions; they are likely technologically inefficient driving usage into devices that may more effectively be performed by devices and websites using the Open Web.

VI. APPLE AND GOOGLE’S INCENTIVES TO INCREASE FUNCTIONALITY AND CONTROL OVER SUPPLY CHAIN AND ECOSYSTEM CAPABILITIES BY INCREASING FUNCTIONALITY IN THE BROWSERS AND SPURIOUS MISUSE OF SECURITY ARE COORDINATED

29. When building their walled gardens Apple’s ITP and Google’s Privacy Sandbox are central as they both seek to increasing control and functionality in the browser. MOW considers that the CMA needs to also understand:
- 29.1 Apple’s ITP project as a mechanism to reduce rivals’ functionality in the browser, effectively an equivalent project to Google’s Privacy Sandbox.
- 29.2 When the CMA considers at 5.144 that “*There are a series of open standards that should, in principle, address any concerns about web compatibility. However, in practice, compatibility issues remain. This appears to be due to: (i) certain browsers*

releasing features without going through formal standards development organisations and processes; and (ii) web developers not developing against standards but for a specific browser or set of browsers,” the CMA should also recognise that Google and Apple coordinate on privacy and security as spurious justification for the creation of walled gardens through the W3C.

29.3 [REDACTED]
[REDACTED] This appears to be highly relevant to the functioning of the W3C as an independent standards-making body and Apple’s claims about security in the context of its WebKit browser engine.³⁷

29.4 As disclosed in Texas litigation,³⁸ Apple, Google, and others adopted a coordinated approach toward misusing privacy and security as an end user concern that they could play on to encourage users to submit to their walled garden strategy, being unaware of the levels of security and privacy available via Open Web alternatives.

29.5 Annex 1 outlines how Google and Apple plan to rig the functioning of browsers by promoting as a standard their own payments systems above those of their competitors.

29.6 Annex 2 includes further information about how Apple and Google both block or plan to block third party use of IP addresses to and for their own benefit.

30. These restrictions also limit competition between browser and apps, and app stores and the open web alternatives.

VII. CMA PROPOSALS AND QUESTIONS: MOW’S OBSERVATIONS ON REMEDIES AND THEIR EFFECTIVENESS³⁹

[REDACTED]
³⁷ See page 216 et seq. and the CMA finding that 5.106 “Overall, the evidence MOW have received to date does not suggest that Apple’s WebKit restriction allows for quicker and more effective response to security threats for dedicated browser apps on iOS” and at 5.113 “Overall, the evidence that MOW have seen to date does not suggest that there are material differences in the security performance of WebKit and alternative browser engines”.

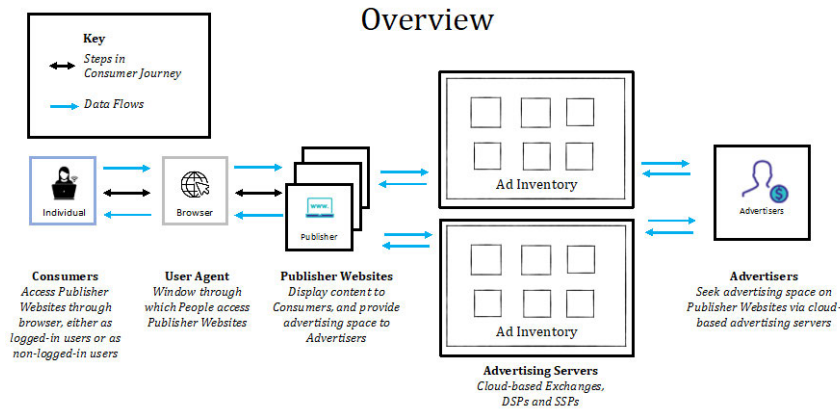
³⁸See the Texas AG unredacted filings, paragraphs 470 et seq. at https://texasattorneygeneral.gov/sites/default/files/images/child-support/20220114_195_0_States%20Third%20Amended%20Complaint.pdf

³⁹ In this section MOW address the point raised in 10.14 “Our final report will also provide our more comprehensive assessment of the most appropriate interventions to address the range of issues that MOW have identified.”

31. The Report identifies certain activities as tied or reserved for Apple and Google or for which prohibition of restrictions, unbundling and non-discrimination and publication remedies would enable greater competition.⁴⁰ MOW agrees that to address these, the CMA should intervene and impose obligations on the platforms to not unreasonably restrict third-party access to hardware and software needed to compete more equitably.
32. The interventions noted by CMA also need to address the most fundamental issue which is the control over end users and their data. This happens via bundling of sign in and the source of market power, however. As discussed in Annex Z of the CMA's Online Platforms and Digital Advertising Market Study Report control over end user data is central to the ability of both platforms to manage their ecosystems effectively. It is with some disappointment that MOW sees that the CMA has overlooked this and left out of the account the market for interoperable non-identity-linked ID management systems and products, such as SWAN which seek to address the ability of platforms to control end user data. [REDACTED]
33. MOW outlines the current position in figure 1 below:

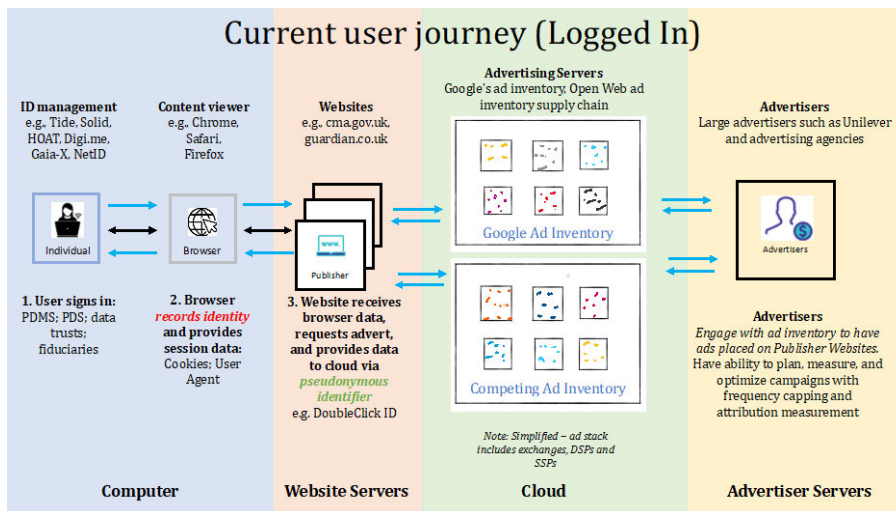
⁴⁰ Such as unbundling Apps from app stores; allowing alternative or additional app stores, or allowing sideloading from Open Web sources, Removing restrictions over commercial freedoms such as removing restrictions on offering alternative payment options for in-app purchases for digital apps; Removing policies that reinforce the position of app stores over Open Web alternatives (for example Apple's rules relating to cloud gaming and advertising prompts); and Offer a greater choice of browser engines within mobile ecosystems; or a requirement to offer (make available or publish?) certain forms of functionality and interoperability to third-party browsers. Prevention of bias; whether in choice architectures, determining defaults and other forms of bias built into the existing platforms.

