Appendix 2: The CMA's assessment of other responses to the First Consultation

Introduction

1. This appendix set outs a summary of responses to the First Consultation that were not covered in Chapter 4 of this Decision, and the CMA's assessment of these responses.[1] For the responses listed in this appendix, the CMA's provisional views were that no, or only very limited, changes to the commitments were required in order to address its concerns.

Consultation responses

Introduction (Section A of the commitments)

First-party data

2. One respondent to the First Consultation (an industry association) was concerned that references to Google's aims in Section A of the Initial Commitments seemed to suggest that first-party data was more secure than third-party data, and give 'carte blanche' for the use of first party data while neglecting the privacy risks associated with it.

3. The CMA recognises that there are privacy impacts which can arise from the use of first-party data as well as third-party data. However, the CMA's provisional view was that no modification was required to Section A of the Initial Commitments to address this concern. Following the Second Consultation, this remains the CMA's view. The CMA notes that the text at issue (paragraph 2 of the Initial Commitments) was removed as a result of addressing some related concerns (as outlined at paragraphs 4.18 to 4.20 of this Decision. The CMA considers that the text within paragraph 2 of the Initial Commitments did not indicate that first-party data is more secure than third-party data, nor did it suggest (implicitly or explicitly) that compliance with data protection legislation is any less important for those responsible for first-party data. The CMA also considers that the text of the Final Commitments contains no such indication or suggestion.

[1] Consultation responses which are relevant to modifications made since the First Consultation are summarised in Chapter 4 of this Decision. All consultation responses in relation to Section J of the commitments were summarised in Chapter 4 of this Decision, so no consultation responses in relation to Section J are summarised in this Appendix 2.

Definitions (Section B of the commitments)

Other definitions

4. While some respondents to the First Consultation (an industry association, an ad tech provider and a publisher) suggested that the Initial Commitments should include additional or modified defined terms, the commitments have not been amended as a result. These representations are detailed below, in alphabetical order of the related definitions.

5. Additional definitions of '**Accelerated Mobile Pages**' or '**AMP**' were suggested during the First Consultation. The CMA's provisional view was that these definitions are not necessary, as Accelerated Mobile Pages were not part of the Privacy Sandbox Proposals, and therefore not within the scope of this investigation. The scope of this investigation has not changed since, and the CMA's view on this point remains the same following the Second Consultation.

6. '**Advertising Solutions**' was an additional term suggested in connection with proposed revisions to paragraphs 23 and 24 of the Initial Commitments. The CMA provisionally considered that all these suggestions are covered by the definition of 'Ads Systems' added since the First Consultation (see paragraphs 4.60 and 4.66 of this Decision). This remains the CMA's view following the Second Consultation.

7. The term '**B2B**' was proposed by one respondent (an industry association) to distinguish, within one part of the Initial Commitments, between 'business to business' advertising services and 'business to consumer' advertising services.[2] The definition was proposed partly on the basis of a view that business to business use cases rarely raise privacy issues. However, in particular since it cannot be excluded that privacy issues may arise in that context, the CMA's provisional view was that this additional definition is not necessary or appropriate. Following the Second Consultation, this remains the CMA's view, for the same reason.

8. '**Competitive Constraint**', '**Discrimination**' and '**Disintermediation**': these additional terms were suggested by one respondent (an industry association) in connection with other proposed revisions to paragraphs 9, 11, 16 and/or 26 of the Initial Commitments. The CMA provisionally considered, and following the Second Consultation the CMA continues to consider, that these additional definitions would be overly specific.

9. One respondent (an industry association) suggested a '**Competing**

[2] The proposed definition itself cross-referred to another proposed definition, namely '**Substitute Product**'.

Functionality' defined term in connection with other proposed revisions to paragraphs 8, 9, 11, 16, and 18 and 19 of the Initial Commitments,[3] aimed at capturing technologies which the Privacy Sandbox Proposal may affect, impair or replace.[4] The CMA provisionally considered that the substantive point relevant to this term and its related suggestions was addressed by Google having amended the definition of 'Privacy Sandbox' since the First Consultation (see paragraphs 4.28, 4.33.a. and 4.44 of this Decision). Following the Second Consultation, that definition has not been amended further, and the CMA's view remains that the defined term proposed is not needed.

10. One respondent (an industry association) suggested several additional terms in connection with the idea that under the commitments Google should allow interoperability of Google's data with competitors. For example, '**Equivalence of Input**' was suggested in connection with an idea that Google should allow competitors to access data on fair, reasonable and non-discriminatory terms. '**Lawful Data**' was another term suggested in this context (and in connection with other proposed additional terms, namely '**Mechanism for Lawful Data Sharing**' and '**Mechanism**'). Since the respondent's proposed additions may pre-empt the outcome of the envisaged dialogue with Google and the envisaged consideration by the ICO under the commitments, the CMA's provisional view was that it is not appropriate to add such definitions. For the same reason, this remains the CMA's view, following the Second Consultation.

11. '**Impacted Organisations**': This additional term was suggested in connection with other proposed revisions to paragraphs 16 and 29 of the Initial Commitments, all apparently aimed at increasing third parties' role in consultation with Google, and testing, before implementation of the Privacy Sandbox. The CMA provisionally considered that the substance related to those suggestions was addressed within what are paragraphs 4.117 to 4.192 of this Decision, in the context of Section D and Section E of the commitments.

12. One respondent (an industry association) suggested that testing under paragraph 16 of the Initial Commitments should include ensuring a lack of threats to '**Long Term Innovation**' (a proposed new defined term) on the part

[3] The term '**Competing Providers**' was another addition suggested, in relation to similar proposed revisions. The CMA's provisional view was that there was no need to define this term in the Initial Commitments, not least as the phrase 'other market participants' (used within the Initial Commitments, and within the Modified Commitments) appeared to encompass those intended to fall within the meaning of 'Competing Providers'. Following the Second Consultation, this remains the CMA's view.

[4] The term '**Substitute Product**' was also suggested in connection with similar proposed revisions. This proposed definition appeared to resemble the concept of 'Alternative Technologies'. For this reason, and because the substance related to this term was addressed in the context of Section E of the commitments (for further details, see paragraphs 4.155–4.192 of this Decision), the CMA provisionally considered that this addition is unnecessary. On the same basis, this remains the CMA's view following the Second Consultation.

of Google's competitors. The CMA's provisional views on what should be covered by testing were set out in the November Notice, at the counterpart of what are now paragraphs 4.171 to 4.184 of this Decision, in the context of Section E of the commitments. The CMA's views, following the Second Consultation, on what should be covered by testing are set out in those aforementioned paragraphs.

13. One respondent (an industry association) submitted that certain additions should be made to the terms '**Monitoring Statement**' and '**Compliance Statement**' within the Initial Commitments. The main effect of these additions, suggested in connection with certain proposed revisions to paragraph 16 and/or paragraph 27 of the Initial Commitments, appeared to be to specify further the seniority and knowledge required in order to sign these statements. The CMA provisionally considered it unnecessary to include such detail – in particular, in light of changes made to Section I of the commitments (on which, an updated summary is now set out at paragraphs 4.330 to 4.384 of this Decision). Given those changes, following the Second Consultation the CMA considers it unnecessary to include such detail.

14. One respondent (an industry association) suggested including the additional term '**NIAC**', to refer to the June Notice. The aim was to help avoid repetition, if the commitments were to cross-refer at multiple places to the June Notice. However, the Initial Commitments did not contain any such cross-references, and the Final Commitments do not contain them either. Following the Second Consultation, the CMA considers such cross-references unnecessary.

15. '**Notice**', '**Notification**' and '**Notify**' were additional, related terms suggested by one respondent (an industry association). The CMA's provisional view was that there was no need to define these words, and that they should be interpreted according to their natural ordinary meaning and the context in which they appear. This remains the CMA's view, following the Second Consultation.

16. '**Privacy**': one respondent (an industry association) suggested that Google's actions should be measured against a definition of privacy centred on the appropriate flow of information. This respondent submitted that this would mean ensuring that data about a user is collected and used only in ways that align with that user's expectations, a principle embodied in various pieces of data protection and regulatory legislation (eg the GDPR). Similarly, two respondents (an industry association and a media agency) suggested an additional term such as 'Privacy' or '**Privacy Concern**'. The suggestion was that the existence of a 'Privacy Concern' should only be accepted on the basis of evidence, and only substantiated 'Privacy Concerns' should be addressed, as agreed with the CMA and the ICO. The aim of this suggestion appeared to be preventing

Google from defining or interpreting privacy in a self-serving way, and preventing Google from using data protection arguments to frustrate competition. The CMA's provisional view was that it is important that the CMA and the ICO are involved in ensuring that the Privacy Sandbox is developed taking into account, for example, impact on privacy outcomes and compliance with applicable data protection legislation. However, these additional definitions appeared unnecessary, in light of the commitments being amended to also refer to 'Personal Data' and 'Applicable Data Protection Legislation' (as now set out at paragraphs 4.31, 4.33.d. and 4.51 of this Decision). In light of those amendments, and the use within the Final Commitments of 'Personal Data' and 'Applicable Data Protection Legislation', the CMA's view following the Second Consultation is that these proposed additional definitions are unnecessary.

17. '**Pseudonymised Data**': This was suggested because the definition of 'Individual-level User Data' in the Initial Commitments referred to 'pseudonymised data', which was not itself defined. However, adding such a defined term – like various other terms which were suggested within certain consultation responses[5] – appeared unnecessary to the CMA. The commitments no longer refer to 'pseudonymised data'. Moreover, the commitments were amended so that all references to 'Individual-level User Data' now refer to 'Personal Data', a term which is itself defined by reference to 'Applicable Data Protection Legislation' (see paragraphs 4.31, 4.33.d. and 4.51 of this Decision). Following the Second Consultation, the CMA considers that this proposed additional definition is not necessary.

18. One respondent suggested because revising the definition of '**Third-Party Cookies**' in the Initial Commitments – mainly on the basis that it arguably included all cookies, such that the true removal of TPCs could arguably not be caught by the standstill obligation. The CMA provisionally considered there to be no material risk of the term being understood in the way suggested by this respondent. Following the Second Consultation, the CMA's view remains the same.

19. The term '**User Agent Client String**' was suggested in connection with proposed revisions to paragraph 11 of the Initial Commitments. The CMA's provisional view was that 'user-agent string' needed no definition, as it is a generally understood term in the context. Moreover, the CMA considers that the proposed definition appeared to conflate the user-agent string (which is to be reduced, under the 'User-Agent Reduction' Privacy Sandbox Proposals) and User-Agent Client Hints (which is to be introduced, under the Privacy Sandbox Proposals). The CMA considers, following the Second Consultation, no

[5] For example, '**Identifiable Living Individual**', '**Identity**' and '**Re-identification**'.

additional definition to be necessary.

