PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

12 February 2020

Privacy International's comments on the Competition and Markets Authority's interim report on its online platforms and digital advertising market study

Privacy International (PI) is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

Privacy International welcomes the CMA's interim report on its Online Platforms and Digital Advertising Market Study together with the opportunity to provide comments on the CMA's initial findings and potential interventions. Our response is primarily focused on the privacy and data protection concerns raised in the initial findings and interventions considered. However, our response is not exhaustive, and we reserve our position in relation to any other existing or future potential interventions or remedies that might arise during the market study and which might have implications for people's rights. We would be happy to provide further comments and assist the CMA during the final stages of its market study.

Response re Initial Findings

PI broadly welcomes the CMA's initial findings, many of which correspond with issues of longstanding concern to Privacy International and with the points raised in our response to the CMA's Statement of Scope.[1]

This includes the indication that Google and Facebook have a dominant or strategic position in major elements of the digital advertising market[2] which can -at least, partially- be attributed to the vast amounts of users' personal

[1] Privacy International, Privacy International's response to the CMA's online platforms and digital advertising market study (30.07.2019), https://privacyinternational.org/advocacy/3101/response-cmas-online-platforms-and-digital-advertising-market-study

[2] CMA, Online platforms and digital advertising, Market study interim report, "*Google has significant market power in the general search sector, having had a share of supply of around 90% or higher in the UK for more than a decade*", page 59; "*Google has significant market power in search adverting*" (5.286); "The evidence we have gathered so far suggests Facebook has significant market power in social media" (3.165).

data that these platforms hold.[3] A lack of transparency characterises how the online advertising ecosystem operates, including how individuals' personal data may be exploited and further processed for purposes that remain unknown to individuals – with knock on consequences for individuals and society. This further exacerbates the lack of consumers' control over their personal data and, at the same time, contributes to strengthening these platforms' dominance or strategic market status (SMS).[4]

In its Response to the Statement of Scope, Privacy International encouraged the CMA to analyse the implications of the interplay between privacy and competition laws, for example by developing guidance on how privacy and data protection standards can be used to help determine the 'harm' relevant for assessing abuses of dominance in the digital market.[5] We note that the CMA's initial findings take stock of the importance of personal data for competition in digital advertising and underline several ways in which platforms may undermine consumers' choices or even deprive them of effective control over their personal data.[6]

However, we would underline that it is essential that personal data is not regarded/ framed as a mere economic asset and urge caution in this regard. For example, while articulating the societal harms that unfair competition can have for consumers, the interim report states:

> competition problems may result in consumers receiving inadequate compensation for their attention and the use of their data. Although many online services are currently provided for free, in a well-functioning market, consumers might be paid for their engagement online, or offered a choice over the amount of data they provide.[7]

In response to this we wish to comment around the suggestions of payment for engagement and also choice in terms of the amount of data provided.

First, it is essential for consumers that the CMA does not endorse the position that many companies take, that there is a binary choice between offering up your data or receipt of a service. Individuals must retain rights over their data. Data is not property; it cannot be sold, or rights relinquished. There is a risk that already asymmetrical situation is exacerbated with the monetization of data. This entails numerous problems from a failure to recognise that privacy

---

[3] See ibid, "*Google's strong position is primarily maintained by three key barriers to entry and expansion: economies of scale in developing a web index, access to click -and- query data at scale, and Google's extensive default positions across desktop and mobile devices*", page 59; "*Google is also able to use its access to data across a large proportion of the internet to provide higher-quality analytics and attribution services which increases the value of the advertising in a way that is very hard for other smaller search providers to compete with. These factors are reflected in the higher revenues per user that Google is able to earn relative to its competitors.*" (5.286); In addition, Facebook may be able to extract more consumer data, or worsen the terms that it offers consumers for this data. (3.170).

[4] Ibid,

[5] Privacy International, Privacy International's response to the CMA's online platforms and digital advertising market study (30.07.2019), page 2.

[6] CMA, Online platforms and digital advertising, Market study interim report, 4.154-4.159 and Appendix F: Consumer control over data collection.