[REDACTED]

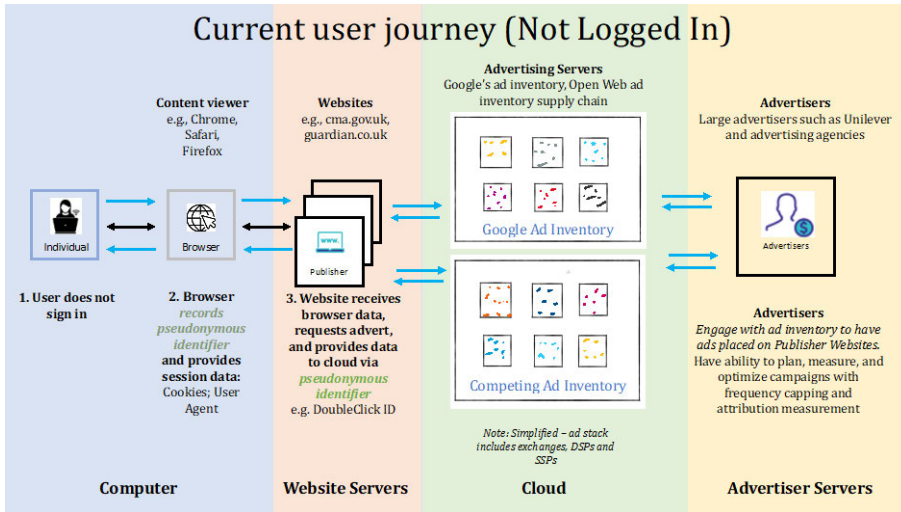


The overview in figure 1 illustrates how sign-in is used to take end user data, and the data flows that then follow in the advertising supply chains.

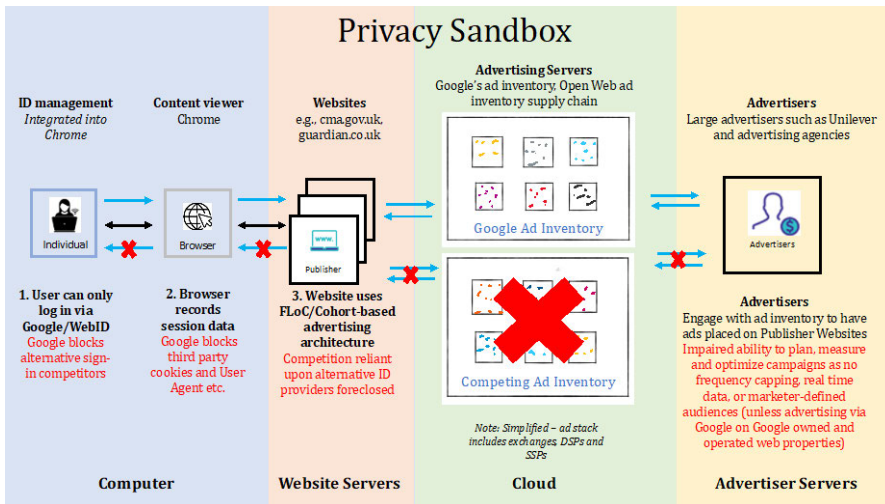
34. MOW outlines in figure 2 the current user journey (logged in):



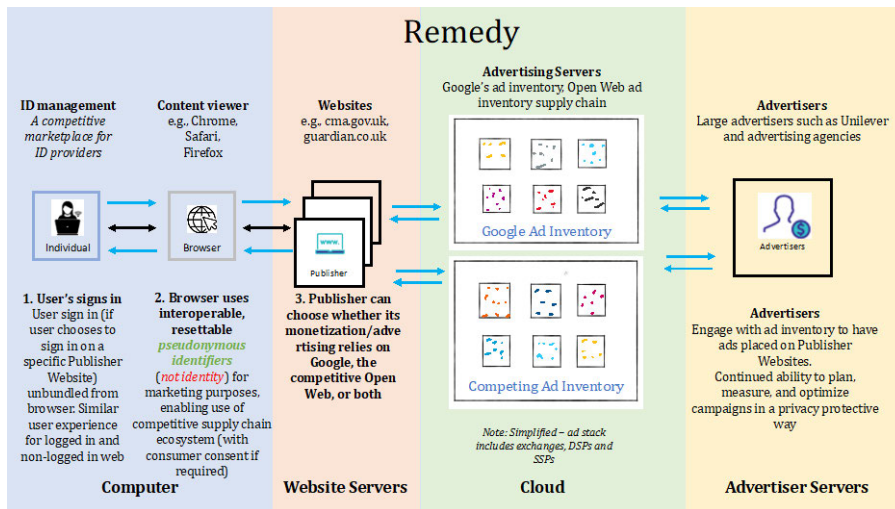
35. And in figure 3 the user journey (not logged in):



36. In figure 4 MOW illustrates the actions being taken by Google and how they impact third parties:



37. In figure 5 MOW outlines how a remedy to unbundle data from the sign in system at the browser level would enable greater competition:



38. Moreover, a further fundamental issue that is not addressed is how the system can become more competitive over time. The CMA has a glimpse of the world that could exist where at paragraph 72 it recognises that freedom of use for browsers and browser engines coupled with improved interoperability “*may also lead to greater functionality being available for web apps and a more widespread uptake of this type of app on mobile devices. This could have the broader effect of reducing the barriers to entry for new operating systems, by breaking a link between operating systems and control over distribution of content through native apps which are accessed through Apple’s and Google’s app stores.*”⁴²
39. In short, if the browsers were truly to operate under the control of end users, then competition throughout each ecosystem, and potentially across ecosystems could be enhanced.
40. The CMA recognises the issue that security and privacy concerns may increase in disaggregated and competitive supply chains and across ecosystems and that safeguards would be needed to protect end users in such a world, but limits its consideration to the “*conditions that might be imposed on third parties by Apple and Google to address those risks*’. This observation is misplaced:
- 40.1 It assumes that Google and Apple will continue to control and operate the browsers in their own interests.
- 40.2 It assumes that browsers should be integrated components within Google and Apple’s platforms.