20. One respondent (an ad tech provider) submitted that it was not clear what '**user-facing services, including Android**' in paragraph 23 of the Initial Commitments was meant to cover. This was based on an assumption that 'Android' refers to the Android operating system which, strictly speaking, is not always a user-facing service. The CMA provisionally considered that the substance relevant to this suggestion is addressed in the context of Section G of the commitments. In any event, the relevant phrase has been replaced – as part of the 'Google First-Party Personal Data' defined term added since the First Consultation – with the following, clearer phrase: 'Google's services available on the Android operating system as deployed in smartphones, connected televisions or other smart devices'.

Purpose of the Commitments (Section C of the commitments)

Submissions regarding the framework for the Development and Implementation Criteria

21. Five respondents (three industry associations, an ad tech provider and a publisher) to the First Consultation queried if it sufficed for Google to commit only to 'taking into account' factors such as the 'Development and Implementation Criteria' listed in the Initial Commitments.

22. Four respondents (two industry associations, an ad tech provider and a media agency) queried whether the Initial Commitments should explain how the 'Development and Implementation Criteria' would be measured or weighted – or how practicable such measurement/weighting would be.

23. The CMA's provisional view was that the commitments need not be amended in the ways suggested in these representations. Any future assessment of whether Google has taken the relevant criteria sufficiently into account should involve the CMA exercising its discretion fully and freely. Indeed, some respondents to the First Consultation supported the idea of the CMA doing exactly that, following an approach based on general principles. On the same basis, following the Second Consultation the CMA's view is that the commitments need not be amended in the ways suggested in the representations summarised above.

Suggestions for additional or amended Development and Implementation Criteria

24. Several respondents suggested adding to the Development and Implementation

Criteria.[6] For example, four respondents (three ad tech providers and a browser) suggested that the commitments should also oblige Google to assess, or not impede, rivals' alternative proposals and solutions (for example, rival advertiser software and services).[7]

25. The CMA considered these representations, together with others relating to other parties' alternative proposals and solutions. In light of the amendments made to the commitments since the First Consultation which are detailed below, the CMA's provisional view was (and, following the Second Consultation is) that the commitments need not be amended further to address those representations.

    (a) Under the commitments, Google will take into consideration reasonable views and suggestions, including on testing, which are expressed to Google by publishers, advertisers and ad tech providers in relation to each of the Privacy Sandbox Proposals.[8]

    (b) In relation to not impeding other parties' alternative technologies, the commitments now include an additional commitment by Google which, in the CMA's provisional view, provided greater certainty for third parties developing such technologies.[9]

Transparency and consultation with third parties (Section D of the commitments)

Public statements by Google

26. One respondent to the First Consultation (a publisher) considered that the reference to 'substantial transparency' in the first paragraph of Section D of the commitments may not be sufficiently precise or reflective of applicable data protection law. Another submission (from certain academics) contained a suggestion that transparency and control do not lead to informed privacy choices for users and that this is a fundamental limitation with the 'self-management' approach to privacy.

---

[6] One respondent (an industry association) suggested developing a fuller framework of principles, to which Google must adhere (for example, the principle that Chrome should provide consumers with simple and easy control over tracking).

[7] Some other respondents made similar submissions, albeit in the context of testing (on which, see paragraph 36 of this Appendix 2) or more broadly.

[8] Paragraphs 12 and 17.c.ii. of the Final Commitments (mirroring the same paragraph numbers in the Modified Commitments), Google will also provide quarterly reports to the CMA explaining substantively how Google has taken into account representations by third parties: paragraph 32.a. of the Final Commitments (and paragraph 32.a. in the Modified Commitments). See also eg paragraphs 4.134.b., 4.143 and 4.156.b. of this Decision.

[9] Paragraph 31 of the Final Commitments (and paragraph 31 of the Modified Commitments). See also paragraphs 4.312 to 4.329 of this Decision.

27. The CMA's provisional view was that no modification to the Initial Commitments was needed to address these concerns. Those commitments already provided for the involvement of the CMA and the ICO with a view to ensuring that the Privacy Sandbox Proposals develop in the appropriate way, and in line with the Development and Implementation Criteria, in relation to user control. That remains the CMA's view, following the Second Consultation.

Involvement of the W3C

28. Various respondents made submissions about the processes of the W3C.

    (a) Three respondents (three ad tech providers) submitted that W3C currently was a forum focused on technical discussions rather than policy issues relating to competition and privacy. One respondent (an ad tech provider) submitted that the forum did not allow for sufficient discussions around privacy issues or competition concerns.

    (b) Some respondents submitted that W3C's processes were not clear to them or could be improved. For example, one respondent (an industry association) submitted that decision-making should include a pre-defined voting system (either within W3C or another industry body), which could allow publishers and ad tech providers to input and to be involved in decision-making in respect of the Privacy Sandbox Proposals. Specific recommendations suggested by another respondent (an ad tech provider) included establishing independent chairs for W3C groups relating to Privacy Sandbox Proposals.

    (c) Four respondents (four ad tech providers) suggested that the W3C's public aim of making decisions by consensus did not work in practice. One respondent (an ad tech provider) raised concerns about certain members' ability to influence the W3C 'Management Team' to 'ban' other members from directly contributing to W3C 'Technical Advisory Group' discussions.

    (d) Three respondents (two industry associations and a publisher) commented on the impact that choice of a specific 'group' within the W3C could have on both governance and decision-making in the development of Google's Privacy Sandbox Proposals. Three respondents (two industry associations and a browser) submitted that Privacy Sandbox Proposals should be developed through formal standards development processes within an open Standard Development Organisation ('**SDO**'), whether this SDO is W3C or another forum. Another respondent submitted (an ad tech provider) that any

commitments accepted in this investigation should state whether the Privacy Sandbox Proposals will become open web standards.[10]

(e) Four respondents (two industry associations and two ad tech providers) submitted that the use of W3C 'Business Groups' and W3C 'Community Groups' was not appropriate for standards development. This was on the basis that they tend to lack tangible and specific criteria for success – and the scrutiny and expertise of technical advisory groups require parties to address all submitted stakeholder concerns ahead of finalising proposals (which delays progress).[11] One respondent (a browser) noted that, although early discussions on proposals often occur in informal fora such as W3C Business Groups and Community Groups to gather 'meaningful impact and feedback', once sufficiently mature, proposals are then formally developed within W3C Working Groups.

29. The CMA understands that creating a W3C Working Group to refine proposals into recommendations requires the making of a decision by consensus among W3C members and must be initiated by W3C staff and that a W3C Director decides which initiatives can move into a W3C Working Group phase.

30. The CMA's provisional view was that the related parts of the commitments needed no modification and that any changes suggested above would not need to form any part of any commitments offered to the CMA by Google. Following the Second Consultation, that remains the CMA's view, on the following basis. The W3C is primarily a technical forum designed to exchange ideas for future standardisation, or targeted work on technical APIs aimed at developing specific standards (ratified by an Advisory Committee agreeing a W3C recommendation). The W3C is not a place intended to discuss, promote, or determine policy decisions on proposals for compliance with national (or international) data protection or competition policy. How the Privacy Sandbox Proposals are considered within the W3C is a matter ultimately for the W3C, and it is not within Google's ability to offer any commitment to ensure that W3C discussions of the Privacy Sandbox Proposals take place in a certain manner or within a certain group.[12] In addition, following amendments to the commitments since the First Consultation, Google will publish on a microsite a process dedicated to stakeholder engagement in relation to the Privacy Sandbox

[10] One respondent (a browser) suggested that the certain Privacy Sandbox Proposals should be developed within various different, specifically named, SDOs.

[11] Two respondents (an industry association and an ad tech provider) suggested that Google should craft measurable success criteria for the W3C's Improving Web Advertising Business Group, independently assess the outcomes of that W3C Business Group, and provide a forum for public comment on those outcomes.

[12] Google has confirmed to the CMA that Google intends for the Privacy Sandbox Proposals to proceed, when appropriate, to the relevant W3C Community Groups, W3C Business Groups and W3C Working Groups, according to W3C processes: see paragraph 13 of the Final Commitments (and paragraph 13 of the Modified Commitments).

Proposals, and will take into consideration reasonable views and suggestions including those expressed in the W3C.[13]

CMA involvement in W3C processes and similar fora

31. Six respondents (three industry associations, two ad tech providers and a specialist search provider) explicitly recommended direct involvement of the CMA in W3C discussions or equivalent fora. Two respondents (two industry associations) suggested that paragraph 13 of the Initial Commitments be modified, to require Google to proactively involve the CMA in discussions in W3C and other fora.[14] Two respondents (an industry association and an ad tech provider) submitted that the CMA should formally apply to join the W3C.

32. One respondent (a specialist search provider) suggested that the CMA should attend discussions and participate in SDO fora as a stakeholder, without the CMA providing ideas, concepts or technologies itself. In that respondent's view, once Google had published sufficient data about one of the Privacy Sandbox Proposals, the CMA could invite comments from stakeholders, and publish an evaluation of that proposal's impact on competition.

33. The CMA's provisional view was that the related parts of the commitments needed no modification. Any CMA decision to join the W3C would not need to form any part of any commitments offered to the CMA by Google. For the same reason, that remains the CMA's view, following the Second Consultation.

34. Other responses included a suggested additional commitment that the CMA will assess the competitive impact of, and recommend, specific alternative proposals made by third parties in the W3C Improving Web Advertising Business Group and other W3C Business Groups. The relevant respondent (an industry association) submitted that Google (and other browsers) should be required as part of this process to consider and provide specific feedback on such proposals.

35. The CMA's provisional view was that the related parts of the commitments needed no modification. That remains the CMA's view, following the Second Consultation, on the following basis. Any CMA decision on how to assess the competitive impact of proposals made by third parties would not need to form any part of any commitments offered to the CMA by Google.

[13] See footnote 8 above within this Appendix 2.

[14] One of these respondents (an industry association) suggested that Google should also commit to proactively include other market participants, regulators and associations in the respective fora.

Involvement of the CMA and the ICO (Section E of the commitments)

Testing to be undertaken under the commitments

36. Two respondents to the First Consultation (an industry association and a browser) submitted that Google's testing and trials should also assess other market participants' alternatives, and proposed alternatives, to the Privacy Sandbox Proposals.[15] Three other respondents (an industry association, a media agency and an ad tech provider) submitted, similarly, that the commitments (and the definition of 'Alternative Technologies') should aim to ensure the consideration by Google of all reasonable proposals, not just of the Privacy Sandbox Proposals.

37. The CMA was of the provisional view that it would be inappropriate to require Google to test third parties' alternative solutions to Google's Privacy Sandbox Proposals, unless these become a part of the Privacy Sandbox Proposals. Following the Second Consultation, that remains the CMA's view.

38. One respondent (an industry association) submitted that Google should test for 'equivalence of functionality', rather than 'effectiveness' (as referred to in Section E of the commitments). For example, Google should test benchmarks such as time to access data (or a proposed cohort),[16] impact on site load speed or yield optimization methods that publishers are currently running.

39. The CMA's provisional view was that effectiveness (as determined by the Development and Implementation Criteria) is the appropriate basis for assessing the impact of the Privacy Sandbox Proposals, and there should not be an additional requirement of 'equivalence'.[17] However, the CMA agrees that there may be benefits in testing benchmarks such as time to access data and site load speed as part of the overall assessment of effectiveness, and this should be factored into the design of future trials. That remains the CMA's view, following the Second Consultation.

