8 July 2021

Competition and Markets Authority (CMA)
By email to: 50972-Consultation@cma.gov.uk

Re: Mozilla's Response to the
Public Consultation on Proposed Commitments in respect of Google's 'Privacy Sandbox' Browser Changes by the United Kingdom's Competition and Markets Authority

To the CMA:

Mozilla welcomes this public consultation on the proposed commitments (hereafter collectively referred to as 'Commitments') offered by Google. We believe that meaningful opportunities for market stakeholders to engage with competition remedies can better inform competition outcomes and commend your efforts in this regard.

Today regulators and technology companies together have an opportunity to improve the privacy properties of online advertising—an industry that has not seen privacy improvement in many years. We strongly support Google's Commitments to refrain from self-preferencing when using the Chrome Privacy Sandbox technologies and not to combine user data from certain sources for targeting or measuring digital ads on first and third party inventory. This is a positive change that all dominant platforms should embrace beyond just advertising or browser technologies to ensure a fairer and more equitable web.

Our submission addresses two issues that—if added to the proposed Commitments—will help ensure a safer online experience for consumers and more competitive internet for all companies.

I. About Mozilla

Mozilla is deeply invested in creating a trusted online ecosystem both as a browser maker and as a stakeholder in the broader internet ecosystem. Mozilla develops and distributes the Firefox web browser, adopted by hundreds of millions of individuals around the world. Mozilla is also a Foundation that works towards educating and empowering people to actively shape their experiences online.

II. Summary

The CMA has the opportunity now to create a higher standard of baseline consumer privacy protections *together with* an even, competitive playing field. This would allow large and small platforms alike to compete on their merits while respecting user privacy, rather than the status quo, where user data collected across product verticals is frequently leveraged to inhibit consumer control and unfairly limit competition. To that end, **we strongly support binding Commitments that would prohibit Google from self-preferencing and prohibit Google from combining user data from certain sources.** We appreciate Google's willingness to put forward these commitments in the context of its Chrome Privacy Sandbox proposals. This approach provides a model for how regulators might protect both competition and privacy while allowing for innovation in the technology sector, and we hope to see this followed by other dominant technology platforms in other spaces as well.

At the same time, we encourage the CMA to reconsider requirements that will hinder efforts to build a more privacy respecting internet. Major technology platforms should be encouraged to remove tracking technologies from their products, particularly third-party cookies, which are used for online tracking and cause significant harm to individuals and society. Consumers would benefit the most if the CMA decoupled its approaches towards: (1) Google's plans to deprecate third-party cookies and (2) other Chrome Privacy Sandbox proposals.

To do this, **we encourage the CMA to narrow the scope and timing of its Standstill Period to only the deployment of new functionality in the Chrome Privacy Sandbox proposals**, such as but not limited to, FLoC and TURTLEDOVE. This would better align the purpose of the Standstill Period to allow for stakeholder feedback on relevant new technologies and timelines prior to Google's wide scale deployment. Further, this would better align regulatory scrutiny alongside well-established standardization processes that enable public engagement during the *development* of technology specifications but have no oversight over stakeholder *deployment* of those technologies.

By contrast, the Standstill Period is currently framed to apply only to Google's removal of third party cookies and is not tied to the actual deployment of the Chrome Privacy Sandbox proposals.

This has two issues: first, global consumer privacy will be disproportionately affected if the CMA prevents Google from deploying limits on third party cookies, something other major browsers have already done because of privacy and security concerns. Further, this does not address the potential issues that arise from deployment of its Chrome Privacy Sandbox proposals, a space in which regulatory oversight could be helpful. Indeed, Google has already publicly delayed its plans to block third party cookies from Chrome until 2023. To ensure this is not further delayed and competition scrutiny does not delay progress on established privacy and security issues, **we encourage the CMA and ICO to jointly recognize the need to expeditiously protect consumers from third party cookie-based tracking and focus the scope of the Standstill Period on deployment of the Chrome Privacy Sandbox proposals.**

