Open Rights Group submission to the Competition and Markets Authority "Notice of intention to accept binding commitments offered by Google in relation to its Privacy Sandbox Proposals"

9 July 2021

Table of Contents

Executive Summary

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK. We were heavily involved in the process leading up to the enactment of the Data Protection Act 2018 ("DPA 2018"), and we worked on issues such as data retention, the use of personal data in the COVID-19 pandemic, data protection enforcement, online advertising and the use of personal data by political parties.

In this submission, we provide feedback to the Consumer and Markets Authority (CMA) "Notice of intention to accept binding commitments offered by Google". While we agree with the CMA analysis of the issues regarding Google deployment of "Privacy Sandbox", we emphasise several issues regarding the substance of Google's commitments (Proposed Commitments). If left unaddressed, ORG believes that these Proposed Commitments would ultimately fail to tackle some of the concerns the CMA has raised, namely that Google could

- exploit its apparent dominant position by denying Chrome web users substantial choice in terms of whether and how their data is used to target and deliver advertising to them; and
- distort competition in the market for the supply of ad inventory in the UK and the market for the supply of ad tech services in the UK.

The issues we identified are:

- Google commits to comply with data protection principles instead of data protection law, whose obligations are more detailed and substantiated.
- Google never commits to deploying an opt-in mechanism, to allow Chrome users' to choose whether to be tracked and targeted with adverting.
- Google's commitments regarding their use of data are vague.

For each of these points, we first explain the issue we identified; then, we compare it against CMA concerns; finally, we provide recommendations.

A.1 – Google does not commit to comply with data protection laws

Google promise to "design, implement and evaluate the Privacy Sandbox proposals" having regard to some "Development and Implementation Criteria". Among these criteria, they include "impact on privacy outcomes and compliance with data protection principles".

We find this commitment to be too generic and open to abuse. In particular, data protection principles are but an aspect of data protection legislation, which also includes data subjects rights (Chapter 3 of the UK GDPR), obligations for controllers and processors (Chapter 4), provisions regarding the transfer of personal data to third countries (Chapter 5) and provisions relating to specific processing situations (Chapter 9). Referring to data protection principles instead of data protection legislation could give Google leeway not to consider their broader obligations under data protection law.

As a general observation, Google has been a repeat offender in the field of data protection. Among the most relevant breaches of data protection laws which are relevant for the issues raised beforehand:

- Google circumvented security protections in web browsers to gain access to third-party cookies for advertising purposes;[1]
- Google was already fined for lack of compliance with data protection law;[2]
- Google extensively relies on deceptive users' interferences to harm consumers and deprive them of agency over their privacy choices.[3]

Thus, their commitment to comply with legal requirements they habitually and continually break should be treated with suspicion.

A.1 – Recommendations:

Google should amend their "Design and Implementation Criteria" to include compliance with data protection law, as opposed to data protection principles.

---

1 See Tech Crunch, *Google under fire for circumventing Safar privacy settings*, at: https://techcrunch.com/2012/02/17/google-under-fire-for-circumventing-safari-privacy-setting/ see also: http://webpolicy.org/2012/02/17/safari-trackers/

2 See BBC, *Google hit with £44m GDPR fine over ads*, at: https://www.bbc.com/news/technology-46944696

3 See Norwegian Consumer Council, *New analysis shows how Facebook and Google push users into sharing personal data*, at: https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/

Furthermore, the CMA should include, where possible stronger safeguards regarding the monitoring of Google compliance with these terms and the implementation of their “Proposed Commitments”.

A.2 – Google does not commit to an opt-in regime

Google states in point 16 letter d (Users' control) that they "will update the CMA on its plans for user controls in relation to the Privacy Sandbox proposals, including default options and choice architectures, and it will share with the CMA the user research and testing which underpins its decisions on user controls." However, Google never commit, there or in any other part of their Proposed Commitments, to the implementation of a clear and GDPR compliant opt-in regime, although "freely given, specific, informed and unambiguous" consent is the only legal basis that can be relied upon in the context of online advertising. The vagueness of Google commitments under point 16(d) is concerning, in particular where Google foresees to base their choices regarding users' controls and defaults on "research and testing", rather than on legal requirements and users' rights.