40. One respondent (an industry association) stated that Google should also test for functionality in relation to 'Accelerated Mobile Pages' or 'AMP'. The CMA's provisional view was that Accelerated Mobile Pages were not part of the Privacy Sandbox Proposals and, therefore, not within the scope of the CMA's

[15] Submissions included the suggestion that tests of 'Alternative Technologies' should demonstrate an absence of threats to long-term innovation by other market participants, arising from conflicts of interest in any and all proposals.

[16] The reference to 'cohort' is no longer relevant: in January 2022, Google announced that it was replacing FLoC with Topics, an API that will provide interest-based topic categories. See Appendix 3 to this Decision, paragraphs 8–11.

[17] The ICO's Opinion (as referred to at footnote 9 of this Decision) sets out the data protection expectations that online advertising proposals should meet.

investigation. Therefore, the CMA provisionally considered that it is not necessary to address this submission through the commitments. The scope of this investigation has not changed since, and the CMA's view on this point remains the same following the Second Consultation.

41. One respondent (an industry association) suggested that reviews of the 'Alternative Technologies' should demonstrate an absence of threats to long-term innovation by market participants, from conflicts of interest in any and all proposals. The CMA provisionally considered that these types of long-term harms would already be captured within the second of the Development and Implementation Criteria (ie impact on competition). However, as a practical matter the CMA considers that effects on long-term innovation are unlikely to be amenable to being assessed quantitatively as part of testing under the commitments. Therefore, the CMA's provisional view was that the Initial Commitments needed no modification in this regard. This also the CMA's view, following the Second Consultation.

42. Thirteen respondents (seven ad tech providers, four industry associations, a publisher and a media agency) suggested amending who would be involved in designing, undertaking and/or evaluating tests relating to the Privacy Sandbox.

    (a) One respondent (an ad tech provider) suggested that the CMA consult with market participants on the design of tests.

    (b) Five respondents (three ad tech providers, a media agency and an industry association) suggested involving other market participants in designing tests, for example to assess whether functionality such as measurement will either still exist or have effective replacements with the Privacy Sandbox. Two respondents (a media agency and an industry association) suggested involving the ICO, or independent experts, in test design.

    (c) Eight respondents (four ad tech providers, three industry associations and a publisher) suggested that market participants (or W3C participants) should conducted and validate tests of Alternative Technologies. One respondent (a publisher) submitted that the CMA should have the option to contract with third parties to assess the effectiveness of Alternative Technologies. Five respondents (three ad tech providers and two industry associations) suggested a role in this regard for independent experts. Three respondents (two ad tech providers and an industry association) proposed that an independent auditor or another independent person audit results relating to the efficacy of the Privacy Sandbox. One respondent (an industry association) suggested that, for transparency, confidential communications between Google and the CMA should be shared with a list of agreed market participants.

43. The CMA's provisional view was that it would be inappropriate to accord third parties and/or experts any formal procedural testing role, and following the Second Consultation this broadly remains the CMA's view. Following amendments to the commitments since the First Consultation, Google will take into account third parties' reasonable views and suggestions regarding testing, and will provide substantive explanations to the CMA (as outlined in paragraph 4.156(b) of this Decision).

44. Four respondents (three industry associations and an ad tech provider) made submissions about the publicity of results from testing done in the context of developing the Privacy Sandbox Proposals.

    (a) Two respondents (an industry association and an ad tech provider) favoured a wider scope of publication obligations in relation to test results – for example, suggesting that Google publish all results (and not just 'material' ones) or all underlying data (not just a description).

    (b) Three respondents (three industry associations) suggested certain obligations for Google if it wished to publish results from tests carried out based on parameters not approved by the CMA. For example, it was submitted that Google should obtain CMA approval before publishing those results, or should at least publish those results subject to the test result publicity requirements set out in paragraph 16.c.v. of the Initial Commitments (which related to the results of tests based on approved parameters).

45. The CMA's provisional view was that the related parts of the Initial Commitments needed no modification. For example, the scope of test result publicity requirements set out in paragraph 16.c. of the Initial Commitments reflected an appropriate balance between transparency for third parties and the resources involved in publishing all test results and accompanying data. Following the Second Consultation, paragraph 16.c. of the Initial Commitments is now paragraph 17.c. of the Final Commitments; the CMA's view remains the same.

Other comments on paragraph 16 of the Initial Commitments

46. Paragraph 16.a. of the Initial Commitments set out ways for Google and the CMA to identify and resolve concerns quickly. Three respondents (two ad tech providers and an industry association) suggested deleting or defining 'material' in paragraph 16.a.i., to lower the risk of Google not informing the CMA sufficiently about changes to the Privacy Sandbox. Another respondent (an ad tech provider) expressed concern that the Initial Commitments did not provide a way to raise concerns once the Alternative Technologies were implemented.

47. The CMA's provisional view was that paragraph 16.a. of the Initial Commitments (now paragraph 17.a. of the Final Commitments) allows concerns to be raised during the period of any commitments accepted, including after the Privacy Sandbox Proposals are implemented. The CMA provisionally considered, and following the Second Consultation continues to consider, that Google updating the CMA on material changes to the Privacy Sandbox is appropriate. This is in particular in light of, for example, the dialogue and meetings provided for elsewhere in Section E (eg paragraphs 16.a. and 16.b of the Initial Commitments, now paragraphs 17.a. and 17.b. of the Final Commitments).

48. Several responses contained references to paragraph 16.d. of the Initial Commitments (now paragraph 17.d. of the Final Commitments). Three respondents (an ad tech provider, a publisher and an industry association) suggested that this should also provide for the ICO to be updated on proposals relating to user controls. The CMA's provisional view was, and following the Second Consultation the CMA's view remains, that the commitments needed no modifications in this regard. This is in light of the pre-existing acknowledgement that the CMA will involve the ICO to achieve the purpose of the commitments.[18]

49. In the context of paragraph 16.d. of the Initial Commitments, two respondents (both ad tech providers) raised a concern that without appropriate amendments to the Initial Commitments, Google could turn to its commercial advantage its bespoke dialogue with the CMA and the ICO in this matter, by later claiming that this meant that the Privacy Sandbox complied with applicable competition law and applicable data protection legislation. The CMA's provisional view was that the commitments needed no such amendments: the concerns summarised above are unfounded. It is open to any individual or business to approach the ICO with regard to data protection issues and to approach the CMA in relation to competition issues. That remains the case following the Second Consultation, and the CMA's view remains that the commitments need no such amendments.

50. Four respondents made specific submissions concerning user choice. One respondent (an industry association) submitted that the Chrome browser should return to its purpose of being a user-agent, giving consumers simple and easy control over tracking. Another respondent (an industry association) submitted that any commitments should require Google to ask users if they consent to websites using TPCs. Three respondents (three industry associations) submitted that valid user consent should be obtained for the processing of personal data. One respondent (a civil society interest group) submitted that users should be able to say no as easily as they can say yes as regards data

[18] Paragraph 18 of the Final Commitments (and paragraph 18 of the Modified Commitments).

processing, and that Google should provide a clear and easy way for users to opt out of TPCs blocking in case any user reconsiders a previous decision to opt in. As user controls including choice architecture and defaults were already explicitly within the scope of the commitments, the CMA's provisional view was that the commitments needed no modification to address these points. The scope of the commitments has not changed since. The CMA's view on this point remains the same following the Second Consultation.

Standstill Period (Section F of the commitments)

Circumstances triggering the Standstill Period

51. One First Consultation respondent (an industry association) suggested that the commitments should provide for multiple 'Standstill Periods' (eg triggered by the removal of TPCs and the removal of any other functionalities or data).

52. Two other respondents (an ad tech provider and a browser) suggested that the deprecation of TPCs should not be delayed by the CMA, given the impact on privacy outcomes. Two respondents (an ad tech provider and a publisher) suggested that the commitments should limit Google's ability to arbitrarily delay the removal of TPCs (as such delay could put at risk potential new competitors and their innovations).

53. The CMA's provisional view was that a clear trigger point was required for the Standstill Period. The deprecation of TPCs was a suitable candidate.[19] Following the Second Consultation (including consideration of the responses outlined in paragraphs 4.200 to 4.204 of this Decision), that remains the CMA's view.

54. However, the CMA did not consider that the commitments should be modified to allow for the possibility of multiple 'Standstill Periods'. Following the Second Consultation, that remains the CMA's view, on the following basis. Under paragraph 17.a.iii of the Final Commitments, where the CMA has notified Google of concerns the CMA has as regards Google's implementation of Privacy Sandbox, and these concerns remain unresolved after 20 Working Days, the CMA may continue its investigation. This applies to any aspect of Google's implementation of Privacy Sandbox, not just the Removal of TPCs. The CMA's provisional view was, therefore that the commitments already provide a means through which it may address concerns relating to the wider implementation of the Privacy Sandbox Proposals. For the same reasons, that is also the CMA's view following the Second Consultation.

[19] See the June Notice, paragraphs 6.47–6.54.

55. The CMA was provisionally satisfied that the Modified Commitments covered the key substantive concerns expressed by consultation respondents about Google removing other functionality or data pre-Standstill Period. That remains the CMA's view, following the Second Consultation (and consideration of the responses to it, as referred to above). The amendments to the commitments since the First Consultation which are outlined at paragraphs 4.199 and 4.211 of this Decision address consultation respondents' specific concerns about the pre-Standstill Period removal of information available via the user-agent string, and/or losing support for the key other non-advertising use cases for IP addresses which were cited as important by consultation respondents.

Pre-requisites for start of the Standstill Period

56. Several respondents to the First Consultation raised concerns that Google could trigger the Standstill Period in the commitments unilaterally, so suggested adding further conditions to be fulfilled before the standstill commenced.

57. Five respondents (two industry associations, an ad tech provider, a publisher and a media agency) suggested that the Standstill Period should only be triggered after appropriate market tests have proven that the Alternative Technologies are adequate, after certain success criteria (which Google should set out) are met, or after the CMA has approved a final version of the Alternative Technologies.

58. Two respondents (both ad tech providers) made related suggestions. One of these respondents suggested that there should be sufficient adoption of Alternative Technologies across the market before Google could implement the removal of TPCs. The other respondent suggested that Google should conduct 'in market' testing for six months before undertaking any fuller roll-out.

59. The CMA's provisional view was that the commitments needed not be modified to include further steps before the Standstill Period can be triggered – and, as noted above, that a clear trigger point is required for the Standstill Period. In addition, the Standstill Period is, in and of itself, an appropriate means to assess at a future point whether the CMA has remaining competition concerns and whether they have been resolved. On the same basis, following the Second Consultation the CMA has reached the same view.

60. One respondent (an industry association) suggested that any commitments should require Google to provide broad, public notice of the Standstill Period.

61. The CMA's provisional view was that the commitments did not need to be modified in this regard. That remains the CMA's view, following the Second Consultation, on the following basis. The commitments already provide for

Google to publicly disclose the timing of the key Privacy Sandbox Proposals, and to update that information as timings change or become more certain.[20] Even in the absence of those provisions, it would be open to the CMA to publicise the commencement of the Standstill Period.

