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

By e-mail: onlineplatforms@cma.gov.uk

30 July 2019

Privacy International's response to the CMA's online platforms and digital advertising market study

Privacy International welcomes the Competition and Market Authority (CMA)'s call for representations on online platforms and digital advertising.

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.

PI employs technologists, investigators, policy experts, and lawyers, who work together to understand emerging technology and to consider how existing legal definitions and frameworks map onto such technology. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

In the last year, Privacy International has conducted research into the ad tech and the data brokers industry exposing[1] and complaining[2] about their exploitation of personal data and the lack of transparency of their activities.

Based on our research and analysis of the current trends, the following sections provide Privacy International's observations on the three broad potential sources of harm to consumers in connection with the market for digital advertising: dominant position of online platforms; the lack of consumers' control over how their personal data is used and collected online; and the lack of transparency of the digital advertising market and its effects on competition and on consumers.

[1] See: https://privacyinternational.org/long-read/1721/snapshot-corporate-profiling.
[2] See: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.

Market power of online platforms in user-facing markets, and the impact on consumers

In the digital economy there is a trend towards corporate concentration. This is particularly true for digital platforms, such as social media platforms, search engines, digital entertainment, or online retailers. The way in which market dominance is measured traditionally does not always capture the extent of their market power, as their products and services are often 'free'.

With their business model relying increasingly on the availability of consumers' data, dominant online platforms can engage in various forms of data exploitation or even impose unfair terms for consumers.[3] In its statement on the data protection impacts of economic concentration, the European Data Protection Board (EDPB) has noted that the increase in the digital markets' concentration "*has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services*".[4]

The effects of this concentration of power are not limited to online and offline privacy. These companies can act as gatekeepers, for example by shaping how we access information on the web, including in some cases (e.g. Google or Apple) which applications we can install on our devices.

When assessing market power, competition authorities have tended to focus on price and outputs, giving little to no consideration to other factors affecting competition, such as quality, innovation and the implications for the exercise of certain fundamental rights, such as the right to privacy and the right to data protection. This narrow approach misses the increasingly important competition implications of the collection and further processing of personal data, especially when done at scale. It also fails to take into consideration the multiple effects that accumulating personal data has on certain types of digital services.

Privacy International encourages 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. As the German competition authority (Bundeskartellamt) noted in its decision against Facebook:

> Monitoring the data processing activities of dominant companies is therefore an essential task of a competition authority, which cannot be fulfilled by data protection officers. In cases of market dominance a competition authority must take into account data protection principles, in particular in the assessment of whether terms and conditions for the processing of data are appropriate.[5]

[3] See, for example, the class action lawsuit launched by the French consumer rights group UFC-Que Choisir against Google, https://www.quechoisir.org/action-ufc-que-choisir-vie-privee-donnees-personnelles-action-de-groupe-contre-google-n68403/.
[4] EDPB, Statement of the EDPB on the data protection impacts of economic concentration, Aug. 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.
[5] See page 7: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf.

Companies exploiting personal data often view privacy and data protection legislation as a threat to their business models. In its 2016 Annual report, Facebook noted how its business may be negatively affected by privacy, data protection, consumer and competition laws.[6] Alphabet Inc.'s 2017 Annual Report to the US Securities and Exchange Commission notes similar concerns and specifically states in relation to data protection regulation that "*these legislative and regulatory proposals, if adopted […] could, in addition to the possibility of fines, result in an order requiring that we change our data practices, which could have an adverse effect on our business and results of operations. Complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business*."[7]

Even where dominant market players may appear, more recently, to have taken a pro privacy and data protection stance,[8] this often stands in stark contrast with their practices,[9] including their position on other privacy protecting legislation, namely the ePrivacy Regulation.[10]

In a competitive market, it should be expected that the level of data protection offered to individuals would be subject to genuine competition, i.e. companies would compete to offer privacy friendly services.[11] However, in a data-intensive digital market characterised by increased corporate concentration, companies in a dominant position have no incentive to adopt business models and practices that enhance individuals' privacy, and they may seek to exclude any privacy enhancing players from any of the markets where they can exert market power.

An example of the impact a digital monopoly can have on both consumers and businesses would be when search engines provide services to third parties that require content indexation capabilities.[12] New or existing search engines must sign 'syndication contracts' to purchase content indexation and content ranking. In exchange, the purchasing company then displays the relevant content, accompanied by ads. As a result, dominant companies monopolising the content indexation market could "force" competitors that rely on their search results to

---

[6] "*Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding privacy, data protection, competition, consumer protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business.*", Facebook, Annual Report 2016, available at http://www.annualreports.com/HostedData/AnnualReportArchive/f/NASDAQ_FB_2016.pdf,

[7] See Alphabet Inc., Form 10-K, available at https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf.