⁴² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3923602 Interoperability: the “Super Tool” of Digital Platform Governance, Yale Tobin Centre for Economic Policy, 2021

- 40.3 It assumes that privacy and security are not factors that are important for end users and matters to be addressed via offerings in competitive markets or via Open Web solutions.
41. MOW observes that if this route is followed CMA would be serving to entrench Google and Apple and not fully using the potential for market-based remedies as is called for in its market investigation guidance.⁴³ MOW therefore asks the CMA to reconsider.

VIII. PRIVACY AND SECURITY AS NON-PRICE FACTORS OF COMPETITION AND THE NEED FOR INDEPENDENT SOURCES OF TRUTH, CERTIFICATION, AND VERIFICATION (PER CHAPTER 7)

42. Security and privacy in digital markets are non-price factors of competition. As such, market forces should be encouraged to develop outside the control of the platforms so that assorted products and services can develop, offering different privacy and security capabilities to consumers.
43. Control over consumers also needs to be addressed. Limiting the power of the platforms may require the CMA to consider how systems of demand aggregation can be added into remedies. Data trusts have been advocated as they could, as with Pensions regulation, operate to end user needs and acting as trustee, to and for the benefit of the end user.⁴⁴
44. This is currently the case for many computing and communications products in business-to-business service that use the same underlying Open Web functionality as the platforms. For example, business-to-business services are frequently deployed in circumstances where higher levels of privacy and security are required than offered in consumer services, in banking and insurance markets.⁴⁵ It can be expected that in a competitive market, some offerings would be more or less private depending on users' assessment of the need for privacy protections, and likewise some offerings could be more or less secure depending on market demand. This is true of postal systems and public and private communications systems with more privacy and

⁴³ See CMA Market investigation guidelines Part 4 - the need for market based approached where possible at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284390/cc3_revised.pdf

⁴⁵ See BT Radianz: <https://www.globalservices.bt.com/en/solutions/topics/optimise-your-financial-markets-solutions-across-the-trade-cycle> and <https://www.globalservices.bt.com/en> on banking and <https://www.globalservices.bt.com/en/solutions/topics/make-security-integral-to-your-business>

security being routinely deployed in systems used for highly secure banking transactions than for other communications.

45. Not everything needs to operate to the highest standard of security and privacy, and if privacy is promoted over security, then privacy becomes a fraudster's charter. Some consumers may also be happy to share unimportant data with insecure web apps, other consumers may wish to exert greater control than is now allowed by the platforms, ensuring that they receive greater benefits than currently available from their unchecked privacy invading and data mining operations. t Since the CMA accepts that the dominant platforms impose their decisions on end users and rivals' ability to offer competing solutions (e.g., through conduct regarding policies, technologies and integrations) but does not appear to recognise explicitly the role for encouraging the market to operate better to resolve the issue.
46. Independent sources of truth are also critical for online markets to operate effectively. Where Google or Apple has an interest in a downstream or upstream activity, they cannot themselves be the source of verification for that activity since they have a conflict of interest. So, for example where Google is looking to block the User Agent String of data in the Privacy Sandbox (which is used for fraud detection and prevention) and proposes that the elimination of competitors who verify and provide certification of that data as a trivial matter to be of no consequence, it overlooks the critical importance of independent companies as independent sources of verification for fraud prevention. Apple likewise overlooked this when introducing its ITP system.⁴⁶
47. There are many instances where *independent* alternatives are important, for estimating value or protecting against security risks and malware or for providing verification of systems and processes where the main platforms have an interest in the outcome and hence cannot be trusted to provide a response contrary to their commercial interests.
48. The CMA asks about verification to protect against privacy risks with relation to third party app stores and whether safeguards could be introduced to mitigate the risks to security and preserve the integrity of users' experiences.⁴⁷ MOW considers this to be not just desirable but necessary. The platforms own self certification cannot be trusted where they have an interest in the outcome and is not currently trusted by the market.


⁴⁶ Referring to it as an unintended consequence <https://webkit.org/tracking-prevention-policy/#unintended-impact>

⁴⁷ Paragraph 7. 58 p 374 & 375

49. In this area a useful role for truly independent standards, monitored and policed by independent authorities such as the DMU with information from third parties, can be foreseen. Before that can take place, however, reform and regulatory intervention is needed with relation to the structure and functioning, and oversight and compliance with competition law of the W3C.⁴⁸

IX. MOW PROPOSAL FOR BROWSERS: ESSENTIAL INPUTS THAT NEED TO BE TREATED AS SUCH AND OPERATE TO THE USERS' INTERESTS THROUGH SYSTEMS THAT OPERATE UNDER FUNCTIONAL SEPARATION AND NON-DISCRIMINATORY INTEROPERABILITY

50. MOW supports the CMA's detailed proposals that would enhance the functionality and interoperability of browsers and enable competition to be introduced in the provision of browsers and choices over browsers to be restored to end users (see page 378 *et seq.*).⁴⁹ MOW notes and support the finding at 8.55 that Apple has substantial and entrenched market power in the supply of its mobile browser and browser engine, and at 8.110 with relation to Google's browser. MOW also notes in 8.115, Google's control of Blink and its position in browsers gives it scope to entrench Google's market power in the supply of ad inventory and in the supply of ad tech services. MOW agrees that Google can use its control to influence competition in the supply of ad inventory and in the supply of ad tech services, through the deprecation of third-party cookies on its browser and other Blink-based browsers (which Google has proposed to do as part of its Privacy Sandbox proposal) or by restricting the functionality associated with user tracking for third parties but retaining this functionality for Google.
51. Rather than assuming browsers continuing under the operational control and for the benefit of the platforms, MOW suggests that they should be regarded as essential inputs that are managed for consume welfare and competitive public benefit, as with other essential services or utilities.
52. The CMA appears to accept the need for non-discriminatory obligations when referring to the absence of self-preference and the need or unbundling with relation to app stores (see pages 388-9) but then may be taking an inconsistent approach,⁵⁰ by not then considering independence

 ⁴⁹ See further p. 380. MOW is also concerned that the CMA seems to assume, while in the middle of a consultation period over the Privacy sandbox undertakings that Google's proposal could be acceptable in the light of the consultation responses from, MOW, among others.