Length of the Standstill Period

62. Five respondents (two industry associations, two ad tech providers and a media agency) suggested that the periods specified in paragraph 18 of the Initial Commitments (ie an initial Standstill Period of 60 days, which can be increased by a further 60 days at the CMA's request) needed to be longer.

63. Four respondents (two industry associations and two ad tech providers) suggested that the minimum Standstill Period should be increased to 120 days; one respondent (an industry association) also suggested adding the option for an extension of 60 days or 120 days. Another respondent (a media agency) suggested that a minimum 180-day period would be appropriate. The reasons cited for these proposals were to give the industry sufficient time to adapt, and to give the CMA sufficient time to analyse the impact of the deprecation of TPCs.

64. The CMA provisionally considered that the length of the Standstill Period required no modification. Following the Second Consultation, that is still the CMA's view, for the following reasons. Under paragraph 18 of the Initial Commitments (now paragraph 19 of the Final Commitments), Google will at the CMA's request increase the Standstill Period to a total of 120 days. The CMA intends to engage closely with Google and industry stakeholders throughout the process, including undertaking a further public consultation. The CMA does not consider that it would require additional time to analyse and consult during the Standstill Period. Further, extending the Standstill Period may delay the implementation of potentially beneficial new technologies.[21]

Ability to re-start or extend the Standstill Period

65. One respondent (an industry association) suggested that the CMA should be able to re-start the periods specified in paragraph 18 of the Initial Commitments in case of a lack of information, or misleading information, from Google.

66. One respondent (an industry association) suggested that there should be fewer possibilities for Google to extend the Standstill Period.

[20] Paragraph 12 of the Initial Commitments (and now paragraph 11 of the Final Commitments).

[21] Various consultation respondents cited these potential benefits: see eg paragraph 52 of this Appendix 2.

67. The CMA provisionally considered that the commitments did not require modification in this regard. That is still the CMA's view, following the Second Consultation. Google is unlikely to have an incentive to extend the Standstill Period, which is now set out in paragraph 19 of the Final Commitments, for longer than necessary. The provision of false or misleading information to the CMA is a criminal offence under section 44 of the Act, attracting criminal penalties. Pursuant to section 31B(4) of the Act, the CMA has distinct powers to continue an investigation if incomplete, false or misleading information led the CMA to accept commitments under the Act.

Other comments in relation to Section F of the commitments

68. One respondent (an industry association) suggested adding some text, to clarify the relationship with section 31B(4) of the Act, to Section F of the commitments.

69. The CMA's provisional view was that the commitments needed no such addition. This was because the commitments already include sufficient information on this relationship. Following the Second Consultation, this remains the CMA's view.

Google's use of data (Section G of the commitments)

Purposes/uses of data

70. With regard to not using publisher data for any purposes other than those explicitly requested by the publisher, one respondent to the First Consultation (an ad tech provider) gave an example of a user looking at content on a publisher's site who has Google Ad Manager or Google Analytics installed. That information might be used to recommend to the user related videos on YouTube, which indirectly leads to a related ad being served to them. The CMA's provisional view was that the scope of the CMA's investigation, and of the competition concerns identified by the CMA during its investigation (as summarised in the June Notice), did not cover Google's use of data to provide its user-facing services and personalise non-ad content on these services. The scope of this investigation has not changed since, and the CMA's view on this point remains the same following the Second Consultation.

71. With respect to Google's use of Analytics customers' data, the CMA's provisional view was that this is addressed by Google's clearer commitment, since the First Consultation, not to use 'Personal Data' provided by Analytics customers to track users for the Targeting or Measurement of digital advertising on either Google owned and operated inventory or ad inventory on websites not owned and operated by Google. This is subject to allowing each Google

Analytics customer to share or export its own Analytics data, including through a linked Google Ads account, for ads targeting and/or measurement. This commitment is reflected in the Final Commitments.[22] Following the Second Consultation the CMA's view on this point remains the same.

72. One respondent (a publisher) submitted that publishers should not be forced to share data with Google. One respondent (an industry association) suggested that Google should commit to using data only for the customer or user's service request, and that any additional use should require an opt-in.

73. The CMA notes that publishers enter into an agreement with Google when they use Google Ad Manager. Under that agreement, publishers allow Google to retain and use all the data that they provide, including to aggregate the data provided by other publishers. The terms of such agreements are not formally a part of the Privacy Sandbox Proposals.

74. One respondent (a publisher) suggested that Google should be prevented from using synced Chrome data for any purpose other than the sync service.

75. On synced Chrome data, the CMA's provisional view was that following amendments to the commitments since the First Consultation Google is prevented from using Personal Data from a user's Chrome browsing history (including synced Chrome history) in its Ads Systems to track that user for the Targeting or Measurement of digital advertising, and it is not necessary to further restrict Google's use of this data (for instance, to prevent spam and fraud or improving Chrome security). The CMA's view on this point remains the same, following the Second Consultation, given Section G of the Final Commitments.

76. Two respondents (a publisher and an industry association) queried whether the restriction to use certain data in Google's Ads Systems should be removed, broadening it to include more systems. Similarly, one respondent (a comparison shopping service) suggested that, at least for certain sources (namely a user's Chrome browsing history and a publisher's Google Analytics account), Google should be prohibited from using this data for any other purposes. One respondent (a publisher) suggested that Google should commit to not using any Chrome-sourced data for any purpose other than delivering a synchronisation service to the user, while another response on behalf of a publisher contained a suggestion to the same end but also allowing use for the purpose of improving Chrome and security.

77. The CMA's provisional view was that broadening the scope beyond ads

[22] Final Commitments, paragraph 26 and footnote 4.

systems would be beyond the scope of the CMA's investigation and of the competition concerns identified by the CMA during its investigation (as summarised in the June Notice). The investigation's scope has not changed, and neither has the CMA's view on this point following the Second Consultation.

78. One respondent (an ad tech provider) submitted that even Google's ability to use data for the purposes of preventing spam and fraud should be restricted. The CMA's provisional view was – and, following the Second Consultation, the CMA's view remains – that it is unnecessary and inappropriate to restrict Google's ability to use data for the purposes of preventing spam and fraud.

79. Additionally, one respondent (a publisher) considered that paragraphs 23 and 24 of the Initial Commitments should not be limited to 'on the web', and should cover the use of data across contexts such as on mobile phones. In this respondent's view, the Initial Commitments would not preclude Google from processing information on-device, including contextual signals, and using such insights to enhance its offerings. Another respondent (an ad tech provider) submitted that paragraph 23 of the Initial Commitments should be amended to specify each device use.

80. The CMA's provisional view was that the Privacy Sandbox changes will not have a direct, material impact on competition in the market for advertising on mobile apps, given that mobile advertising identifiers on Android devices are not affected by the Privacy Sandbox Proposals. On that basis, the commitments did not need to cover advertising activities on mobile apps as well as on the web. Also, following amendments to the commitments since the First Consultation, Google is prevented from using Personal Data from Google's services on the Android operating system as deployed in smartphones, connected televisions or other smart devices to track users to target or measure digital advertising on non-Google web inventory, and this is not limited to situations where the Personal Data is processed on-device. For the above reasons, following the Second Consultation the CMA's views on this point remain the same.

Data sources or services

81. On the theme of which exact data sources or services should be covered for paragraphs 23 and 24 of the Initial Commitments, many respondents submitted additions were warranted. These included:

    (a) ad servers;

    (b) DV360;

(c) Google Analytics non-publisher accounts and other analytics services such as Firebase;

(d) consumer-facing software and business-facing software involved in controlling publisher auctions; and

(e) with respect to paragraph 24 of the Initial Commitments specifically:

(i) Customer Match;

(ii) Google's current and future technology or current and future user-facing services;

(iii) Google Search and YouTube;

(iv) Android; and

(v) any Personal Data collected from rival publishers or rival ad solutions.

82. Eleven respondents (four publishers, three industry associations, two ad tech providers, an advertiser and a civil society interest group) raised concerns about the effectiveness of commitments specifying a list of data sources that Google commits not to use.

(a) Six respondents (four publishers and two industry associations) suggested that paragraphs 23 and 24 of the Initial Commitments should be reviewed with a view to securing principles-based commitments. This reflected in part the concern that the inclusion of specific prohibitions on using the data in paragraphs 23 and 24 was inconsistent with the principles-based approach adopted in the rest of the Initial Commitments and risked giving the impression that these provisions alone were sufficient to address competition and data protection concerns in relation to the Privacy Sandbox.

(b) One respondent submitted (an industry association) that Google should by default not use data which Google collects from one of its services for the purpose of targeting or measuring digital advertising shown on another service, unless the user has proactively granted free, informed, and explicit consent, consistent with the purpose limitation principle and other requirements under the applicable data protection legislation.

(c) Two respondents (both ad tech providers) commented on future services offered by Google not falling within the restrictions in Section G and the need for flexibility to revisit the commitments.

(d) Four respondents (two industry associations, an advertiser and a civil society interest group) suggested that the method for determining which data

Google is permitted to use under paragraphs 23 and 24 of the Initial Commitments should be reversed. In other words, instead of specifying which data Google is not allowed to use, the commitments should prohibit Google from using any data, except for an exhaustive list of data Google may use and/or an exhaustive list of permitted uses. One respondent (an industry association) suggested that, in addition to a 'whitelist', the Initial Commitments should list, in a non-exhaustive way, specific data sources Google is not allowed to use.

(e) One respondent (an ad tech provider) suggested that Google should commit not to combine user data from any sources for advertising services. Two respondents (two ad tech providers) suggested that Google should commit to not using any individual-level user data from any of Google's owned and operated inventory to track users for targeting.

83. The CMA's provisional view was that the specific provisions of Section G are supplementary obligations that are binding on Google alongside the broader principles-based commitments set out in the Purpose of the Commitments and the Development and Implementation Criteria, and other obligations to which Google is subject. Following the Second Consultation, that remains the CMA's view, for the following reasons. The CMA will assess the overall impact of the Privacy Sandbox Proposals on competition in the light of a number of factors (including evidence on the effectiveness of the Privacy Sandbox tools) and will consider the need for further action if any remaining competition concerns are not resolved before the removal of TPCs.[23] Similarly, in relation to obligations under the applicable data protection legislation, the provisions of Section G of the commitments do not imply that any conclusions have been reached in relation to Google's obligations under the applicable data protection legislation.[24]

84. In relation to various submissions to the effect that paragraph 24 of the Initial Commitments should further constrain Google's ability to use data for advertising on owned and operated inventory (eg the suggested inclusion of all user-facing services such as Search and YouTube), the CMA's provisional view was that adding such restrictions to the commitments was unnecessary. As noted in paragraph 83 above of this Appendix 2, the CMA would wish to assess the overall impact of the Privacy Sandbox Proposals on competition in the light of a number of factors, including evidence on the effectiveness of the Privacy Sandbox tools. Following the Second Consultation, the CMA's view is unchanged. The case for any further restrictions on Google's use of data can be

[23] Paragraphs 6.55 to 6.63 of the June Notice contain text to this effect.