Indeed, the ICO found in their "2019 update report into adtech and real-time bidding"[4] that consent is the only legal basis that can apply to the processing of personal data for advertising purposes. Although these findings were made in the context of real-time bidding and third-party cookies, the conclusions that were reached there would still apply to the new adtech systems Google is developing.

Firstly, explicit consent is always necessary for the processing of special category data, such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership [...] data concerning health or data concerning a natural person's sex life or sexual orientation". Users' behaviour on the Internet inherently exposes at least some of these traits. Indeed, the taxonomies of some of the biggest adtech providers show that profiling Internet users based on very sensitive aspects is the norm.[5] For instance, Google existing adtech systems include categories such as "substance abuse", "diabetes", "chronic pains" and "sleep disorder".[6]

Secondly, separating special category data from non-sensitive information in the context of behavioural advertising does not seem feasible in practice. However, even if it were possible to do so, consent would still represent the only available legal basis for this processing. Indeed, the ICO points out that "trying to apply legitimate interests when an organisation has GDPR-compliant consent would be an entirely unnecessary exercise and would cause confusion for individuals". Furthermore, the

4 See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/

5 For instance, Internet users are usually targeted based on categories such as "belonging to the LGTB community", "AIDS and HIV", "incest and abuse support", "brain tumour", "incontinence", "depression", "infertility", "sexually transmissible diseases", "political affiliation".

6 See ICCL, *Johnny Ryan's key insights*, at: https://www.iccl.ie/wp-content/uploads/2020/09/Real-Time-Bidding-2-years-on-Key-insights.pdf

ICO finds that “the nature of the processing within RTB makes it impossible to meet the legitimate interests lawful basis requirements” and that “consent is also the most appropriate lawful basis for the processing of personal data beyond the setting of cookies”. In other words, the ICO identifies consent as the appropriate legal basis even in the event of a phase-out of third-party cookies.

Thirdly, it is worth noticing that the analysis of a given user’s behaviour to target advertising based on their interest is superfluous to browse the Internet. If turned on by default, it would breach the principle of “data protection by design and by default”, where personal data must be processed with the highest privacy protection by default. Thus, an opt-in regime wouldn’t only be needed because it is the appropriate legal basis, but as for the adherence to the same principles that Google allegedly commits to implement.

A.2 – Analysis against CMA stated concerns

Unfair terms on Chrome users: Google could impose unfair terms on Google users in several manners:

- **Legitimate interest as a legal basis:** Google could claim that its privacy sandbox proposals are processing users’ data based on legitimate interest. However, reliance on legitimate interest would require that processing those data is necessary to achieve legitimate purposes, and those purposes override data subjects interests, rights and freedoms. Google would likely lack any ground to claim that online tracking is “necessary” for targeting advertising — given that this can be done without the need for personal information. Furthermore, their interest could not possibly override that of the data subjects, given the pervasiveness of online tracking and the well-documented harms associated with tracking advertising.

  However, Google lack of a clear commitment to implement a strictly opt-in, consent-based regime for its adtech systems may indicate Google intention to unlawfully process Chrome users’ data behind the veneer of legitimate interest.

- **Contractual obligation as a legal basis:** Google could claim that thei Privacy Sandbox proposals are processing users’ data based on contractual obligations — for instance, the terms and conditions that Chrome users submit to when installing this software. However, personal data can be processed to fulfil a contractual obligation only and insofar this processing is necessary to fulfil contractual obligations. Tracking users’ activities online to deliver targeted advertising is in no way necessary to provide the

functionality that a web browser is meant to offer and, indeed, the majority of the other browsers in the market is not processing personal data for this purpose.

However, in the absence of a clear commitment to implement a strictly opt-in, consent-based regime for its adtech systems, Google may try to justify the unlawful processing of users' data by relying on the Terms of Use of Chrome.

- **Invalid consent and dark patterns:** Google currently relies on dark patterns and deceptive design to force users' consent and reduce individuals' agency over their privacy choices.[7] The UK GDPR does provide a clear description of the requirements for consent to be freely given, specific, informed and unambiguous.