⁵⁰ Both internally inconsistent and inconsistent with the CMA Final Report of June 2020 into Online Markets and Digital Advertising.

and non-discrimination including data separation and operational separation with relation to browsers and sign in data.

53. Taking the next step would involve addressing the underlying incentives that operate on the people in the business which drive them to prefer and promote the businesses own products and services and discriminate against those of rivals.
54. The following has been applied in different settings as part of remedies packages to address anticompetitive outcomes from vertical integration. These remedies have been tried and tested in many different industries, from payments systems to telecommunications.⁵¹ They benefit consumers by ensuring an alignment of incentives to support compliance with the non-discrimination obligations, and also to ensure that abuse, as may be identified in any snapshot review, is e not simply replaced with other forms of abuse once the reviewer has moved on.
55. All markets depend on investment receiving an adequate return. All business is risky. When markets have been dominated for so long, as they have here, there is a need to nurture entry and encourage investment.
56. MOW commends Professor Martin Cave’s seminal paper “Six Degrees of Separation,”⁵² which discusses the subject of incentive alignment and their importance for effective remedies to antitrust and regulatory problems where enduring platforms are concerned. The OECD studies listed below, particularly the 2011 study, consider the effect of functional and structural separation on investment incentives, and recommended that incentives to invest should be considered by organisations such as the CMA in situations such as this.
57. The CMA should consider a system of incentive alignment whereby those that operate the browser truly ensure that its functionality is likely to operate to and for the benefit of the end user. For this to operate over time the system needs to be considered over time in a dynamic environment. To achieve effectively competitive outcomes where vertical integration has been the previous and prevailing industrial structure, a degree of “market liberalisation” is needed and entry needs to be encouraged. The business system needs to be considered together with the incentives that operate on individual managers within that system.

⁵¹ See for example the OECD’s studies: <https://www.oecd.org/daf/competition/sectors/19635977.pdf>
<https://www.oecd.org/daf/competition/sectors/45518043.pdf>
<https://www.oecd.org/daf/competition/sectors/50056685.pdf> and
<https://www.oecd.org/daf/competition/recommendationconcerningstructuralseparationinregulatedindustries.html>

⁵² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=994798

58. Today, teams of engineers are funded by Google and Apple respectively to maintain and upgrade the browser engines Chromium and WebKit and to do so in a way that benefits Google and Apple. Those engineers work out what is needed to achieve effective functionality for end users and the firm. They are also managed for the benefit of each platform and degrade interoperability or promote their own integrated offerings according to the wishes of the platform owners in their respective business interests. If they were to operate under separate financial and management incentives that truly ensure impartiality and non-discrimination, then the objective of each browser organisation would be to improve the functionality of the browser for all uses. That would place the browser in the hands of each end user as a tool for accessing the internet, and to do so on a non-discriminatory basis, that would start to adjust the systems to accept rivals' products and promote entry – and allow success based on competitive merit rather than ownership.
59. MOW advocates that the Open Web, if accessed on a non-discriminatory basis and if given a fair chance to operate as a competing distribution platform can provide the features, functions, products, and services that consumers need.
60. Taking one central example from the CMA's report:
- 60.1 If the browser were operating on:
- (a) a non-discriminatory basis,
 - (b) as a functionally separate entity,
 - (c) with incentives aligned to end user need,
 - (d) with open APIs,
 - (e) equal access and interoperability,
 - (f) and sideloading enabled,
 - (g) with a choice of payment systems,
 - (h) with apps provided by suppliers to meet consumers' needs,

- 60.2 and the platforms were under cross-promotion⁵³ and must carry⁵⁴ marketing obligations, it is highly likely that Open Web based alternatives and apps would flourish.
61. Consumer choices would be improved, and prices could be expected to fall. Entry would be encouraged, and technical innovation would also increase as more components of the vertically supply chain would be opened up to competitive pressure, rather than being hidden within the vertically integrated platforms as at present.
62. To achieve such an outcome would involve operating browsers under conditions of operational separation in business units under separate financial incentives. The different models of functional separation should be considered carefully over the next six months.⁵⁵

X. CMA CONCERNS TO BE INVESTIGATED

63. MOW notes that the CMA is interested in further investigation of Apple limiting functionality of Web Apps, Google’s Privacy Sandbox, and Apple’s ITP. MOW is however surprised and concerned that the CMA has quoted and referenced the W3C as if it were an independent standards-making body [REDACTED]

XI. OVERDUE NEED FOR EFFECTIVE REMEDIES AND ENFORCEMENT ACTION

64. MOW has outlined above and further below matters that have not been properly considered by the CMA. They are important as any effective remedy needs to be fully thought through. The CMA, for instance, is suggesting a series of non-discrimination obligations and remedies, for the DMU. But none of which would be likely to be effective if not also coupled with some form of operational or functional separation and incentive alignment.
65. The CMA’s enforcement actions and considerations, proceeding as they are from assessments of point failures, will at best be point solutions and fail to address the underlying operation and

⁵³ Such as browser choice screens or carousels or requirements to provide equivalent visibility subject to end user “Reach” and under monitored measurement metrics.

⁵⁴ Such as apply to must carry for news obligations in broadcasting regulation

⁵⁵ MOW would not consider that functional separation is a form of structural remedy in the sense of a PCI or procompetitive intervention as used by the CMA in its DMU proposals. It is not an intrusive imposition on the recipient firm – rather it is a mechanism for securing compliance with FRAND terms and conditions which are behavioural remedies without which such non-discrimination and unbundling obligations are incapable of being effectively policed.

functioning of the platforms over time. Effective remedies and incentive alignment over time should, as a minimum, be thoroughly considered during the second half of the market study.