[8] See, for example, Facebook: https://www.washingtonpost.com/gdpr-consent/?destination=%2fopinions%2fmark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas%2f2019%2f03%2f29%2f9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html%3fnoredirect%3don%26utm_term%3d.3a7544694000&noredirect=on&utm_term=.35aa4fe4ed3d; Google: https://www.blog.google/outreach-initiatives/public-policy/proposing-framework-data-protection-legislation/; Twitter: https://www.bloomberg.com/news/articles/2019-04-03/twitter-s-dorsey-adds-his-voice-to-support-of-regulation-in-tech.

[9] See: https://privacyinternational.org/blog/2773/are-you-serious-mr-zuckerberg.

[10] See: https://privacyinternational.org/blog/2815/new-faith-privacy-regulation-we-need-proof-conversion and https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/.

[11] In its 2014 assessment of the proposed merger of Facebook and WhatsApp (Case No. COMP/M.7217), the European Commission acknowledged that "*competition on privacy*" exists. It stated that "*apps compete for customers by attempting to offer the best communication experience*," including with respect to "*privacy and security, the importance of which varies from user to user but which are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues*," http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[12] See, for example: https://about.ads.microsoft.com/en-gb/resources/training/syndicated-partner-network.

include, for instance, unique identifiers in the URL of the ads that they place. This can seriously undermine the privacy protections offered by these companies to their users as they are then obliged to uniquely identify users, enabling tracking for the providing company, even if they as a company do not collect or retain that data.

In 2015, the Wall Street Journal published a Federal Trade Commission report relating to an investigation into Google's search and advertising practices.[13] The Report notes that "*Google has tied up a substantial portion of this distribution channel with exclusive and restrictive agreements. In the market for search syndication, Google has exclusive or restrictive agreements with 12 of the top 20 companies (60 percent) and 4 of the top 5 (80 percent)*."[14]

Dominant online platforms may seek to exclude rivals from the market by imposing data portability restraints (network effects), which can act as a barrier for entry into the market. At the same time, portability restraints undermine the effective exercise of users' data protection rights. The European Commission's report on Competition policy in the digital era noted that the right to data portability "*should be interpreted with a view to ensuring individual control of the data subject over his or her data, in particular with a view to avoiding data-induced lock-ins*."[15] The need to pursue "*personal data mobility and systems with open standards*" was one of the recommendations made by the Furman review.[16] In its decision against Facebook, the German Competition Authority (Bundeskartellamt) also noted:

> [Facebook's] strong identity-based network effects lead to a lock-in effect which makes it difficult for users or prevents them from switching to another social network. Existing functionalities and interfaces do not alleviate the consequences of Facebook's incompatibility with other social networks.[17]

Privacy International encourages the CMA to explore 'behavioural' remedies to limit anti-competitive behaviour of platforms with a dominant or "strategic" position in the online market.[18] This could be achieved by imposing , for example, open standards obligations on which systems could be built to enable compatibility of services, as well as stronger data portability obligations on online platforms with a dominant or strategic position so as to reduce any pronounced lock-in effects.[19]

---

[13] https://graphics.wsj.com/google-ftc-report.
[14] See page 104 of the Report, https://graphics.wsj.com/google-ftc-report/img/ftc-ocr-watermark.pdf.
[15] European Commission – Competition Policy in the digital era, final report 2019, page 82, http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
[16] 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.
[17] See: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3.
[18] For example, in the first *Microsoft* case, the Commission ordered Microsoft to provide interoperability information to competitors and to provide a version of Windows without the Windows Media Player, see Commission decision of 24 March 2004 in case 37792 *Microsoft*, http://europa.eu/rapid/press-release_IP-04-382_en.htm?locale=en.
[19] In a letter to FTC, on 12 July 2019, the Knowledge Ecology International (KEI) argued, for example, that Facebook's interoperability could be extended not only to Facebook-owned apps and services, but also to other social media web clients and apps as a remedy to counter-balance its strong network effects, https://www.keionline.org/wp-content/uploads/facebook-interoperability-remedies-FTC-KEI-12July2019.pdf.

The Furman review 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] In its Statement of scope,[21] the CMA aims to take on this suggestion and examine possible data sharing mechanisms.