It is equally critical for new functionality introduced by the Chrome Privacy Sandbox proposals to be thoroughly vetted to understand their implications for privacy and competition by all relevant stakeholders in a public and transparent manner. For this reason, **we encourage the CMA to require an explicit commitment by Google to not deploy relevant Chrome Privacy Sandbox proposals unless they have been developed via formal processes at open SDOs.**

III. The Standstill Period Should be Narrowed to Ensure Expeditious Consumer Protection from Online Tracking

Third-party cookies (TPCs) represent a wrong turn taken years ago in browser development. While they have some legitimate uses, like federated login, they are mostly used to track consumer behaviour. They provide the underlying technology that allows for much of the harmful activity we see online today: collection of data without consumer knowledge, sharing and selling of that data, and use of that data to target and manipulate people with massive social consequences, for example, misinformation campaigns and voter manipulation. While notionally some consumers might consent to this tracking, most people have no idea it is occurring. Consequently, because they do not know that tracking is occurring, they cannot adequately protect themselves. Cookie consent banners, intended to empower consumers with more control, have made this situation worse by bombarding consumers with dialog boxes that they tend to ignore or quickly dismiss by clicking "I agree" without providing meaningful consent.[1] Finally, studies[2] show that, when users do understand tracking, they object to it strongly.

If users cannot reasonably be expected to protect themselves, it is critical that the browser step in with default protections. At Mozilla, we have been working for years to drive the industry in a better direction away from third-party cookies tracking. In 2015, Mozilla launched Tracking

[1] Most EU cookie 'consent' notices are meaningless or manipulative, study finds by Natasha Lomas, TechCrunch. (10 August 2019) Available at: https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/

[2] Australian Community Attitudes to Privacy Survey (2017). Available at: https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2017/acaps-2017-report.pdf

Protection,[3] our first major step towards blocking tracking in the browser. In 2019, we turned on a newer version of our anti-tracking technology by default for all users.[4] The merits of these changes have been apparent to the privacy community for years,[5] which is why every other major browser besides Chrome (which between them occupy well over 30% of the market share for web browsing in the UK)[6] has sought to clamp down on cookie-based cross-site tracking.

Chrome is the only major browser that currently does not offer some level of default protection from tracking via third party cookies, and the internet cannot evolve in a more privacy-respecting direction without Chrome. For this reason, we believe the CMA should decouple its approach to third party cookies from its approach to Google's Chrome Privacy Sandbox proposals. It is important for agencies such as the CMA and Information Commissioner's Office (ICO) to publicly recognize the value of expeditiously limiting the role of third party cookies used for web tracking from all browsers to better protect consumers from harm. This can be done by narrowing the scope and timing of the CMA's Standstill Period and applying that period only to the deployment of new functionality in the Chrome Privacy Sandbox proposals.

Those proposals are complex and require considerable examination from regulators and industry to understand their full implications, which these Commitments go a long way in helping set up. On the other hand, proposals that limit the use of third party cookies for pervasive and opaque web tracking should move forward on an unconditional time frame. As evidenced from their widespread adoption in various forms by the rest of the browsing industry, the privacy benefits of this approach are clear and urgently needed.

A. A False Binary between Competition and Privacy Should be Rejected

As the CMA notes in its notice of intention document[7] (hereafter referred to as the Consultation Paper), many parties have built their business models to depend on extensive user tracking. Because this tracking is so baked into the web ecosystem, change is difficult. This ubiquity is not however a reason to codify the status quo that harms consumers and society. Rather, it is a reason

---

[3] Firefox Now Offers a More Private Browsing Experience, Nick Nguyen, Mozilla Blog. (3 November 2015). Available at: https://blog.mozilla.org/en/products/firefox/firefox-now-offers-a-more-private-browsing-experience/

[4] Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise, Dave Camp, Mozilla Blog. (4 June 2019). Available at: https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[5] Englehardt, Steven, and Arvind Narayanan. "Online tracking: A 1-million-site measurement and analysis." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. Available at: https://webtransparency.cs.princeton.edu/webcensus/