[24] In particular given the amendments to Section A of the commitments since the First Consultation, as outlined at paragraphs 4.18-4.20 of this Decision. See also the ICO Opinion (as referred to at footnote 9 of this Decision).

considered further, if necessary, during the Standstill Period or beforehand, once there is greater certainty as to the precise form that the Privacy Sandbox Proposals will take.

85. Two respondents (an ad tech provider and an industry association) queried whether paragraphs 23 and 24 of the Initial Commitments applied to data that Google has accumulated in the past.

86. The CMA's provisional view was that any historical use of data was beyond the purpose of the commitments, but noted that the commitments prohibited Google from using data collected in the past for purposes which would no longer be in line with the commitments. This remains the CMA's view, following the Second Consultation.

87. Some respondents (including two ad tech providers, an industry association and a publisher) submitted that certain obligations in Section G of the Initial Commitments may be imprecise, as some terms were not defined. One of these respondents (an industry association) suggested defining 'first and third-party data'. A related point was that 'third-party inventory' was not defined.

88. The CMA's provisional view was that amendments made to the commitments since the First Consultation have clarified these terms, where needed. The CMA's view remains the same, following the Second Consultation, as the Final Commitments also reflect those amendments. With respect to terms containing 'first-party' and 'third-party', the meaning of these terms depends on the context in which they are used, so it is impractical to include them as a defined term in the commitments.[25]

89. Some respondents (including two industry associations) were concerned about the use of data from WebID, and that Google might be using email addresses collected via WebID for advertising purposes. Similarly, three respondents (two industry associations and a data owner) submitted that Google might use IP addresses or the user-agent string whilst denying them to others.

90. In the CMA's provisional view, any such behaviour would be precluded under the obligation on Google not to discriminate set out in Section H of the commitments. This is also the CMA's view, following the Second Consultation. This view takes into account, in particular, amendments made since the First Consultation to Section H (on which, see paragraphs 4.287 to 4.329 of this Decision).

91. One respondent (an ad tech provider) submitted that the commitments should

[25] The ICO Opinion (as referred to at footnote 9 of this Decision) sets out further discussion of the terms 'first-party' and 'third-party' in relation to online advertising.

not allow Google to use probabilistic methods for estimating across browsers and devices, and the possibility for timing attacks – but did not mention for what purposes. A different respondent (a publisher) gave the example of a feature which DV360 has called 'Modelled frequency management for anonymous inventory', speculating whether this feature is using fingerprinting (which can be probabilistic).

92. The CMA's provisional view was that the purpose of the commitments is not to prevent Google from using fingerprinting to track users. Rather, it is to ensure that Google does not use fingerprinting to track users for targeting or measuring digital advertising whilst restricting others' ability to do so, as set out in Section H of the commitments. Given the provisions of the Final Commitments, following the Second Consultation the CMA's view on this point remains the same.

Data sharing with third parties/structural remedies

93. Five respondents (two ad tech providers, two industry associations and a publisher) suggested that instead of a commitment not to rely on specific data, Google should be required to share data with third parties. For example, it was suggested that data from Google's own user-facing services, such as Analytics data on Google's properties, should be shared on equal terms with Google's competitors in the ad tech market. One respondent (a publisher) submitted that Google should make available pricing and bid data, commission rates for each part of the value chain, bid auction outcomes and conversion data. Another respondent (an industry association) indicated that Google should offer free of charge, high-quality, real time and continuous access to information on FLoCs[26] (or any other use case) as well as pricing conditions relating to bids placed by advertisers and intermediaries. One further respondent (an ad tech provider) submitted that Google should provide access to any indirect data Google uses to improve or optimise its advertising capabilities to all ad tech participants.

94. The CMA's provisional view was – and, following the Second Consultation remains – that a data access commitment is not required. The issue of data access can be considered further, if necessary, during the Standstill Period or beforehand, once there is greater certainty as to the precise form that the Privacy Sandbox Proposals will take.

95. One respondent (an ad tech provider) suggested that Google's (alleged) dominant position and conflicts of interest across the ad tech value chain could

[26] The reference to 'cohort' is no longer relevant: in January 2022, Google announced that it was replacing FLoC with Topics, an API that will provide interest-based topic categories. See Appendix 3 to this Decision, paragraphs 8–11. For details of possible competition concerns in relation to Topics, see paragraphs 3.41–3.43 of this Decision.

be effectively addressed only through separation interventions, and that the CMA should consider separation remedies as part of the DMU.

96. The CMA's provisional view was that structural separation was not required at this time. These issues can be revisited, if necessary, in due course. As outlined at paragraphs 4.418 to 4.422 of this Decision, this remains the CMA's view, following the Second Consultation.

Temporal application

97. One respondent (an industry association) suggested that 'after the Removal of Third-Party Cookies' was not the correct temporal application for Section G of the commitments. The implication was that (extensive) limits on Google's use of data should apply irrespective of progress on the Privacy Sandbox, from the date of acceptance of any commitments.

98. The CMA's provisional view was that, to address issues raised by the CMA, the provisions of Section G should apply once TPCs are removed.[27] This remains the CMA's view, following the Second Consultation.

Obligation not to discriminate (Section H of the commitments)

Conflicts of interest

99. Almost half of the respondents to the First Consultation (nine ad tech providers, five industry associations, two publishers, a browser and a data owner) submitted that Section H was too narrow in scope, making the submissions including those outlined immediately below.

    (a) Section H should: (i) cover Google providing access to its own properties and apps (eg YouTube); and (ii) not be limited to Google's advertising products, ie Google should not use the browser changes to self-preference any of its products or services. The CMA provisionally considered that requiring Google to allow for access as noted under (i), or to expand the commitments as noted under (ii), would be outside of the scope of the competition concerns of this investigation. The investigation's scope has not changed, and neither has the CMA's view – following the Second Consultation – that the commitments therefore require no modification in this regard.

    (b) Section H should not be limited to the removal of TPCs but include other proposals under the Privacy Sandbox that could have a significant impact on

[27] See the ICO Opinion (as referred to at footnote 9 of this Decision).

the web advertising ecosystem (eg WebID, Gnatcatcher, Event Conversion Measurement API,[28] User-Agent Reduction and Privacy Budget).[29] The CMA provisionally considered that the commitments need no modification in this regard. This remains the CMA's view, following the Second Consultation – on the same basis, ie that Section H clearly refers to the Privacy Sandbox Proposals as defined in Section B of the commitments, and is not limited to the removal of TPCs.

(c) Section H should also include a limitation on Google discriminating against third parties with which Google does not directly compete, thereby preventing Google from benefiting certain market participants over others. To the extent that this relates to the CMA's competition concerns, the CMA provisionally considered that this is already covered by the scope of Section H and, therefore, the commitments needed no modification in this regard. Given the provisions of the Final Commitments, following the Second Consultation the CMA's view on this point remains the same.

(d) Section H should adopt a wide interpretation of non-discrimination, not limited to self-preferencing but including non-disintermediation. The CMA provisionally considered that the commitments did not need to be modified. This remains the CMA's view, following the Second Consultation – on the same basis, ie that the one respondent appears to be seeking to incorporate a particular interpretation of the European Commission's decision in *Google Search (Shopping)* into the commitments; the CMA notes that the European Commission decision in question does not itself refer to disintermediation.

100. One respondent (a publisher) requested more clarity as to the scope of the commitments, in particular whether Google providing preferential treatment to third parties in return for them agreeing not to compete would be included. The CMA provisionally considered – and, following the Second Consultation, considers – this point to be outside of the scope of the investigation. The CMA therefore does not consider any modification to the commitments to be required.

101. One respondent (an industry association) suggested that the obligation not to discriminate should be more specific, to avoid Google arguing that certain aspects which the CMA would want to see implemented fall outside the scope of the commitments (and thus avoid potentially lengthy legal disputes to

[28] Regarding the Event Conversion Measurement API, one respondent (an ad tech provider) explained that this API relies on last click attribution thereby not considering other contributions of other marketing channels, pointing out that the last click of a consumer is often on a search ad. It was submitted that the attribution metrics should be broadened to include non-search events. In January 2022, Google updated this API. It is now known as Attribution Reporting API, and includes view-through attribution: see Appendix 3 to this Decision, paragraphs 21–26.

[29] One of the respondents (an ad tech provider) indicated that this point should also apply to Sections C, D, E and F of the commitments.

establish whether discrimination has taken place). In this respondent's view, to address this concern, the following should be considered in relation to the commitments:

(a) including a reference to external legal standards (eg case law);

(b) providing examples of behaviour which the CMA would consider amounts to self-preferencing (eg reduction of interoperability between Chrome and third-party service providers), specifying certain impacts on third parties that would be regarded as self-preferencing;

(c) providing examples of what the CMA considers to be competitively sensitive information (eg bidding data shared by DSPs with Chrome in TURTLEDOVE); and

(d) clarifying that self-preferencing cannot be justified.

102. The CMA notes that Section H of the commitments is intentionally broad in scope and not intended to be exhaustive, whether by eg setting out (or cross-referring to) a summary of case law, or by listing specific behaviours that may amount to self-preferencing. The CMA provisionally considered that the inclusion of specific examples would risk limiting the scope and its assessment of the Privacy Sandbox Proposals. For the same reason, following the Second Consultation the CMA is of the view that the commitments do not need to be modified further in order to address on the above representations.

103. Several respondents also expressed concerns over the effectiveness of Section H.

(a) Two respondents (an ad tech provider and an industry association) stated that Google's own ability to target would need to be restricted (eg by limiting targeting capabilities on Google's owned and operated inventory to the level of targeting available under the Privacy Sandbox Proposals).

(b) Seven respondents (four ad tech providers, two industry associations and a publisher) submitted that, in order to tackle Google's data advantages and conflicts of interest across the ad tech value chain, a structural or at least functional separation of Chrome from Google's advertising activities is necessary. Four respondents (three ad tech providers and an industry association) submitted that, in the alternative, Google should turn over administration of the Privacy Sandbox to an independent entity. One respondent (an ad tech provider) submitted that this could be an independent standard-setting body, such as the Interactive Advertising Bureau, or a specially constituted body, such as the Transparency &

Consent Framework Board. Another respondent (an ad tech provider) suggested that the CMA should consider the application of structural remedies at the very minimum in the context of its work within the DMU.

104. The CMA's provisional view was that, at this stage, it is not necessary or appropriate to include requirements for operational separation within any commitments. This remains the CMA's view, following the Second Consultation, for both the reasons outlined at paragraphs 4.418 to 4.422 of this Decision, and the following reasons. The CMA recognises the importance of having in place an effective monitoring regime under any commitments. This regime was further refined, following the First Consultation, as outlined at paragraphs 4.430 to 4.384 of this Decision in relation to Section I of the commitments, as regards independent monitoring in particular. At this stage, the CMA considers that appropriate measures are in place to reassure third parties that action will be taken if Google does not comply with its non-discrimination obligation. Whether an element of operational separation is required is an issue that can be more appropriately considered during (or before) the Standstill Period, as needs be, when there is more clarity as to the precise form that the Privacy Sandbox Proposals will take.