[7] Ibid, para 12.

and data protection are fundamental rights, to the difficulty of assessing the value of data and that such an approach would disproportionately impact on those already in vulnerable situations.[8]

Second, whilst consumers should have a choice over the amount of data they provide, it is imperative that the burden rests with not with consumers but with companies and as a matter of data protection law, companies should not be seeking data unless there is a clear justification for doing so, in accordance with the principles of data minimization and purpose limitation as well as the requirement of a legal basis. We would reiterate the concerning practices employed by many companies, supposedly offering individuals a 'choice', as highlighted in the report 'Deceived by Design' by the Norwegian Consumer Counsel.[9]

Response re Interventions

We welcome the CMA's approach towards considering structural or behavioural regulatory interventions (remedies) to limit anti-competitive behaviour of platforms with a dominant or 'strategic' position in the online market.[10]

For the purpose of this submission we will focus on potential interventions to give consumers greater control over their data, however as noted above we reserve our position further to comment on other proposed interventions. In particular we welcome engagement with Data Protection Authorities as well as direct action by the CMA using order making powers through a market investigation.

With this in mind we welcome consideration of the following:

- Consumers should have the option to use services without the use of their data for personalised advertising.
- This should be the default position.
- An obligation of 'Fairness by design'. It should be enforceable and enforced, and should complement existing obligations of fairness and data protection by design and by default in data protection law – which currently suffer from an implementation and enforcement gap.
- Competition and data protection authorities should consider jointly the interface between consumer, competition and data protection law. These are complimentary frameworks which must be used in tandem to address systemic problems with the current state of online advertising.

The interim report mentions that the "*inability of smaller platforms and publishers to access user data may therefore create a significant barrier to entry*"[11] and that "*Google and Facebook are better able to track users and*

[8] https://privacyinternational.org/long-read/3088/our-data-future
[9] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf
[10] Ibid, Chapter 6.
[11] Ibid, para 39.

demonstrate the effectiveness of using their platforms relative to others, which is likely to create a barrier to entry for potential rivals".[12]

The interim report goes on to state:

> 43. In principle, the General Protection Regulation (GDPR) makes gaining and managing consent within a 'walled garden' to deliver a particular purpose, an easier exercise than sharing data between firms to deliver the same purpose. Large, vertically-integrated platforms such as Google and Facebook may therefore have an easier task in obtaining consent from consumers to use their data for personalised advertising compared with publishers such as newspapers involved in the supply of display advertising in the open market.

Concerns re consent by dominant companies and data sharing incentives

Privacy International underlines that, while online platforms may offer products or services for free or at a very low price, these services are often used to mask data exploitation practices.[13] At the users' level, consumers do not know how their personal data is collected, used and shared with other parties; nor do they know when they have been tracked and profiled.[14] Because users' data is a valuable commodity (a "*proxy for price*", as noted by the European Data Protection Supervisor),[15] dominant online platforms increasingly continue to find ways to obtain yet more data in order to maintain and expand their control on the market.[16] Therefore, the fact that dominant companies like Google and Facebook might have better ways of ensuring consent will not always mean that this consent is obtained through

---

[12] Ibid, para 41.
[13] https://privacyinternational.org/long-read/3088/our-data-future.
[14] See: https://doteveryone.org.uk/report/digital-understanding/.
[15] EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, Sept 23, 2016, available athttps://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.
[16] For instance, in 2015 Facebook was fined by the Belgian Data Protection Authority ("DPA") for tracking the online activities of Belgian non-Facebook users through social plug ins (such as the like-button), cookies and invisible pixels on third-party web sites, https://www.dataprotectionauthority.be/news/judgment-facebook-case.The Belgian DPA's action was based on KU Leuven University's research revealing that Facebook's privacy policies breach European law. This comprehensive study, drafted at the request of the Belgian Privacy Commission, outlines the different data collection techniques, such as cookies, pixels, social plug-ins and other similar technologies used by Facebook to build up user and non-user profiles, see: https://www.law.kuleuven.be/citip/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation. The Belgian DPA's decision was challenged by Facebook on grounds of jurisdiction, however in February 2018 the Belgian Court of First Instance once again ruled that Facebook violated privacy laws, by deploying technology such as cookies and social plug-ins to track internet users across the web. The court ordered Facebook to stop tracking Belgians' web browsing habits and destroy any illegally obtained data. https://www.dataprotectionauthority.be/news/victory-privacy-commission-facebook-proceeding. In 2017, Facebook was also fined by the French Data Protection Authority (CNIL) for different privacy violations, among them "unfair" tracking of users and non-users as they browse the internet, without offering users sufficient warning. https://www.ft.com/content/10f558c6-3a26-11e7-821a-6027b8a20f23.