  However, in the absence of a clear commitment to comply with data protection laws as opposed to "data protection principles", Google may try to purport their new adtech systems as opt-in while effectively depriving individuals of a free and fair choice over the use of their personal information.

An unfair advantage over competitors: A growing number of studies are showing that in general, consumers are not comfortable with online tracking and profiling.[8] This indicates that, if given a choice, a large majority of consumers would decline the offer. The recent implementation by Apple of a simple opt-in feature in their iOS devices does provide support to this thesis, as it is estimated that less than 4% of iOS users are allowing online tracking.[9]

However, in the absence of a clear commitment to target users' based on their consent, Google can target users that would otherwise be out of reach. Given that

- advertising is valuable insofar it can reach the audience it is intended to, and
- recent data suggest that around 96% of Internet users would decline the offer to be targeted with advertising, either by Google or others

It follows that Google effectively gains an unfair advantage on the market by targeting most Internet users' unlawfully and against their will. This distorts competition against other companies that may not be in the position to circumvent

7 See Norwegian Consumer Council, *New analysis shows how Facebook and Google push users into sharing personal data*, at: https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/

8 See Norwegian Consumer Council, *Out of Control Report, §3.1. Consumers do not want to be tracked, but feel powerless*, at: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

9 See Ars Technica, *96% of US users opt out of app tracking in iOS 14.5*, analytics find, at: https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/

legal requirements, as well as against forms of privacy-enhancing advertising that may lawfully serve advertising without requiring users' consent — for instance, contextual advertising — that would otherwise be able to reach a much wider audience compared to Google.

A.2 – Recommendations:

Google should commit to process Chrome users' data based on their "freely given, specific, informed and unambiguous" consent, according to article 4(11) of the UK GDPR.

Apple's recent implementation of the App Tracking Transparency framework shows how baseline consent requirements would need to be implemented in practice by Google, namely:

- individuals shouldn't be tracked or targeted with advertising based on their interests by default;
- individuals should be allowed to deny online tracking with the same ease as they can consent to it; and,
- individuals should be given the option to deny tracking once and ask not to be bothered again with this question.

A.3 – Proposed Commitments are framed in unclear language

In letter G of their Proposed Commitments, Google promise not to use "any Individual-level User Data" from the sources listed below to track and target users:

- Google's current and future user-facing services, including Android;
- a user's Chrome browsing history, including synced Chrome history;
- a publisher's Google Analytics account; and
- uploaded by an advertiser to Customer Match in accordance with Google's Customer Match policy.

The same is repeated in §23 of their Proposed Commitments (Google owned and operated inventory). While these commitments are welcomed in principle, their wording is concerning and it risks undermining their substance.

Firstly, committing not to reuse these "Individual-level User Data" to track and target users seem to intend that these same data could be instead repurposed in an aggregated or otherwise non "individual-level" form. Given that "individual-level" user data lacks a legal or any other definition, this raises concerns over the extent to which Google is committing not to reuse their first-party data to target users with advertisement.

Secondly, Google oddly commits not to rely on "a publisher's Google Analytics account". The language chosen by Google here seems to indicate that they intend to commit to data siloing Analytics data only and insofar they refer to a publishers' website. Websites, however, can be operated by a variety of actors that are not publishers. Furthermore, Google runs a large number of analytics services on several domains — for instance, "Google Firebase" in the context of cloud services.[10]

Thus, excluding some of these analytics services, or excluding only those Google Analytics accounts that are operated by the publishing industry, would be at odds with the concern that Google could gain an unfair advantage over competitors through the use of data from their user-facing services in Google's advertising businesses. Furthermore, and lacking a meaningful understanding of what does Google intend for "Individual-level User Data", the extent to which this commitment is suitable to address these concerns or not is difficult to measure.

10 See: https://firebase.google.com/

A.3 – Analysis against CMA stated concerns

Unfair terms on Chrome users: purpose limitation is the cornerstone of data protection and individuals' control over their data. If organisations were allowed to collect information under a pretext and later reuse these data for other purposes, it would undermine individuals' ability to make ponderated choices.