105. Several respondents (an ad tech provider, an industry association, a data owner and a browser) noted self-preferencing concerns regarding specific Privacy Sandbox Proposals. For example, one of these respondents submitted that moving the auction to Chrome eliminates competition between SSPs and Google and implies that Google has the ability to self-preference and discriminate, as competitors will need to adjust and adapt to Google's changes. The CMA's provisional view was that the commitments need not be modified in order to reflect these representations, as Google's commitment not to discriminate as set out in Section H is broad enough to cover the concerns. Given the provisions of the Final Commitments, following the Second Consultation the CMA's view on this point remains the same.

106. Several representations were made in relation to FLoC.[30]

(a) Two respondents (a data owner and a browser) noted that through the FLoC proposal, Google would become the owner of segmented audiences excluding other providers of audiences, limiting available segmentation, and providing Google with the opportunity to extend its FLoC audiences into other channels thereby further entrenching its position.

[30] In January 2022, Google announced that it was replacing FLoC with Topics, an API that will provide interest-based topic categories. See Appendix 3 to this Decision, paragraphs 8–11.

(b) Two respondents (an industry association and a browser) submitted that FLoC would provide Google with central controls, and that a further commitment was needed: to require FLoC to be open source and subject to arbitration for the specification of central parameters. Otherwise, Google could ensure that the way(s) in which cohorts are created would be optimised for Google's systems and access to the data and information could allow for self-preferencing of other parts of Google's advertising platform.

(c) Four respondents (two ad tech providers, a publisher and a browser) raised concerns that Google will have a significant advantage compared to its rivals in decoding FLoC IDs (or in using FLEDGE), because FLoC IDs remains a black box to third parties, while Google has an intricate understanding of FLoC IDs.

(d) One respondent (a browser) submitted that FLoC would increase Google's data advantage as more overall user data would be needed to infer users' interests and preferences from FLoC than is the case with TPCs.

(e) One respondent (a browser) submitted that training advertising models to better understand users at the group level benefits from larger datasets and greater scale, which Google is privy to, giving Google a further advantage.

107. In addition to these representations regarding FLoC, one respondent (an ad tech provider) suggested that Fenced Frames[31] would make the ad tech industry dependent on Google for all measurement data, and further consolidate Google's position. Similarly, the respondent confirmed a concern noted in the June Notice, that if FLEDGE[32] were implemented with a 'trusted server' operated by Google, there could be room for Google to favour its own operations – and suggested that independent control and governance of such a server will be required.

108. The concerns raised by these respondents are consistent with those identified in paragraphs 5.71 to 5.73 of the June Notice. Some competition concerns expressed in relation to FLoC may still apply to the Topics API, and/or other APIs.[33,34] As set out in the June Notice (from paragraph 6.67) the CMA provisionally considered that the substance of these concerns relating to potential information asymmetries or data advantages would be addressed

[31] On 'Fenced Frames', see Appendix 3 to this Decision, paragraph 16.

[32] On 'FLEDGE', see Appendix 3 to this Decision, paragraphs 14–18.

[33] See Chapter 3 of this Decision.

[34] For example, the CMA notes that the concern mentioned above in paragraph 106(c) of this Appendix 2, in relation to FLoC, does not apply to Topics. This is on the basis that the output of Topics is designed to be understandable to all market participants. For further detail on 'Topics', see Appendix 3 to this Decision, paragraphs 8–11.

under the obligation not to discriminate set out in Section H of the commitments. The addition (since the First Consultation) of a new final sentence within Section H, clarifying setting out that the removal of Chrome functionality will remove that functionality not only for other market participants but also for Google,[35] provides further assurance to market participants. Given the provisions of the Final Commitments, following the Second Consultation the CMA's view on this point remains that no further amendments to the commitments are required in this regard.

Reporting and compliance (Section I of the commitments)

Compliance Statements

109. Two respondents to the First Consultation (an ad tech provider and an industry association) submitted that the CEO, rather than a delegated authority, should be required to sign Compliance Statements under the commitments. Respondents referred to both the importance of responsibility for compliance at the top of organisations, and to due diligence, personal knowledge and penalties.

110. The CMA's provisional view was that the commitments need not be modified as suggested. This remains the CMA's view, following the Second Consultation, on the following basis. The CEO is not necessarily the only appropriate individual within Google to sign Compliance Statements. Any individual signing these should be sufficiently senior to have authority to sign on behalf of Google, but sufficiently close to the operations of Google and the detail of the obligations in the commitments to understand the procedures and processes behind the statement.

111. One respondent (an industry association) suggested that reporting concepts from the US Sarbanes-Oxley Act should apply, to ensure that Google took certification seriously. In this respondent's view, as Google had to put in place internal controls to comply with US Securities and Exchange Commission's governance obligations, Google (and not the CMA) would be doing the work on verification tasks.

112. The CMA's provisional view was that the application of Sarbanes-Oxley reporting concepts is not appropriate in the context of any commitments entered into voluntarily under the Act. Following the Second Consultation, the CMA's view on this point has not changed.

[35] Final Commitments, paragraph 30 (and Modified Commitments, paragraph 30): see final sentence beginning 'For the avoidance of doubt, Privacy Sandbox proposals that…'.

Frequency of statements

113. One respondent (an ad tech provider) suggested that Google should provide both the Compliance Statement and the Monitoring Statement on a monthly basis.

114. The CMA's provisional view was that the commitments did not need to be changed as suggested. While there may be some periods in which additional reporting is required, monthly statements on compliance and monitoring would be overly burdensome on both Google and the CMA; provision for these on a quarterly basis is sufficient for the CMA to monitor effectively in this context. Following the Second Consultation, the CMA's view on this point remains the same.

115. Two respondents (an advertiser and an industry association) suggested that the CMA should publish Google's Monitoring Statements.

116. The CMA provisionally considered – and, following the Second Consultation, still considers – that these statements are likely to contain commercially sensitive information, so it would not be appropriate to require their publication.

Other suggestions in relation to Section I of the commitments

117. One respondent (an industry association) also proposed: (a) a power for the CMA to stop the Privacy Sandbox project in the event of Google's non-compliance with certification requirements; (b) a further anti-avoidance provision preventing purported 'personal' representation by Google at standard-setting bodies and open-source collaborations, reflecting industry experience that this can be a means to evade responsibilities; and (c) a requirement to articulate a private redress mechanism in respect of any breach of any commitments accepted, as in section 2(4) of the US Tunney Act (ie Antitrust Procedures and Penalties Act).

118. Three respondents (two industry associations and an ad tech provider) suggested that there should be a further anti-avoidance provision, to cover changes to like or equivalent effect, or modelled on the European Union's Digital Markets Act. A further respondent (an ad tech provider) suggested various additional commitments to address the future risk of any anti-competitive behaviour. One respondent suggested that anti-avoidance mechanisms in respect of other aspects of the Initial Commitments should be included.

119. The CMA's provisional view was that the commitments require no modification to address these suggestions. This remains the CMA's view, following the

Second Consultation, on the following basis. These suggestions appear to invite measures that would go beyond what is necessary to address the CMA's competition concerns. It suffices that the commitments include the anti-circumvention provision at paragraph 33 of the Final Commitments, and that the Monitoring Statements refer to the Monitoring Trustee's review of possible circumvention by Google of key provisions of the commitments (see Annex 3 of the Final Commitments, point C1).

Section J of the commitments

120. For the CMA's summary and assessment of First Consultation responses including submissions on Section J, see paragraphs 4.385 to 4.399 of this Decision.

Sections K, L and M of the commitments

121. One respondent to the First Consultation (an industry association) suggested that Section K of the Initial Commitments ('Variation or substitution') should be modified to further provide that Google may only offer a variation or substitution of any commitments as envisaged by section 31A(3) of the Act 'on the basis of substantial contemporaneous public evidence'.

122. The CMA's provisional view was that the commitments needed no such further provision. Relevant provision for variation or substitution is made in section 31A(3) of (and Schedule 6A to) the Act. It is neither necessary nor desirable to purport to place a restriction on how Google may seek to vary any commitments accepted by the CMA under the Act. Following the Second Consultation, during which the CMA received no further responses on Section K, the CMA's view remains the same.

123. No material representations were received, in response to the First Consultation, in relation to Section L of the Initial Commitments ('Effect of invalidity').

124. With regard to Section M ('Governing law and jurisdiction'), one respondent to the First Consultation (an industry association) raised a concern that under the Initial Commitments, Google had not expressly submitted to the exclusive jurisdiction of the courts of England and Wales. It was submitted that, in the event of a dispute arising out of the Initial Commitments, Google or a member of its corporate group might seek to challenge jurisdiction in the absence of such provision.

125. The CMA's provisional view was that Section M did not need to be modified to address this concern, since the relevant clause as drafted likely sufficed in all

the relevant circumstances. For the same reason, following the Second Consultation, the CMA's view on this point remains the same.

Other comments – scope of the commitments

126. Several respondents to the First Consultation commented on the scope of the Initial Commitments.

127. One respondent (an ad tech provider) suggested that accepting commitments relating to the web advertising market alone may be counterproductive, and that the Initial Commitments should address some known cross-market anti-competitive practices. The CMA's provisional view was that no change to the commitments was required to address this representation. The CMA assessed the appropriateness of any commitments offered during this investigation on the basis of the scope of the CMA's investigation. Following the Second Consultation neither the investigation's scope, nor the CMA's view on this point, has changed.

128. Two respondents (two ad tech providers) submitted that by disabling TPCs, Google's Chrome is following similar actions by competing browsers (notably Apple's Safari browser), so any remedy applied in this matter should be equally applied to other browsers. Three respondents (two ad tech providers and an industry association) similarly submitted that the CMA should seek to impose similar rules on all browsers deprecating TPCs (and possibly even mobile operating systems restricting third-party use of data), to at least set out what user control mechanisms may be acceptable. The CMA's provisional view was that commitments did not need to be modified in this regard. Following the Second Consultation, this remains the CMA's view. The CMA's investigation concerns Google's conduct, and only Google can offer commitments to address the CMA's competition concerns.

129. Five respondents (three publishers and two industry associations) suggested that the Initial Commitments should also cover Google's 'Accelerated Mobile Pages' or 'AMP'. Another respondent (an industry association) submitted that, as Accelerated Mobile Pages had the potential to distort competition by self-preferencing Google's advertising products and services, the CMA should obtain additional commitments from Google. The CMA's provisional view was the commitments needed no modification, as Accelerated Mobile Pages were not part of the Privacy Sandbox Proposals, and thus not within the scope of this investigation. This investigation's scope has not changed since, and neither has the CMA's view on this point following the Second Consultation.