66. MOW also considers there may be a certain lack of coherence in the CMA's position. In brief:

66.1 The CMA has now identified current market failure and current anti-competitive practices that have been affecting UK consumers for many years. It has extensive powers, particularly under Schedule 8,⁵⁷ that apply at the end of a full Market Investigation. The next stage in the process chosen by the CMA is to conduct a further study.

66.2 On the one hand, the CMA is claiming the need for greater powers now, while on the other it is not fully investigating the issues it needs to address or using its existing enforcement powers or demonstrating why its current powers would be insufficient to address those issues. It might be said that to call for new powers now might be legally premature when the existing ones have not been tried.

66.3 The CMA is instead suggesting the DMU (part of the CMA) will deal with the issues. It may need to consider the difficulty of answering these questions in Parliament while seeking additional powers, without using the current powers already granted.

67. Moreover, time and the market move on as more reports are written. The CMA's Online Platforms and Digital Advertising Final Report identified the issues to be addressed, and then the CMA took the Privacy Sandbox case, pending the introduction of the proposed legislation. Consistency would suggest interim enforcement would be necessary now that the issues have been identified in the Market Study.

68. Furthermore, MOW is puzzled about the CMA's purported "SMS" findings. If the CMA were to seek to rely on its findings in the Report to assess the "Significant Market Status" of platforms in the markets that exist at the time the new legislation is passed, say in 2- or 3-years' time, would not any party then subject to that legislation not reasonably simply ask for the assessment to be made under the terms of the new legislation?

69. While MOW has sympathy with the CMA that its teams are looking to new legislation and wishing it were in place, it does not yet exist. As such MOW considers these matters to be

⁵⁷ Enterprise Act 2002, Schedule 8

important, that the CMA may have fallen into error, and urge the CMA to reconsider its determination not to make a market investigation or use its existing enforcement powers.

70. MOW commends the CMA for recognising that it may need to revisit its decision on enforcement action. MOW suggests that the decision to revisit actions, including interim relief under existing law, should be reassessed as soon as possible. MOW welcomes the Study and its Report, together with others,⁵⁸ and the exposure they bring of the factual position to a broader community. However, it is nevertheless very surprising and disappointing that CMA has identified and analysed the issues but, once again, has failed to take enforcement action.

⁵⁸ The CMA's Digital Markets Strategy: February 2021 refresh. Government consultation on A new pro-competition regime for digital markets, July 2021. Unlocking digital competition, Report of the Digital Competition Expert Panel, March 2019. The CMA's market study into online platforms and digital advertising, case page. See also advice of the DMU taskforce: <https://www.gov.uk/cma-cases/digital-markets-taskforce>

MOVEMENT FOR AN OPEN WEB

RESPONSE TO CMA MOBILE ECOSYSTEMS

MARKET STUDY INTERIM REPORT

ANNEX 1

Distortion of Competition Concerns with the W3C Web Payments API

The W3C presents itself as a standards organization that promotes interoperable web technologies that help people interact with organizations worldwide. Such standards should aim to make the web work regardless of which web-enabled software is used.

W3C's Mission is expressed as follows:

“The social value of the Web is that it enables human communication, commerce, and opportunities to share knowledge. One of W3C's primary goals is to make these benefits available to all people, whatever their hardware, software, network infrastructure....”¹

Unfortunately, a new W3C Web Payments API proposal fails to meet that goal. Instead, this W3C specification would justify Google and Apple granting their own payment solutions first place in the queue of payment cards that will be put into every mobile phone browser. The lead editor is Google.²

A pro-competitive justification for W3C involvement in payments would be to facilitate payments and ease transactions between users and merchants by reducing the hassle of re-entering payment card details into the merchant's web form. In principle, that should be a good thing for users and merchants.

“This specification standardizes an API to allow merchants (i.e. web sites selling physical or digital goods) to utilize one or more payment methods with minimal integration. User agents (e.g., browsers) facilitate the payment flow between merchant and user.”³

It is necessary to ensure a match between the payment providers technically supported by the merchants and those that users have accounts with.

The proposed specification goes beyond its original scope of passive facilitation to allow active interference and discrimination. It includes language that would justify the browser (“user agent”) reordering or restricting which payment methods are presented to the user by the merchant.

The example concerning phrases include “if the user agent **wishes** to disallow the call to show” merchant-supported methods and this specification “allows the user agent to act as if the user had immediately aborted the payment request, **at its discretion.**”⁴

This would allow organizations that not only build B2C browser software but also operate B2B payment solutions to self-preference their own solutions in the list of payments systems, determining the sort order,

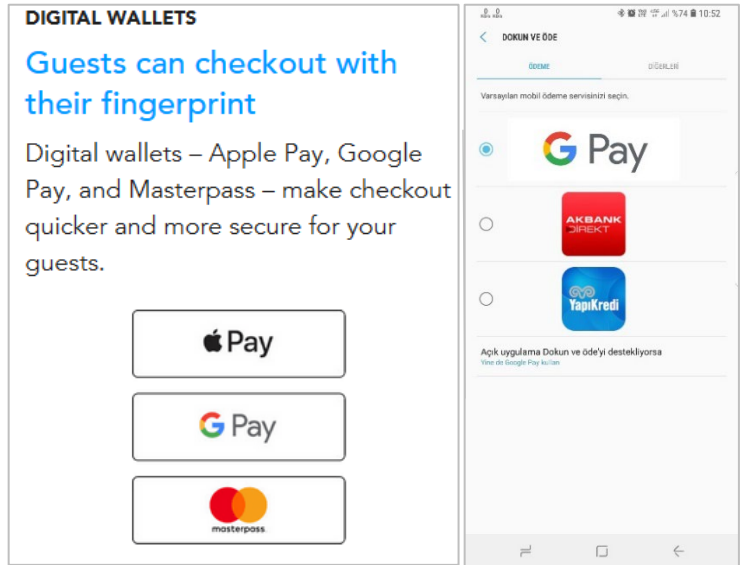
¹ <https://www.w3.org/Consortium/mission#principles>

² <https://www.w3.org/TR/payment-request>

³ <https://www.w3.org/TR/payment-request>

⁴ <https://www.w3.org/TR/payment-request>, section 3.3.6 and 3.3.12 (emphasis added)

rather than an order desired by the user (or the merchant):



Moreover, certain merchants offer different discounts to ordinary credit card holders for different types of transactions (e.g., higher discounts to food than gas or travel than office supplies or vice versa). A user ought to be able to choose which payment method they prefer when initiating payment rather than having this order determined by the browser. Under W3C standards and “Priority of Constituencies”, the browser is supposed to act as the agent of and in the interest of the user, focused solely on facilitating the transaction.