Google vague wording regarding their commitments under letter G (Google use of data) may ultimately allow them to escape their Proposed Commitments, for instance by arbitrarily categorising certain data as "non-Individual-level Data", or by excluding from the scope of their commitments any Analytics services that could be said not be "a publisher's Google Analytics account". In turn, this would expose users' to unfair treatment and privacy harms.

Unfair advantage over competitors: based on the observations above, Google ability to evade their commitments under letter G would allow them to rely on first-party data to gain an unfair advantage over their competitors.

A.3 – Recommendations

The Proposed Commitments should clarify what "Individual-level User Data" means and how they would be distinguishable from "non-Individual-level User Data". This could be achieved by referring to legal definitions under article 4 of the GDPR, such as "personal data" as opposed to "anonymous data".

Furthermore, the Proposed Commitments should define what sources of data Google intends to use to target users with advertisements, as opposed to what sources of data they intend to exclude from this scope.

B – Broader considerations regarding the CMA approach

Open Rights Group observes that the CMA is taking on the most relevant tech issues we are facing today. At the time of writing, the CMA has or is conducting investigations in the field of

- Digital markets and online advertising
- Algorithmic discrimination
- Facebook use of data
- Apple's app marketplace
- Online fake reviews

Furthermore, the CMA was given the lead to regulate digital markets from both a competition and data protection perspective with the Digital Markets Unit. This should be seen in relation to adtech, whose issues go well beyond competition: today's adtech market is rigged by illegality, fraud and harm for users, both in terms of privacy and their overall welfare.[11] This led to growing demands from policymakers to ban tracking advertising. Likewise, users' opt-out rate after Apple new tracking feature shows that users do not trust online trackers.

While we do recognise the CMA effort to cooperate with the ICO, we cannot ignore that an analysis of the data protection implications of Google Privacy Sandbox is fundamentally missing from the CMA "Notice of intention". The same can be said about the existing "third-party cookies" based advertising systems, which would remain in place if the CMA were to halt Google plans to phase out TPCs.

However, lack of compliance with data protection and abuses in this field are at the core of the adtech issue. Any meaningful reform must have a holistic approach, and regulators' focus shouldn't be sectorial.

B – Recommendations:

The CMA must make sure that competition, consumer and data protection issues are duly tackled in the process.

The CMA should be ready to consider to develop, together with the ICO, an enforcement plan against Google's failure to scrap the current RTB/third-party cookies adtech system and address the illegality of their existing adtech products.

11 See Norwegian Consumer Council, *Time to Ban Surveillance-Based Advertising*, at: https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

Conclusions

Open Rights Group praises the CMA attempt to proactively monitor Google's phase-out of third-party cookies and the deployment of Privacy Sandbox. Existing adtech systems are rigged with illegality and data abuse, making the reform of the adtech sector a priority for protecting individuals rights to data protection on the Internet.

However, we identified several concerns regarding Google's "Proposed commitments", namely:

- Google commits to comply with data protection principles as opposed to data protection law, whose obligations are wider and more substantiated.
- Google never commits to the implementation of a clear opt-in regime to allow Chrome users' behaviour to be tracked and used to target them with adverting.
- Google's commitments regarding their use of data are vague.

In order to address these issues, we provide a set of recommendations, summarised below:

- Google should amend their "Design and Implementation Criteria" to include compliance with data protection law, as opposed to data protection principles.
- The CMA should impose, where possible, stronger safeguards regarding the monitoring of Google compliance with the "Proposed Commitments"
- Google should commit to process Chrome users' data based on their "freely given, specific, informed and unambiguous" consent. Chrome Users should be able to say no as easily as they can say yes, and should be able to set their preferences permanently.
- The "Proposed Commitments" should clarify what "Individual-level User Data" means and how they would be distinguishable from "non-Individual-level User Data", possibly by referring to the legal definitions of "personal data" and "anonymous data".
- The "Proposed Commitments" should define what sources of data Google intends to use to target users with advertisements, as opposed to what sources of data they intend to exclude from this scope.

We are of the view that, if left unaddressed, they would pose a threat to the stated objectives of the CMA. Ultimately, it would represent a missed chance to drive meaningful change in the adtech market, and ensure that the new proposals to replace adtech existing "TPCs" systems result in substantial rather than cosmetic improvements.