fair means or that it is valid.[17]

The solution to 'free' services should not be paying for privacy-enhanced products; privacy should not be something consumers have to pay for.[18] In addition, certain data exploitation practices would still constitute a violation of the relevant data protection and privacy laws, regardless of whether consumers refused to pay for not tolerating intrusive tracking. For example, a platform that implements cookies and other tracking technologies for third party marketing or advertising without users' valid consent would still be violating relevant privacy and data protection laws, regardless of whether the user is able to afford a paid membership or subscription for a service.

Privacy International is alarmed that any effort to monetise users' personal data or offer remuneration to users in return for their personal data will have harmful consequences for consumers and competition. It will inevitably infringe upon individuals' informational self-determination, as it will deprive them of every meaningful control over their personal data. At the same time, it will further exacerbate existing competition problems as dominant players will be the able to offer higher 'rewards' than competitors. Additionally, companies would have little incentive to promote data transfers or portability from one service to the other, as they will be heavily invested in purchasing data.

Concerns re access to data as a remedy

We note that one of the potential interventions in general search set out in Appendix J of the interim report is third-party access to search queries and click data (supply-side remedies). Specifically, this access remedy would require Google to provide competitor search engines with "*access to a number of data points, potentially some or all of; user queries, URLs returned, user clicks and any click backs, and other relevant data, such as location data or previous search, required to interpret the data above*".[19] This remedy seems to build on the Furman review which also identified situations where open access to personal data held by dominant business would be seen as an "*essential and justified step needed to unlock competition*".[20]

Privacy International is deeply concerned about suggestions or potential remedies that might suggest open access to data or users being offered remuneration for providing personal data to services.

First, personal data is not just any other economic asset. Privacy and the protection of personal data are fundamental human rights. As both the CMA[21] and the Information Commissioner's Office[22] have acknowledged, the

[17] See, for example, https://noyb.eu/4complaints/.
[18] https://privacyinternational.org/long-read/3088/our-data-future.
[19] Ibid, Appendix J: Potential interventions in general search, paras 32-45.
[20] Unlocking digital competition: Report of the Digital Competition Expert Panel, March 2019,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.
[21] CMA, interim report.
[22] Information Commissioner's Office (ICO), Update report into AdTech and real time bidding, June 20, 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-

way in which several players currently collect, amass and generate data often lacks transparency and seeks to maximise the amount of data available, through unfair means. This creates a race to the bottom; these dominant players already hold vast amounts of personal data across multiple services, and, even then, they still seem to be in a constant mission for more.[23] Data enhances their dominant position and exploitation –the lack of transparency, the manner in which such data is collected and then used, are all points which need addressed. This is why modern data protection laws like the EU General Data Protection Regulation include principles such as transparency, fairness, data minimisation and purpose limitation, and recognise the right to data portability, and demand that individuals must be given the tools to be in control of their data.

Second, Privacy International is very concerned that the implementation of personal data sharing standards can pose grave risks also for the security and integrity of consumers' personal data.[24]

Third, considering the vast quantities of data that Google holds hold on users and the opacity that the online advertising ecosystem is shrouded in, Privacy International seriously questions whether any data-sharing (third-party access) remedies could ever adhere to strict data protection laws, even if effectively pseudonymised. According to the interim report, the categories of personal data that could potentially be shared constitute user queries, location data or other relevant data that might be necessary to interpret the data received.[25]

There is a fine line between pseudoanonymous and anonymised data. The first can still render an individual identifiable. For example, journalists from the German public broadcaster NDR were able to identify the sexual preference and medical history of judges and politicians, using online identifiers.[26] This is just one example, that serves to illustrate the insights that can be gleaned from seemingly mundane and pseudonymous data and the value it might have.[27] Even if it is not a company's intention to directly identity an individual, this is still possible, due to the vast amount of data it might collect and generate. And, even when data seem to be truly anonymised by companies, and consequently exempt from the protection guaranteed by the General Data Protection Regulation, for example, this anonymisation might still lead to the re-identification of individuals. In a recent study, researchers were able

---

time-bidding-report-201906.pdf.