A number of W3C members have filed formal objections to the proposed specification.⁶ Among the concerns are potential problematic behavior such as:

- “1. consistently ranking a rival payment provider or processor at the bottom of the list,
2. withholding disclosure of payment providers or processors that do not pay an app-store-like facilitation fee,
3. restricting the list of payment providers or payment processors due to other internal business priorities.”

This W3C list of objections notes that “*the Payments Work Groups operates under,*” W3C Antitrust and Competition Guidance. That Guidance requires that: “*W3C does not play any role in the competitive decisions of W3C participants nor in any way restrict competition.*”⁷ At least some of the formal objections to this specification identify a clear breach of the W3C Antitrust and Competition Guidance. Moreover, this specification as written contradicts W3C’s Priority of Constituencies (according to which specifications should place the interests of authors and site owners ahead of user agents’ interests) and core mission of promoting interoperability and equal access for all.

⁵ Sources: <https://singenuity.com/features> & <https://forum.donanimhaber.com/profil/59275#lg=59275&slide=2> (Google translate of Turkish reads: “Select your default mobile payment service. If open app supports Tap & Pay. **Tap Use Google Pay anyway.**”)

⁶ <https://www.w3.org/2021/12/prapi-objs.html> (last update: 4 Jan 2022)

⁷ <https://www.w3.org/Consortium/Legal/2017/antitrust-guidance> (last update: 1 Mar 2017)

MOVEMENT FOR AN OPEN WEB

RESPONSE TO CMA MOBILE ECOSYSTEMS

MARKET STUDY INTERIM REPORT

ANNEX 2

ISPs turning against Apple's version of Gnatcatcher

Apple introduced a similar feature to Gnatcatcher¹ in their last OS update, called Private Relay². Paid iCloud users are able to turn this beta feature on, which reroutes the traffic through anonymization servers just like Gnatcatcher. The feature has now been used for a few months by paid iCloud users, and some ISPs (Vodafone, Telefonica and T-Mobile) are starting to push back and to block Private Relay and demanding regulators to ban it.

ISPs say that Private Relay cuts off networks and servers from accessing “vital network data and metadata” and will have “significant consequences in terms of undermining European digital sovereignty”. They say it will also impact “operator’s ability to efficiently manage telecommunication networks”.³

Both in Gnatcatcher and in Private Relay, communication is encrypted when it leaves the device, so ISPs or routers on homes or offices cannot monitor where the data is going or what kind of pages are accessed. Additional services like content filtering (such as restricting access for children or employees to some web pages) are not working.⁴

“The director of the public consulting firm 419 Consulting, Andrew Campling, recently published a pretty good statement on the impact Private Relay could have on broadband ISPs and cellular network operators (here). Not only does Andrew warn that this could affect congestion management and peering optimization activities by ISPs, but he also points out that it could become more difficult for ISPs to adhere to certain Quality of Service (QoS) -related metrics set by regulators.”⁵

The volumes in Private Relay today are nothing compared to the volumes of data that would be rerouted with Gnatcatcher, and ISPs are already strongly against it.

Apple’s Private Relay and Google’s Gnatcatcher make it impossible for homes and companies to configure content filtering on their broadband router to protect children and employees from malicious content. It would also prevent ISPs from offering parental control or content filtering services. This would pose

¹ <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>

² <https://support.apple.com/en-gb/HT212614>

³ <https://9to5mac.com/2022/01/10/european-carriers-seek-to-block-iphone-private-relay-feature/>

⁴ <https://hitechglitz.com/apples-private-relay-service-poses-challenges-for-uk-isps/>

⁵ <https://blog.apnic.net/2021/11/26/impact-of-private-relay-netops-isps/>

security threats. The only ones able to provide these services would be the browser makers (Apple or Google), which would be very anti-competitive against ISPs currently offering these services.

Furthermore, Apple's Private Relay and Google's Gnatcatcher route all traffic through Apple/Google and encrypt all data between the user and Apple/Google. This brings clear privacy and security risks. Apple/Google could intercept and monitor all traffic in the world, while there would be no option for governments to work with local ISPs to track criminal activity online, since the traffic through ISPs would be encrypted. The Open Web would transform into a big anonymous Tor-network, controlled by Apple and Google.

While Private Relay and Gnatcatcher are marketed as privacy improvements, they bring security threats for families with children, employees and governments and put Apple and Google as gatekeepers for all Internet traffic. Apple and Google try to maximize their dominance by blinding everyone else from knowing what happens online.

The essence of ISPs complaint about Private Relay is that IP addresses are used for communications. The control that the browser owners can exert over the supply chain using both browser and IP routing means that they are the source of much data traffic and can control data traffic. Traffic management means that they can and do manage communications infrastructure, as exemplified below in their coordination of cloud computing.

In practice Google and Apple restrict users' ability to use this web functionality. Apple has adopted a walled garden strategy for many years, with integrated products and a proprietary apps store. Building parallel "Walled Gardens of apps stores" and stifling innovation on the open web appears to be a current Google project.⁶ Coordination between Google and Apple at senior-level meetings has been referred to in *USA vs Google*, and it may not be a coincidence that both companies have independently developed their walled garden strategies or that they have a mutually reinforcing interest in stifling innovation and applications developments from being supplied over the Open Web.⁷ Apple is also reported to use Google data centres for cloud storage.⁸

This impacts the telecommunications operators and all content management platforms (such as Akamai) and cloud computing centres that are used by B2C suppliers. The issue may impact businesses such as Microsoft which uses remote data centres to host its Azure platform on which remote applications are currently running.

⁶ See Texas vs Google para 18: "Google has an appetite for total dominance, and its latest ambition is to transform the free and open architecture of the internet. Google's plan is to create a walled garden around the internet in which it controls websites and mobile applications. Google calls its emerging venture the [redacted], a world in which publisher content is operated by Google. Internally, it refers to this model as [redacted]. Google's documented plan is to capture online publishers on the open internet and transform them into content creators generating revenue for Google on a completely closed platform—like YouTube content creators."