130. Two respondents (an ad tech provider and an industry association) suggested that Google should commit to honouring the Initial Commitments (or at least

clarify which parts of them will apply) on a worldwide basis. One respondent (an industry association) wanted clarity on whether Google could remove TPCs outside the UK before the Standstill Period. The CMA notes that Google has announced publicly that Google will apply, on a global basis, any commitments accepted by the CMA in this investigation.[36]

Other comments – specific Privacy Sandbox Proposals

131. Ten respondents (five industry associations, three ad tech providers, a publisher and certain academics) to the First Consultation made other submissions, by reference to particular elements of the Privacy Sandbox Proposals. One of these respondents (an ad tech provider) suggested that Google should commit to offering publishers the ability to opt-out of participating in Google's Alternative Technologies without suffering any negative consequences, while those who opt-in should remain free to use rival solutions not developed by Google. In that respondent's view, Google should also commit to not hindering publishers from using their first-party data for the purposes of ad targeting or measurement on their inventory. Another of these respondents (an ad tech provider) also suggested that the Initial Commitments should explicitly prevent Google from hindering publishers' access to rival ad technology and services. Respondents also made submissions about the following proposals:

(a) TURTLEDOVE, FLEDGE and Fenced Frames: one respondent (an industry association) suggested that the Initial Commitments should have set out 'guard rails' specifying the required minimum properties (for example, setting the minimum group size for TURTLEDOVE);

(f) FLoC: one respondent (an industry association) submitted that the CMA should oblige Google to implement a centralized processing solution; two respondents (an industry association and certain academics) noted the possibility of inferring sensitive data about cohorts, and one of them submitted that there is a risk of discrimination which merits mention in any commitments;[37]

(g) Gnatcatcher: one respondent (an industry association) suggested that Google add specific commitments relating to Gnatcatcher, including

[36] See eg Google blog, Our Commitments for the Privacy Sandbox, 11 June 2021 (accessed on 2 February 2022).

[37] The reference to 'cohort' is no longer relevant: in January 2022, Google announced that it was replacing FLoC with Topics, an API that will provide interest-based topic categories. See Appendix 3 to this Decision, paragraphs 8–11. The CMA currently understands that any respondent concerns, relating to FLoC cohorts, about inferring sensitive data or a risk of discrimination may apply only to a much lesser extent to topics provided by the Topics API.

ensuring that the proposal is not altered in a way that harms legitimate business interests;

(h) First-Party Sets: one respondent (an industry association) submitted that the CMA should ensure that First-Party Sets data are not combined with Chrome browser functionality in a way that gives Google an unfair advantage over other market participants who are not active in the browser market;

(i) Privacy Budget: one respondent (an industry association) submitted that Google should commit to maintain access to data that allows competitors to create anonymous, probabilistic ID models, and extend the Privacy Budget accordingly ie access to IP addresses should not be blocked even if the Privacy Budget is used up; and

(j) Attribution and measurement: one respondent (an industry association) suggested also obliging Google to offer tools that enable attribution and measurement under the Privacy Sandbox while protecting users' privacy, taking into account the Development and Implementation Criteria.

132. The CMA's provisional view was – and, following the Second Consultation remains – that the commitments need not be modified to address the above points. The aim of the commitments is to ensure that general principles concerning the design, development and implementation of the Privacy Sandbox Proposals apply to the entirety of those proposals.

Appendix 3: Google's Privacy Sandbox Proposals

1. Google's Privacy Sandbox Proposals refer to Google's proposals to phase out support for TPCs and other means of cross-site tracking and introduce a number of alternatives to replace some of the functionality of TPCs.

2. This Appendix sets out the CMA's current understanding of proposals included in the Privacy Sandbox which are relevant for this Decision.[1]

First-Party Sets

3. Currently, the web standards community defines a TPC as a cookie which has been set by a domain which is different to the domain that a user is currently on. Cross-site tracking more generally is also defined by this pattern: identifiers are used to link a user's behaviour across different sites, also known as domains.

4. Following Google's intention to remove TPCs and other forms of cross-site tracking,[2] Google proposes to introduce 'a mechanism by which a set of registrable domains (a '**First-Party Set**') can declare themselves to be the same 'party' or entity, such as web properties owned by the same company, or domains with different ccTLDs used by the same website'.[3]

5. Google has informed the CMA that under the First-Party Sets mechanism, developers of multiple domains belonging to the same organisation will maintain the ability to access their own cookies, across their own domains, as these domains will be treated as first-party properties for this purpose. Such cookies will not therefore be categorised by Chrome as TPCs and will enable cross-site tracking across multiple domains or web properties, where those domains or web properties belong to the 'same organisation'.

6. Google has informed the CMA and the ICO that the First-Party Sets mechanism is under discussion in the W3C and that therefore this definition is potentially subject to change.

[1] To form its understanding the CMA has relied on publicly available information such as blog posts and discussions in relevant developer fora as well as meetings with and submissions by Google and third parties. See, in particular, The Privacy Sandbox: Technology for a More Private Web (accessed on 3 February 2022). For more information on the Privacy Sandbox see Digging into the Privacy Sandbox (web.dev), updated January 2022, and The Privacy Sandbox - Chrome Developers (each as accessed on 3 February 2022).
[2] See paragraphs 2.28–2.30 of this Decision.
[3] Google, Intent to Experiment: First-Party Sets and 'SameParty' cookie attribute (accessed on 3 February 2022). In this context, 'ccTLDs' refers to country code top-level domains.

Interest-based targeting

7. Currently, market participants use TPCs and make use of other web functionality as tracking methods such as link decoration, localStorage, iframes, User-Agent HTTP header and IP addresses to track users across multiple websites on Chrome,[4] to form profiles and infer individual user interests from browsing histories in order to target individual users with relevant advertising (interest-based targeting, also known as behavioural targeting). The below proposal is Google's suggested replacement for interest-based targeting without individual-level user tracking.

Topics

8. The Topics API is intended to enable interest-based targeting.[5] The initial taxonomy includes 350 topics,[6] and are publicly listed.[7] The topics are easy to interpret by humans, for example /Pets & Animals. The topics list will have ongoing human curation, with sensitive topics excluded. Google has stated that eventually it would like the taxonomy to be maintained by an external party, and that the IAB has expressed interest.[8]

9. Google proposes to create a model that would assign topics to websites (a classifier), based only on the hostname (including the domain and any subdomains), but not the full URL and query parameters, the content of webpages or any other information to assign topics to it. Google has informed the CMA that Google intends to make public the code and weights for the classifier model, as well as the labelled dataset used to train the model. Over time, the classifier model will improve. The classifier is initially developed by Google and built into Chromium, but it has indicated willingness to open source it and/or let it be externally maintained.

10. Every week, Chrome will calculate (locally on the user's device) the top five topics from the user's browsing history of sites that use the Topics API that week. Users can remove sites from their browsing history, remove specific topics, or disable Topics entirely. When callers on a website call the Topics API, the API will return one of the top five topics for each of the last three weeks (up

[4] Often these methods are combined to provide a robust signal that tracks a user across sites. For example, in this blog post (accessed on 3 February 2022) iframes and localStorage are combined to achieve cross-site tracking. localStorage can hold more data (5MB) than a cookie (4KB).
[5] An overview of the Topics proposal can be found here (accessed on 3 February 2022). Topics replaces Google's previous proposal, Federated Learning of Cohorts ('**FLoC**') and is intended to meet the same objective of enabling interest-based targeting.
[6] Google estimates a sample from 350 topics represents ~8 bits, in contrast to ~16 bits from FLoC.
[7] The first version of the taxonomy is listed on the GitHub page here (accessed on 3 February 2022).
[8] See notes from a meeting on 30 November 2021 of W3C's Improving Web Advertising Business Group here (accessed on 3 February 2022).

to three topics in total) for the user. Given the topic returned to callers on any given website is one of five possible topics, different websites may receive different topics for the same user, making cross-site tracking harder. All the callers on any given website for a given user will receive the same topic, and callers on a website cannot learn new topics by calling the API multiple times in a week (the API will return the same topic for that site and user). A user's topic is only returned to a caller if that caller had called the Topics API for that user on a website that is about that topic in the last three weeks. Finally, there is also a 5% chance of a random topic being returned to the caller, ensuring each topic has lots of members (k-anonymity) and providing some plausible deniability.

11. For more information, see Google's explainer for the Topics API.[9] This contains a discussion of privacy and security considerations, as well as open questions such as whether sites should be able set their own topics, and what happens if a site disagrees with the topics assigned to it by the browser.[10]

Retargeting and advertiser-defined audiences

12. Retargeting is the practice of serving targeted ads to specific individuals who have visited an advertiser's website. For example, an advertiser may wish to show an ad of the specific product that a user has browsed or placed in a basket on its website. For retargeting to be possible following the deprecation of TPCs, a mechanism is needed for advertisers to create their own targeting cohorts or 'interest groups'.

13. There have been a number of different proposals put forward by Google and other market participants aimed at allowing advertisers to retarget users, while meeting Google's aim of preventing cross-site tracking. Google's proposal is TURTLEDOVE, which it has refined over time in response to feedback and ideas in counterproposals (such as SPARROW, PARROT, TERN and Dovekey). FLEDGE is an early prototype to experiment with ad serving using TURTLEDOVE ideas. The CMA understands that Google's latest position on TURTLEDOVE is set out in Google's explainer for FLEDGE.[11]

Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE), First 'Locally-Executed Decision over Groups' Experiment (FLEDGE) and related proposals

14. Advertiser websites ask browsers that visit to join one or more advertiser-defined interest groups for a limited amount of time. A key difference with current

[9] Google's explainer for the Topics API is available at the GitHub page here (accessed on 3 February 2022).
[10] See the first few GitHub issues opened here (accessed on 3 February 2022).
[11] Google's explainer for FLEDGE is available at the GitHub page here (accessed on 3 February 2022).

retargeting approaches using TPCs is that the advertiser does not keep information about which browsers are in which interest groups. For each interest group, the browser stores information about who owns the group, JavaScript code for bidding logic,[12] and how to periodically update that interest group's attributes. Browsers will prevent individual-level targeting by only showing ads and allowing updates for interest groups that are targeted to at least 100 people (although it is unclear how this can be enforced without a centralised server). Later, when a browser visits a different webpage with an opportunity to show a display ad, the browser will run an on-device auction,[13] using appropriate auction logic determined by both the seller and the buyer. The auction may produce no winning ad, in which case the seller may choose to show a contextually targeted ad.[14]

15. Buyers that have eligible interest groups have an opportunity to bid. The browser executes each buyer's bidding logic. For each eligible interest group, the browser may make an uncredentialed (cookie-less) fetch from a 'trusted' key-value server,[15] allowing the buyer (the advertiser or DSP) controlling the interest group to make the browser take account of real-time data (such as the remaining budget of the ad campaign). Advertisers and DSPs upload information (key-value pairs) to the trusted server in advance. The governance and technical guarantees of this 'trusted' key-value server have yet to be fully developed. As part of the proposal, at a minimum, the server must not do any event-level logging or allow other market participants to be able to access information that would enable them to correlate or link interest group requests with other bid requests (such as for contextual ads) that are sent when users visit a website.[16]

16. The winning interest group ad is rendered in a '**Fenced Frame**', a mechanism that prevents the surrounding webpage from learning about the contents in the frame, and thereby leaking information about the user's ad interests.[17,18] Fenced Frames will initially be optional during the transition period before the deprecation of TPCs. Google's original proposal is that the browser will only serve ad content that was previously downloaded (that is, requiring the browser to pre-download interest-group ads). In the explainer for FLEDGE, Google entertains the possibility that advertisers and DSPs could upload ads on to a

[12] This contrasts with a number of other counterproposals, such as SPARROW, which allow for the bidding logic to be hosted by a trusted server (a Gatekeeper) rather than in the browser.
[13] By contrast, SPARROW allows the auction to be run by a trusted 'Gatekeeper' server rather than in the browser.
[14] Currently, more design work is needed for TURTLEDOVE and FLEDGE to be able support multi-level decision-making which are commonly used in modern ad tech supply paths, with multiple auctions, header bidding, etc.
[15] For FLEDGE, as a temporary mechanism, buyers can use any server.
[16] However, in the transition period before the deprecation of TPCs, Google is allowing event-level FLEDGE reports. Google plans to move to aggregate reports in the long term.
[17] As a temporary mechanism, FLEDGE will allow frames to communicate with outside servers.
[18] Google's explainer for Fenced Frames is available at the GitHub page here (accessed on 3 February 2022).