Privacy International is very concerned that the implementation of personal data sharing standards might pose grave risks for the security and integrity of consumers' personal data.[22]

Personal data is not just any other economic asset.[23] Privacy and the protection of personal data are fundamental human rights. The way in which dominant players currently collect, amass and generate data often lacks transparency and seeks to maximise the amount of data available, through unfair means.[24] 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. 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 includes 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. At the very least, before imposing any data sharing obligations, it would be advisable from competition authorities to evaluate what problems the sharing raises from a data protection point of view and seek the opinion of data protection authorities.

Lack of consumers' control over the personal data used and collected by online platforms

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.[25] Because users' data is a valuable commodity (a "*proxy for price*", as noted by the European Data Protection Supervisor),[26] dominant online platforms increasingly continue to find ways to obtain yet more data in order to maintain and expand their control on the market.[27]

---

[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] https://assets.publishing.service.gov.uk/media/5d1b297e40f0b609dba90d7a/Statement_of_Scope.pdf.

[22] On 11 July 2019, the Irish Data Protection Commission (DPC) received a data breach notification from Google, following Google Ire 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.

[23] See: https://privacyinternational.org/long-read/3088/our-data-future.

[24] See: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[25] See: https://doteveryone.org.uk/report/digital-understanding/.

[26] EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, Sept 23, 2016, available at https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

[27] 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

When faced with a demand to consent to the terms of service and privacy policy by a company in a dominant position, users often have no genuine choice but to accept. This lack of choice is caused by a combination of factors: the significant relevance of network effects in these markets -where the utility of a service increases the more people use it, meaning that entrants require a 'critical mass' of users in order to compete, while users may only use the competing service when it has been generally adopted; lock-in of users; lack of alternatives; imposition of terms and conditions with poor privacy safeguards.[28] Companies such as Google, Facebook or Amazon continue to impose terms and conditions to users which allow them to collect, analyse and share personal data in ways that people do not understand (or cannot genuinely consent to).[29]

Privacy intrusive default settings, deceptive designs, vague or misleading language and threats of downgrading the service are just some examples of abuses and signal how consumers' data protection rights can be undermined in the online market.[30] Accordingly, they raise serious transparency concerns, as consumers will very often be unaware of the extent of the collection and use of their personal data, allowing thus platforms to extract data from them.

In a report dated December 2018, Privacy International revealed how Facebook routinely tracks users, non-users and logged-out users outside its platform through Facebook Business Tools.[31] It was found that at least 61 percent of the apps tested automatically transfer data to Facebook the moment a user opens the app. This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not. If combined, these personal data could paint a fine-grained and intimate picture of people's activities, interests, behaviours and routines, some of which can reveal special category data, including information about people's health or religion.[32]

Furthermore, Privacy International's investigation found that some apps routinely send Facebook data that is incredibly detailed and sometimes sensitive. Again, this concerns data

---

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.

[28] See, for example, WhatsApp forcing its users to accept new terms and conditions that led to the sharing of personal data with Facebook: https://www.theverge.com/2017/5/18/15657158/facebook-whatsapp-european-commission-fine-data-sharing.

[29] See, for example, the complaints filed by noyb – the European Center for Digital Rights against Facebook, Google, WhatsApp and Instagram. The complaints, which were filed on behalf of consumers across the EU, allege that these four companies were violating users' data protection rights by "forcing" them to agree to abusive and bundled data exploitation practices, https://noyb.eu/4complaints.

[30] See, for example: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[31] See: https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf.

[32] See: https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report.

of people who are either logged out of Facebook or who do not have a Facebook account.[33] This practice (which is not only limited to Facebook) illustrates how social media platforms can use their dominance in the online market to track users and non-users outside of their platforms.

Consumers often mistakenly assume that data that is not associated with their name is truly anonymous. However, 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.[34] 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, there are many more[35] and the value it may have. Even if it is not a company's intention to directly identity an individual due to the vast amount of data they collect and generate, it is possible, 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 to demonstrate that, despite the anonymisation techniques applied, "*data can often be reverse engineered using machine learning to re-identify individuals*."[36]

Further, a report by Digital Content Next found that "*a major part of Google's data collection occurs while a user is not directly engaged with any of its products*."[37] Considering that the Android operating system is the most widely used worldwide with more than 2 billion users, this raises significant concerns around the magnitude of the personal data collected. The report also showed that anonymised data collected by Google through passive methods, could still be associated with personal data of users through advertising.[38]