⁷ See further in Appendix I how open web functionality can provide competing alternatives to Apple and Google products and apps.

⁸ <https://www.lightreading.com/enterprise-cloud/infrastructure-and-platform/apple-partners-with-google---steve-jobs-spins-in-grave/a/d-id/740983>

For cloud computing, reducing IT costs and the shift from desktop to data centre, the use is widely believed to reduce costs, but we would accept that in outsourcing contexts much depends on the infrastructure being compared: “nevertheless the largest sample, 41 percent, said cloud computing reduced costs from 10 to 25 percent, while 19 percent said it providing 25 to 50 percent in IT savings, and 27 percent said it only cut costs by 10 percent or less”⁹

	<u>m1.large</u>	<u>m3.large</u>	<u>m4.large</u>	<u>m5.large</u>	Reduction from previous year/generation	3-year reduction
2008	<u>\$0.40</u>					
2009	<u>\$0.40</u>				0%	
2010	<u>\$0.34</u>				-18%	
2011	<u>\$0.34</u>				0%	-18%
2012	<u>\$0.32</u>				-6%	-25%
2013	<u>\$0.26</u>				-23%	-31%
2014	<u>\$0.24</u>	<u>\$0.23</u>			-13%	-46%
2015	<u>\$0.175</u>	<u>\$0.14</u>			-64%	-103%
2016	<u>\$0.175</u>	<u>\$0.133</u>	<u>\$0.120</u>		-17%	-80%
2017	<u>\$0.175</u>	<u>\$0.133</u>	<u>\$0.108</u>		-11%	-113%
2018*	<u>\$0.175</u>	<u>\$0.133</u>	<u>\$0.100</u>	<u>\$0.096</u>	-13%	-46%

* Latest Internet Archive data from Dec 2017 but confirmed to match current Jan 2018 AWS pricing.

10

Hence, if Google and Apple can generate efficiency benefits in terms of cost savings, such as from increased use of cloud computing, they have no incentive to pass those costs savings on to end users or shop around for the best and cheapest source of supply. The fact that the Open Web could deliver similar or equivalent services over a highly effective, potentially as fast or faster, and cheaper platform than Google and Apple is an important matter to consider further when looking at alternatives, counterfactuals and potential competition from the Open Web, absent the current restrictions and bundling.

Google and Apple appear to have adopted a copycat approach to IP routing. Their restrictions benefit themselves since they enable the control of traffic within their platforms and prevent it from being processed by Open Web based services. Coordination between Google and Apple at senior-level meetings has been referred to in *USA vs Google*, and it may not be a coincidence that both companies have independently developed their walled garden strategies or that they have a mutually reinforcing interest in stifling innovation and application developments from being supplied over the Open Web. Apple is also reported to use Google data centres for cloud storage.¹¹

⁹ <https://virtualizationreview.com/blogs/the-schwartz-cloud-report/2013/02/does-cloud-computing-reduce-it-costs.aspx>

¹⁰ <https://appdeveloperomagazine.com/why-the-cost-of-cloud-computing-is-dropping-dramatically/>

¹¹ <https://www.lightreading.com/enterprise-cloud/infrastructure-and-platform/apple-partners-with-google---steve-jobs-spins-in-grave/a/did/>

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 markets¹

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 analysis⁵ and the duty to promote competition⁶ 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.

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:

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.

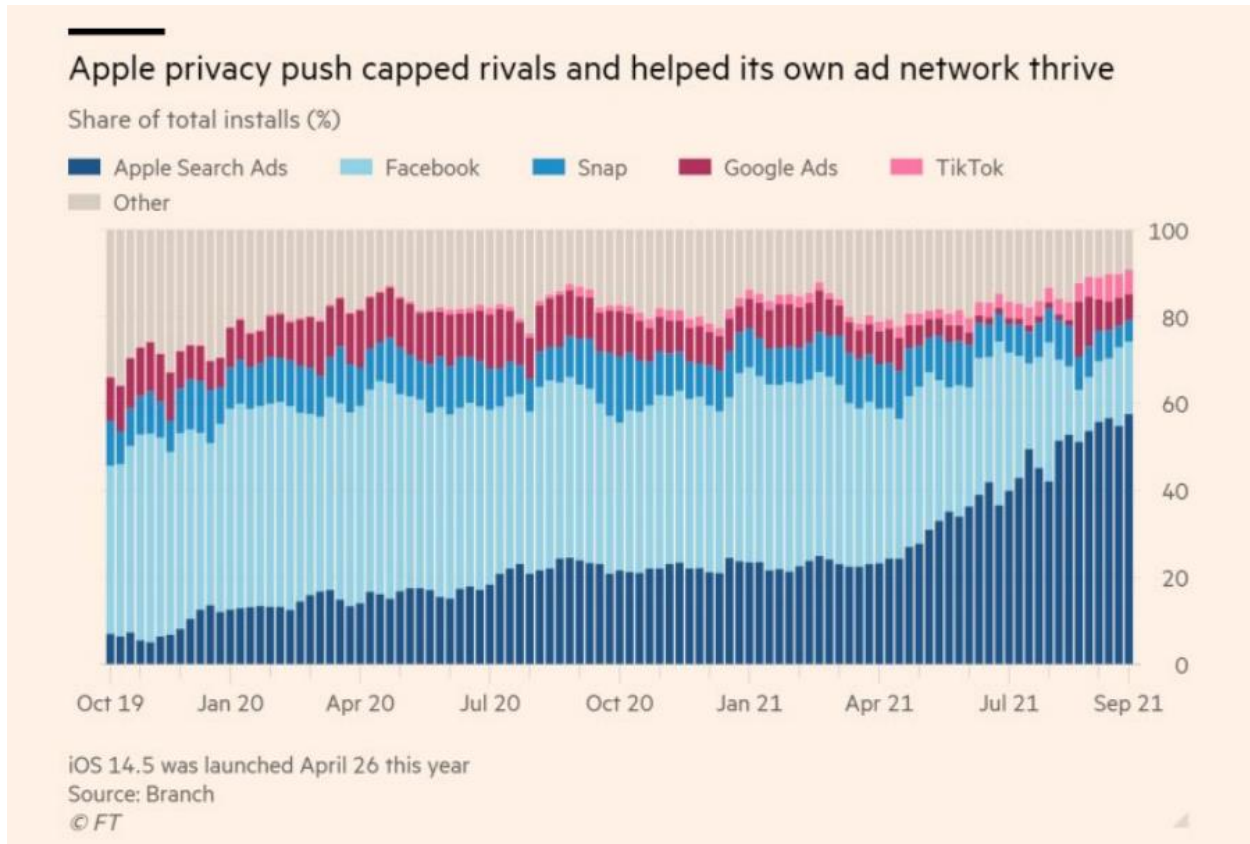
⁶ UK Competition & Markets Authority, "Online platforms and digital advertising" (2020) https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