[6] StatCounter, Browser Market Share in the United Kingdom (June 2020 - June 2021) https://gs.statcounter.com/browser-market-share/all/united-kingdom&sa=D&source=editors&ust=1625590279285000&usg=AOvVaw0SlaDdjq-qoc-ujrAmex9U

[7] Notice of intention to accept commitments offered by Google in relation to its Privacy Sandbox Proposals (Case number 50972), Competition Markets Authority. Available at: https://assets.publishing.service.gov.uk/media/60c21e54d3bf7f4bcc0652cd/Notice_of_intention_to_accept_binding_commitments_offered_by_Google_publication.pdf

to move away from that status quo to find and deploy better technology that continues to offer commercial value but with better privacy and security properties.

Many third-party advertising companies that depend on ubiquitous user tracking would take the opposite approach and seek to protect the current system of flawed technology, including defending the use of third party cookies for tracking users across the web with insufficient informed consent. To that extent, we believe that some criticism of Chrome's Privacy Sandbox initiative is a red herring to take advantage of legitimate competition and privacy concerns in order to forestall long overdue privacy improvements to the internet.

We hope the CMA rejects the false choice between a more competitive or a more privacy-preserving internet. Consumer welfare is at the heart of *both* competition and privacy enforcement. First, solving only for competition in the short run at the behest of outdated internet technology with poor privacy and security properties leaves consumers and society unprotected, while actively exposing it to harm. It also stalls the development of newer and better technologies which cannot happen overnight but will require a long period of collaboration by multiple parties prior to being ready for deployment. Second, the underlying competition issues here are a result of concentrated market power across several key spaces; they can be addressed through existing competition remedies that do not hinge on freezing the evolution of internet technologies that would empower consumers with better privacy and security.

B. Structural Solutions Should be Used to Limit First Party Data Use

The most dominant technology companies today are also the largest third-party trackers on the internet. These companies stand to lose from the removal of tracking mechanisms from mobile and desktop platforms. This is best evidenced by Facebook's aggressive campaign against Apple's App Tracking Transparency initiative,[8] which gives consumers more control to block tracking identifiers on iOS devices to prevent cross-app and web tracking.

At the same time, as demonstrated by the CMA's extensive investigations into the advertising market,[9] the same companies also enjoy extensive first party relationships with consumers. Those first party relationships could allow these dominant platforms to adapt to a world without third-party cookies more easily or to leverage first-party data to power display advertising on third-party sites even more extensively than they already do. Consumers often do not understand how their data is used and leveraged across large platforms or how to make switches. This could further lock in users, websites, and advertisers into the walled garden ecosystems of such platforms.

[8] Facebook and Apple Are Beefing Over the Future of the Internet, Gilad Edelman, Wired. (29 January 2021). Available at: https://www.wired.com/story/facebook-apple-feud-over-privacy-internet-future/

[9] Final Report on the Online Platforms and Digital Advertising Study, Competition Markets Authority, United Kingdom. (1 July 2020) Available at: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

We believe the CMA and ICO can tackle this competition and privacy problem directly through targeted interventions governing how data can be shared and used within the holding structures of large platforms. This leverages classic competition remedies and is far better than using regulatory authority to prop up an outdated and harmful tracking technology like third party cookies. To this end, we strongly support Google's Commitments to foreclose the use of data from Android, Chrome browsing history and sync data, Google Analytics, and Customer Matching for targeting after implementation of Chrome Privacy Sandbox proposals. This is a positive direction for the evolution of a more private and secure internet that will benefit consumers around the world. Indeed, this particular commitment is something all dominant platforms should embrace and start practicing immediately, beyond just advertising or browser technologies, to ensure a fairer and more interoperable internet for both consumers and companies apart from the largest platforms.

Because browser sync data provides a holistic portrait of users' activity online, Google's specific commitment not to use this data for targeting third-party inventory or its own inventor represents a significant step forward both for consumers and for competition. We believe that other large online platforms should emulate such a move and limit the potential for intra-group data sharing across product or service verticals to be used for targeted advertising.