[23] https://privacyinternational.org/explainer/2293/competition-and-data.

[24] On 11 July 2019, the Irish Data Protection Commission (DPC) received a data breach notification from Google, following reports that contractors could listen to recordings made from people's conversations with their Google Assistant, https://www.bloomberg.com/news/articles/2019-07-12/google-data-breach-faces-review-by-irish-privacy-watchdog. In April 2019, a similar investigation by Bloomberg revealed that thousands of Amazon employees around the world are listening in on Amazon Echo users, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[25] Appendix J, para 41.

[26] https://www.theregister.co.uk/2016/11/07/browsers_ban_web_of_trust_addon_after_biz_is_caught_selling_its_users_browsing_histories/.

[27] See: https://privacyinternational.org/corporateabusetimeline.

to demonstrate that, despite the anonymisation techniques applied, "*data can often be reverse engineered using machine learning to re-identify individuals*."[28]

Fourth, we refer to two recent PI investigations. The first one relates to a Privacy International study that reveals how popular websites about depression in France, Germany and the UK share user data with advertisers, data brokers and large tech companies, while some depression test websites leak answers and test results with third parties.[29] The findings raise serious concerns about compliance with European data protection and privacy laws. This research also shows that some mental health websites treat the personal data of their visitors as a commodity, while failing to meet their obligations under European data protection and privacy laws. The second report focuses on menstruation apps, which are not just concerned with menstruation cycles but may also collect information about users' health, sexual life, mood etc. Due to the sensitivity of this information, Privacy International looked into whether any of these special-category data were shared with third parties without users' consent or even knowledge. As the report exposes, several apps conducted – at the time of the research – what we believe to be extensive sharing of sensitive personal data with third parties, including Facebook.[30]

This clearly demonstrates the importance for any proposed remedy to properly reflect on all consumers' wellbeing in the digital era, by assessing their needs, as well as respecting dignity and preventing the risk of social exclusion and stigmatization of certain groups and minorities. Therefore, we urge the CMA to consider GDPR-compliant alternatives to data sharing remedies, and, at the very least, extensively evaluate what problems the sharing raises from a data protection and privacy point of view and seek the opinion of data protection authorities.

Response re Market Investigation Reference

Finally, we ask the CMA to revisit its conclusion not to make a market investigation reference. As the CMA's initial findings rightly indicate, "*given the [...] number of consumers affected by them, a market investigation would appear to be a proportionate response*".[31] We are conscious of the fact that the anti-trust issues identified in the interim report are of global nature, as well as of the need that any changes pursued unilaterally by the UK need to be pragmatic. However, this should not deter the CMA from action.

For the reasons set out in our response to the Statement of Scope and taking into account the findings of this interim report, we still consider that a Market Investigation Refence to be the most appropriate mechanism.

---

[28] https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/.
[29] https://privacyinternational.org/campaigns/your-mental-health-sale.
[30] https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data.
[31] CMA, interim report, 7.9.

We strongly believe that a market investigation reference will not only provide the CMA with the opportunity to further investigate and understand the nature and extent of the issues in the market, but also to examine what the appropriate range of remedies might be to address them. Notwithstanding data-sharing remedies or remedies that might have onerous implications for consumers' privacy and data protection rights, and well-being in general, the CMA could use its order making powers to introduce increased interoperability in social media, as well as changes to the arrangements for determining the default search engine on browsers and devices. We do not believe the ongoing consideration by Government to be a sufficient justification to stall this process and use of the CMA's existing powers.