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 positions¹² 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

the platforms¹⁴ 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 trusts¹⁷ and stewards¹⁸ 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 ID¹⁹ 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>

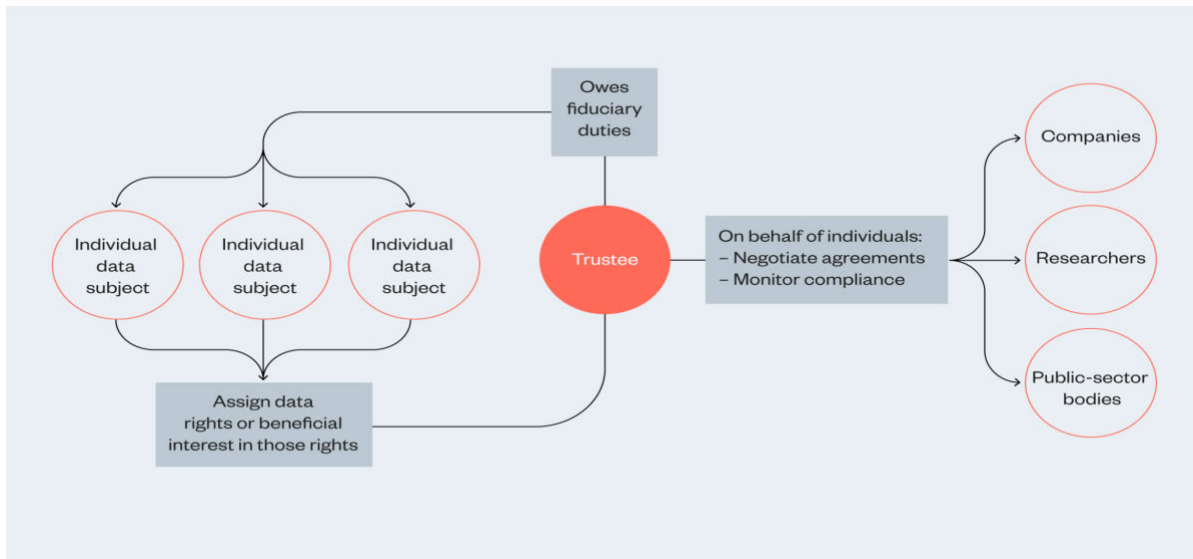
¹⁹ As discussed by the CMA in Annex Z of its Digital Advertising and Online Markets Final Report

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 choice²⁴ 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 remedy²⁶ 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

²⁹Important 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 decisions³² 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:



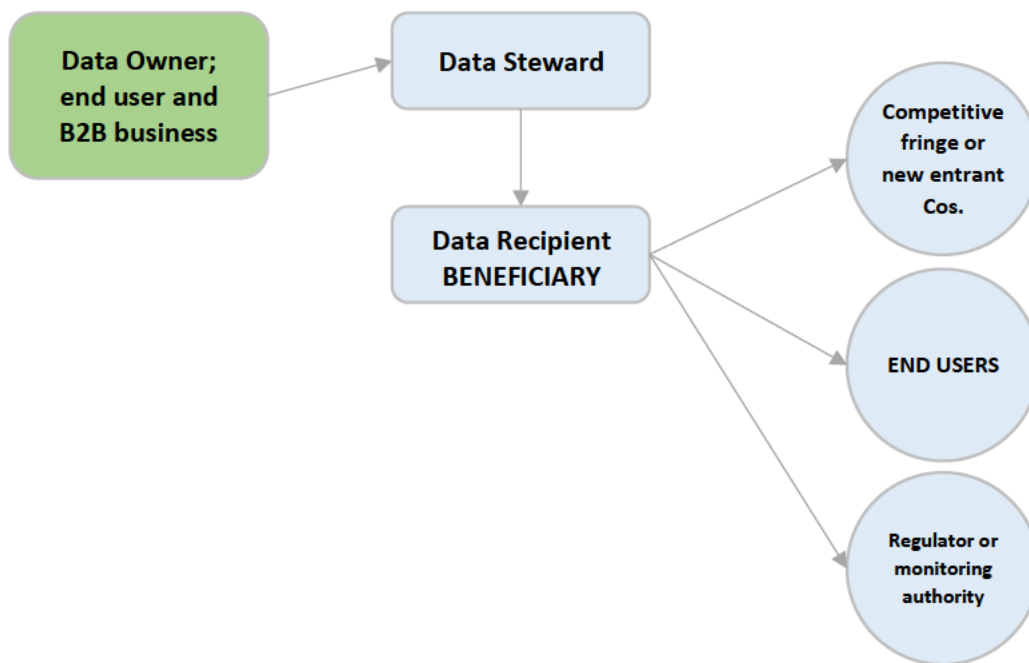
³¹ See [redacted] <https://support.google.com/admanager/answer/7560930?hl=en>

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 regime³⁵ 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 Wilbury 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."

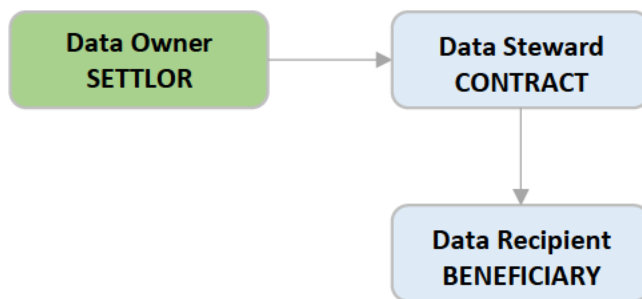
³⁸ <https://www.sharingcities.eu/sharingcities/resources>

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

⁴⁴See 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 buyer⁴⁵ 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.

⁴⁸High 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.community⁵¹ 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/>