Laws like the Digital Markets Act (DMA), being considered in the European Union, also contain similar provisions that place such limitations on certain kinds of intra group data sharing.[10] We encourage the CMA to consider enshrining such restrictions in law for dominant platforms. Until that occurs, we encourage the CMA to use targeted competition interventions, such as those in these Commitments, as the cornerstone of its efforts to create a more competitive market while ensuring that consumer privacy is protected and not weakened.

IV. The Commitments Should Require Engagement through Formal Open Standards Processes & Timelines

The Chrome Privacy Sandbox proposals have the potential to have a wide-ranging impact on the internet over the coming years. Although they show promise, there remain many technical issues, including substantial privacy concerns. For this reason, we believe it is extremely important that the final Commitments explicitly require the relevant sub-components of the Chrome Privacy Sandbox proposals to both be developed via the formal processes and oversight of applicable Standards Development Organizations (SDOs) *and* deployed pursuant to agreed upon timelines in such SDOs.

[10] Opinion 2/2021 on the Proposal for a Digital Markets Act, European Data Protection Supervisor. (10 February 2021) Available at: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf

A. Standards Underpin a Decentralized & Interoperable Internet

Many of the underlying standards that form the bedrock of today's internet have been transparently debated and collaboratively developed at SDOs by relevant stakeholders through formal processes. For example, Transport Layer Security (TLS) is a foundational security protocol that was developed at the Internet Engineering Task Force (IETF). Cascading Style Sheets (CSS) is a cornerstone technology to develop webpages and was developed at the World Wide Web Consortium (W3C).

These seminal standards were not developed overnight or by a single company; rather, multiple stakeholders, including different browsers and browser engines, worked collaboratively and transparently over years in open SDOs. This approach, sometimes colloquially referred to as "rough consensus and running code"[11] prioritises real world deployment and validation and helps ensure critical technologies for the internet also serve the collective interest. This also allows third party vendors (service providers) and browsers to operate across diverse offerings of the same or similar services, and create consistently clear experience expectations for consumers, which is especially vital for online advertising.

Mozilla has always believed that a vibrant and open internet depends on fair conditions, open standards, and opportunities for a diversity of market participants to participate. We have substantial experience contributing to open SDOs over the last two decades, having played a key role in the development and implementation of critical standards such as TLS 1.3 and HTTP/3 as well as industry wide initiatives like Let's Encrypt. It is through open standards that we believe the internet can remain decentralized, open, and interoperable.

B. Commitment to Final Standards, Deployment & Timelines by Influential Stakeholders is Necessary for Effective Competition

Global standards development is a voluntary consensus-driven process. For this reason, **stakeholder commitment to final specifications and deployment on specific timelines is especially relevant for competition**. The commitment and deployment, particularly by large stakeholders, is necessary to materialize theory developed in SDOs into practical applications used widely across products in a particular industry. Markets can be distorted, and consumers impacted, either due to the absence of commitment to the final standard itself *and/or* not respecting the agreed upon timelines to deploy or deprecate relevant technologies. An example of this is the implementation of WebRTC in browsers,[12] where premature deployment of a non-standard interface in Chromium resulted in over half a decade of compatibility problems between websites and other browsers.

---

[11] "On Consensus", RFC 7282, IETF. Available at: https://datatracker.ietf.org/doc/html/rfc7282

[12] What is Unified Plan and How Will it Affect your WebRTC Development?, Callstats.io. (10 January 2019) https://www.callstats.io/blog/what-is-unified-plan-and-how-will-it-affect-your-webrtc-development

A related issue is **preventing unilateral implementation of critical technologies by stakeholders without SDO collaboration**. As the CMA has already noted based on comments received by third parties,[13] implementation of web features by dominant browsers often leads to them becoming de facto web standards, often well before the relevant SDO has formally adopted the underlying standard itself. This could put many of the Chrome Privacy Sandbox proposals at risk of becoming de facto industry benchmarks merely via their unilateral implementation by a few players, leaving publishers and other browsers without choice or say in the matter. Taking the relevant standards to the appropriate formal SDOs, on the other hand, will help ensure that their properties are validated rigorously while also allowing for relevant public visibility and engagement to stakeholders via open processes. It will also allow for other browsers to play the appropriate role in the development of standards themselves. Importantly, if their intent to improve the privacy properties of online advertising is successfully validated, these technologies will likely require implementation in browser engines beyond Blink (which is part of the Chromium open source project, on which several browsers are based) to have lasting impact.