In its Update report into adtech and real time bidding, the Information Commissioner's Office (ICO) noted that "*the privacy notices provided to individuals lack clarity and do not give them full visibility of what happens to their data*."[39] The ICO also underlined that "*the scale of the creation and sharing of personal data profiles in RTB appears disproportionate, intrusive and unfair, particularly when in many cases data subjects are unaware that this processing is taking place*."[40]

Privacy International raised similar concerns in its submission before the ICO on ad-tech companies and data brokers.[41] Privacy International's submissions demonstrated that many companies fail to comply with basic Data Protection Principles or even seem to work under the assumption that derived, inferred and predicted data and demographic segments do not

---

[33] Ibid.
[34] See: https://www.theregister.co.uk/2016/11/07/browsers_ban_web_of_trust_addon_after_biz_is_caught_selling_its_users_browsing_histories/.
[35] See: https://privacyinternational.org/corporateabusetimeline.
[36] https://www.imperial.ac.uk/news/192112/anonymising-personal-data-enough-protect-privacy/
[37] See: https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.
[38] Ibid.
[39] 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-time-bidding-report-201906.pdf.
[40] Ibid.
[41] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

count as personal data, even if they are linked to unique identifiers or used to target individuals.[42] The lack of transparency is exacerbated by the fact that these companies are non-consumer facing, most people have never heard of these companies, and, even if they have, there is a dearth of information as to where the data is sourced and who it is shared with. Accordingly, this has a knock-on effect on the exercise of rights and the ability to exercise any control, for example through an access or erasure request. Difficulties faced by members of Privacy International's team in exercising access request rights are set out in the complaints as well as challenges with opt-out mechanisms, there were further frustrations with follow up erasure requests.[43] There was also a lack of willingness to provide Data Protection Impact Assessments and Legitimate Interest Assessments which would provide further insight into companies' justifications for processing and how the rights of individuals have been taken into consideration.

The lack of transparency around the exploitation of users' personal data by online platforms has also negatively impacted the online trust of consumers. According to a 2019 Special Eurobarometer Survey, the majority of respondents indicated that they have partial control over the information they provide online, with 62% of them being concerned.[44] Concerns were also expressed by users in the CMA's report into the collection and use of consumer data. The report found that consumers were concerned about the potential misuse of their data, while they unable to fully understand the precise data companies collected on them and how this data was used exactly.[45]

Privacy International urges the CMA to address the lack of transparency and related lack of consumer control over what happens to their personal data in the digital market, by exploring ways to strengthen transparency and meaningful consent mechanisms around personal data flows. The inherent information asymmetry in the online market could be improved, for instance, by imposing a 'fairness by design' duty that would require online platforms to provide for privacy policies in concise, exhaustive and clear language, granular consent mechanisms, and by limiting the ability of online platforms to share data across various applications. The latter was an approach that the German competition authority (Bundeskartellamt) also decided to follow in its decision against Facebook.

Lack of transparency of the digital advertising market and its effects on competition and on consumers

It is impossible for individuals to understand where their data ends up. At the market level, it has become equally impossible to map, monitor and audit how data flows in an increasingly opaque data ecosystem[46] and some legislative initiatives have emerged seeking to provide more transparency and control over data brokers.[47] However, this is in a context where there is no comprehensive data protection legislation. Yet, whilst data protection law mandates transparency requirements for individual data controllers, including providing information as

[42] https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what
[43] https://privacyinternational.org/blog/2549/have-companies-deleted-your-data
[44] http://europa.eu/rapid/press-release_IP-19-2956_en.htm.
[45] https://www.gov.uk/cma-cases/commercial-use-of-consumer-data.
[46] http://crackedlabs.org/en/corporate-surveillance.
[47] See, for example, Vermont's Data Broker Regulatory Regime, enacted on May 22, 2018, available at https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/H-0764/H-0764%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf

to the source of personal data and the categories of recipients of personal data, it does not provide for transparency of a particular market, including the digital advertising market.

Between the demand and supply side of digital advertising are a number of intermediaries, whose role is both to enhance and enrich users' data, and to offer technologies permitting programmatic advertising. These actors rely on data collected through various means and participate in the sharing of personal data at a large scale, through processes such as real time bidding (RTB). What online platforms have in common is their ability to monetise users' attention to sell advertising, while at the same time the more user data they have the more targeted digital ads can be.