Development at open SDOs would also address competition concerns raised to the CMA surrounding the difficulty in independently evaluating the effectiveness of the Chrome Privacy Sandbox proposals and the process of incorporating feedback from market participants.[14] The standards development processes at SDOs have been honed over the past three decades to specifically account for the reality of testing and iterating upon complex technologies with a wide diverse range of stakeholders. These processes and the inherent flexibility (balanced with SDO oversight through formal working groups) will radically improve the visibility of the development of these proposals.

C. Recommendations for Chrome Privacy Sandbox Proposals

We believe there is a role for regulatory agencies to engage with these proposals in a balanced way—that cultivates competition—but does not disrupt existing SDO processes and technical development processes which are necessary to improve the internet.

We encourage the CMA and Google to update the final Commitments to require development of these proposals at SDOs, which is where critical elements of online infrastructure have, and should continue, to be developed. At the W3C, early discussions often occur in informal forums such as business and community groups to gather meaningful input and feedback. Sufficiently mature proposals are then formally developed in Working Groups. The table below shows how this might work across the different Chrome Privacy Sandbox proposals. The rationale for

[13] Notice of intention to accept commitments offered by Google in relation to its Privacy Sandbox Proposals (Case number 50972), Competition Markets Authority. (Para 4.24, Page 20) Available at: https://assets.publishing.service.gov.uk/media/60c21e54d3bf7f4bcc0652cd/Notice_of_intention_to_accept_binding_commitments_offered_by_Google_publication.pdf

[14] *Same as Footnote 13*

development before the W3C is that it has ownership over browsers and their interface with web sites whereas the IETF has ownership over the development of networking components.

Chrome Privacy Sandbox Proposals	**Relevant SDO for development**
FLoC	W3C
FLEDGE	
Attribution Reporting	
WebID	
SameSites Cookies and First Party Cookie Sets	IETF and W3C
Trust Tokens	
Gnatcatcher (Wilful IP and Near Path NAT)	IETF

Competition and consumers would further benefit if the final Commitments included an express reference to deploy technologies pursuant to both the agreed-upon final specifications *and* the specific timelines that stakeholders arrive at in a consensus driven manner. SDOs are the natural place for voluntary and collaborative technology development amongst multiple stakeholders. However, neither SDOs nor anyone else should *require* an influential stakeholder to adopt the resulting agreed-upon final standard or deploy it and/or deprecate old technology on specific timelines. In other words, regulatory oversight is not needed in the technology development space, but enforceable voluntary measures (such as in this case) would be helpful in ensuring that influential market stakeholders do not distort competition by making deployment decisions that contravene final standards and timelines agreed upon in an SDO setting.

V. Conclusion

As we have stated before,[15] there is a real opportunity now to improve the privacy properties of online advertising by drawing upon the internet's founding principles of transparency, public participation, and innovation to make progress. We strongly believe that the best way to maximise the chances of this occurring is for the Chrome Privacy Sandbox proposals to be developed at open SDOs and urge the CMA to ensure this is reflected in the final Commitments in this investigation. We also encourage the CMA to consider the safety implications to consumers globally if Google cannot limit cookie-based tracking in Chrome. We hope the final Commitments are amended accordingly to balance *both* privacy and competition.

[15] Building a more privacy preserving ads-based ecosystem, Mozilla Blog. (28 May 2021) Available at: https://blog.mozilla.org/en/mozilla/building-a-more-privacy-preserving-ads-based-ecosystem/