It is worth noting that what is understood to be users' data can cover quite a large variety of data. In the case of the Facebook platform, for example, this includes all information provided by the user plus tracking information, while in the case of programmatic advertising it will range from browsing history to location, inferred interests, purchase history and other profiles created by various third parties.

The extent that users' personal data might be shared within the online demand-supply chain for the purposes of targeted advertising remains opaque. These transparency concerns were also highlighted by the ICO update report. According to the ICO, "*it is unclear whether RTB participants have fully established what data needs to be processed in order to achieve the intended outcome of targeted advertising to individuals. The complex nature of the ecosystem means that in our view participants are engaging with it without fully understanding the privacy and ethical issues involved*."[48] The RTB system does not operate in a complete vacuum, rather according to industry frameworks, namely the IAB Europe (Transparency and Consent Framework) and Google (Authorised Buyers Guideline). Various concerns with these frameworks have been raised in a complaint to the ICO and are echoed in similar complaints around the EU.[49]

Large platforms often occupy different positions in the complex online advertising ecosystem.[50] This consequently raises a series of concerns relating to the conflict of interest faced by these platforms, which for example may be a data source, an advertiser and a publisher amongst other roles. A report commissioned by the Department for Digital, Culture, Media & Sport on online advertising in the UK highlighted that, as a consequence of their ownership of also strong user data assets, "*Google and Facebook are, to some extent, able to set their own terms to advertisers and publishers*."[51]

On 17 July 2019, the European Commission announced that it is opening "*a formal antitrust investigation to assess whether Amazon's use of sensitive data from independent retailers who sell on its marketplace is in breach of EU competition rules*."[52] Based on the

[48] Information Commissioner's Office, Update report into adtech and real time bidding, June 20, 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[49] https://fixad.tech/
[50] See, for example: https://www.nytimes.com/2018/08/12/technology/google-facebook-dominance-hurts-ad-tech-firms-speeding-consolidation.html and https://www.theguardian.com/media/2019/jul/22/internet-advertising-grow-digital-scandals-facebook-google.
[51] See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777996/Plum_DCMS_Online_Advertising_in_the_UK.pdf.
[52] http://europa.eu/rapid/press-release_IP-19-4291_en.htm

Commission's preliminary findings, Amazon appears to abuse its dominant position on the online market, by using competitively sensitive information about its marketplace sellers.

Similarly, focusing on the huge power of online platforms in the online advertising market, the Cairncross Review underlined that there "*is undoubtedly a lack of transparency across the advertising supply chain*" and that "*online platforms can impose terms on publishers without consulting or negotiating with them*."[53] It concluded that, due to the opacity of the online advertising market, there is a need for regulators to study the market.

Privacy International encourages the CMA to consider remedies that would address the online platforms' dual role of marketplace and seller. This should include articulating clear rules on the terms on which dominant platforms or platforms with strategic market status (as described in the Furman review) transact with other market participants and increasing transparency both to consumers and advertisers in the different activities undertaken by the platforms; and separation between certain activities in the digital advertising value chain. Furthermore, Privacy International encourages the CMA to review the frameworks under which the RTB system is operating from a competition perspective, including whether such agreements effect the prevention, restriction or distortion of competition, including fixing the conditions under which personal data is exchanged, sharing various sources of data and having multiple roles within the ecosystem.

Conclusions

In all, Privacy International believes that the digital advertising market is shrouded in opacity. The lack of transparency in the online advertising ecosystem, as well as the unlawful personal data-gathering practices, in which online platforms, ad tech companies and data brokers seem to engage, have undermined consumers' fundamental rights and affected their control over the personal data they surrender to these platforms. Ultimately, this has resulted in a significant loss of consumers' trust in the online market.

In line with the recommendations of the Furman review, Privacy International therefore urges the CMA to address the inherent lack of transparency and the consumer detriment in the online advertising market, by making a market investigation reference under section 131 of the Act that will scrutinise the role of dominant or strategic platforms in the digital advertising market and strengthen the enforcement of consumers' rights against abusive practices. In carrying out such investigation, we encourage the CMA to liaise closely with its competition and data protection counterparts both domestically and internationally.[54]

[53] See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf.

[54] The growing need for continued cooperation and support between regulators, in in order to achieve a better understanding of anti-competitive practices, and convergent competition enforcement in cross-border practices and multijurisdictional cases was recently highlighted by the G7 Competition Authorities, see Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy" Paris, June 5, 2019, http://www.autoritedelaconcurrence.fr/doc/g7_common_understanding.pdf.