'trusted' CDN server that does not keep logs of the resources it serves, from which browsers could render ads. As with the trusted key-value server, the governance and technical guarantees of the trusted CDN server have yet to be fully developed.

17. To address user feedback, Google has added features to FLEDGE, eg a way for ads to be composed of multiple parts and stitched together on the browser.[19] Google is also supporting multiple auctions run by different SSPs.

18. TURTLEDOVE will need to allow sellers and bidders to learn the outcome of the auction. As a temporary mechanism, FLEDGE as originally proposed would allow sellers and buyers to send event-level reports to their servers, to perform logging and reporting on the auction outcome (as well as verification of viewability, etc.). More design work is needed on a 'trusted-server' reporting mechanism that does not allow reporting to be used to learn the interest groups of users visiting the publisher's site.

Measurement, attribution and reporting

19. Currently, TPCs are used to determine whether and how many ads have been served successfully to users that were in targeted groups (measurement), and to help assess ad effectiveness by determining whether views and clicks on the ads led to conversions (attribution). The outcomes of ad auctions and delivery need to be reported to advertisers and publishers (reporting), to facilitate payment and show performance of contracts, and to enable improvements to future optimisation.

20. Privacy Sandbox contains some proposals for measurement, attribution and reporting following the removal of TPCs.[20]

Event-level reports in the Attribution Reporting API

21. This proposal would allow advertisers to attach a set of metadata (including an impression ID, intended conversion destination, expiry dates) to their ads, which would be stored by the user's browser when the ad is clicked or viewed. If the user visits the intended destination page and converts, the browser records the conversion event and, with a delay (potentially one day), sends a report to the publisher and advertiser (potentially via a common ad tech intermediary) that a conversion occurred which can be attributed to a click on an impression, without the inclusion of any information about the user.

[19] See Google's explainer for FLEDGE at is available at the GitHub page here (accessed on 3 February 2022).
[20] See, Google, Attribution Reporting - Chrome Developers, May 2021 (accessed on 3 February 2022).

22. Under Google's proposal,[21] there are some limits on the amount of information that would be stored by the browser. The browser will store a 64-bit event identifier for each ad click, enough for a unique ID for every click, so every click can be mapped to detailed data about the user. The browser will only allow 3-bits of conversion data (ie eight distinct values) to be attached to a click event, and 1-bit for view events,[22] so that conversion events cannot be mapped to detailed data about the user. Chrome will add noise to the conversion data, so that a proportion of the time (to be calibrated by browsers, using differential privacy, as currently proposed) Chrome will report a random value instead of the actual conversion data.

23. Chrome will report up to three conversion events per click and will send up to three reports (if the browser is open) within reporting windows (eg 2 days after ad click, 7 days after ad click, and a maximum of 30 days after ad click).

24. Market participants currently use a variety of attribution models (ie ways of assigning credit for a conversion to events leading up to it). Google's proposal initially supported only last-click attribution,[23] but Google has since added the capability for advertisers to prioritise different kinds of ad events they would consider as important conversion metrics across publishers. In this set-up, if multiple ad events are associated with a conversion, the API will report for the event with the highest priority.

25. The initial Event Conversion Measurement API was made available to developers for Origin Trials on 6 October 2020, and ended on 25 January 2022.[24]

26. In January 2022, Google announced that it was adding new features, both for event-level and summary reports. A limited number of redirects will allow multiple ad tech providers (up to 10, under current proposal) to participate in a chain of verification, and to produce their separate reports for publishers and advertisers. This is intended to better match the way third parties are configured today and facilitate adoption. Chrome is also introducing filtering options to exclude certain kinds of conversions, to reduce the risk of erroneous attribution as previously reported by stakeholders. Google has also said that it intends future versions will support web-to-app and app-to-web attribution in Android.[25]

---

[21] Attribution Reporting: What's changing in January 2022? - Chrome Developers (accessed on 3 February 2022).
[22] The limits on conversion data for view events are more restrictive, as views do not require significant active user interaction or intention, and happen more frequently than click events.
[23] This is where all the credit for the conversion is given to the website hosting the ad that was last clicked, and all other relevant ad clicks or views before the conversion are given no credit.
[24] Chrome Origin Trials, Trial for Conversion Measurement, ending January 2022 (accessed on 3 February 2022).
[25] For the relevant previous stakeholder reports, see GitHub page here (accessed on 3 February 2022). For information on the relevant future versions, see GitHub page here (accessed on 3 February 2022).

In the transition period before TPCs are deprecated, an opt-in debug mode with unique debug IDs is intended to allow ad interactions and conversions to be paired.

Aggregated reporting: Multi-browser aggregation service, Aggregate Conversion Measurement API, and Aggregated Reporting API

27. Google has explored designs for a 'multi-browser aggregation service', a mechanism that would be able to aggregate information from multiple sources (such as browser clients or websites) in a privacy-preserving way, preventing the entity performing the aggregation from learning the underlying data from each source.[26]

28. Google explores how some of the limits of the Attribution Reporting API (discussed in the previous section) can be overcome, without compromising on privacy, through aggregating data across multiple users' browsers. For example, it may be possible for market participants to have more granular conversion data (more than 3-bits) at a faster rate, and multi-touch attribution models. Using such a multi-browser aggregation service, an ad tech provider could combine information from multiple browser clients in a report that is only sent if there is sufficient aggregation.[27]

29. In addition, the aggregation service may also support a generic Aggregated Reporting API, which can combine information across multiple websites into a single report, supporting use-cases like measuring reach (the number of distinct users that viewed an ad) and a form of frequency capping (although this would be a per-user per-publisher cap, rather than a per-user cap, which is calibrated using aggregated data).[28]

Combating Spam and Fraud

30. Websites currently rely on identifiers and cross-site tracking to establish whether a user is trustworthy or engaged in spam or fraud. Privacy Sandbox includes a proposal for a Trust Token API.[29] The aim of this API is for trust signals to be transmitted between websites without allowing the users' identity to be discovered across sites. Rather the Trust Token API aims to enable sites to collaborate in segmenting users into 'trusted' and 'untrusted' categories. To do so, a website that has already established a user's trustworthiness would be

[26] Google, Multi-Browser Aggregation Service explainer (accessed on 3 February 2022).
[27] Google, Conversion Measurement with Aggregation explainer (accessed on 3 February 2022).
[28] Google, Aggregated Reporting API (accessed on 3 February 2022).
[29] Google, Trust Token API (accessed on 3 February 2022). The proposal makes use of the 'Privacy Pass' protocol.

able to issue that user's browser with trust tokens.[30] These tokens could then be redeemed on other websites establishing trust without identifying the user or providing information on the origin of the token. The tokens themselves will allow for limited information to be communicated. Additionally, sites will have limits on how many issuers can be on them.

Cross-site privacy boundaries

31. Privacy Sandbox contains other proposals to mitigate workarounds that market participants may use to continue cross-site tracking without the use of TPCs.

32. This section focuses on selected proposals that aim explicitly to combat fingerprinting: the practice of collecting, linking and using a wide variety of information about the browser, other software, or the hardware of the user, in conjunction, for the purpose of identification and tracking. Unlike cookies, which can be deleted by users to prevent identification via that particular vector, many of the browser and system characteristics used for fingerprinting cannot be easily modified by the user (such as system fonts).[31]

33. Much of the identifying information that could be used in fingerprinting is part of how the internet and World Wide Web currently work and is requested and used by websites that do not engage in fingerprinting to provide necessary and useful functionality to users, including fraud and spam detection.

User-Agent Reduction and the User-Agent Client Hints API

34. Currently, when browsers send requests to a web server to load content, browsers send a user-agent string which tells the web server information about the user's browser and device. This information can be useful for websites (for instance, to select the most suitable version of a website for the user's browser and device, or to monitor for fraud and abuse), but it also reveals extra information that can be used for fingerprinting.

35. Under the Privacy Sandbox Proposals, the amount of information that is made available to websites via the user-agent string will be reduced ('**User-Agent Reduction**').[32] Specifically, the high-entropy values such as minor version numbers will be removed, whereas the browser name, major version, mobileness and operating system name will remain.[33] For the high-entropy values, a replacement API called User-Agent Client Hints is being made

[30] This website is known as the 'issuer'. Any website can issue trust tokens.
[31] For an overview of fingerprinting see Market Study, Appendix G, pages 14–19.
[32] For more details on the User-Agent Reduction, see the Chrome page here (accessed on 3 February 2022).
[33] Mobileness refers to a Boolean value as to whether the device is a mobile device or not.

available through which websites can request additional information from browsers about specific features, and browsers may give specific 'hints' in response.[34] Whether the browser will provide correct information will eventually depend on how much information is requested (in the sense of how 'uncommon' or identifying that information is) and the website's available Privacy Budget.[35] However, before the removal of TPCs, third parties will be able to make unlimited requests for (and receive) User-Agent Client Hints, ie Google will not enforce the Privacy Budget limits.[36]

36. User-Agent Client Hints will make all the values that Google is reducing in the original user-agent string available as 'hints'. The key differences between the user-agent string in its original form and User-Agent Client Hints include:

    (a) User-Agent Client Hints will itemize each of the different granular (high-entropy) data values that would otherwise appear together in the user-agent string, into distinct pieces of data that can be requested individually; and

    (b) websites will need to actively request the individual User-Agent Client Hints they wish to receive, rather than receive them all by default.

37. User-Agent Client Hints is currently available in the stable version of Chrome for websites to adopt. The User-Agent Reduction is planned to take place from April 2022, but sites will be able to opt into a deprecation trial that can extend access to the original user-agent string for at least six months until the final phase of reduction.[37]

Global Network Address Translation Combined with Audited and Trusted CDN or HTTP-Proxy Eliminating Reidentification ('Gnatcatcher')

38. IP addresses have primarily carried out two functions: to identify the host of a network interface; and to provide the addressable location of the host in the network, allowing a path to that host to be established. However, by their very nature, IP addresses also are a close-to unique identifier for web users, and a unique identifier for a browser at a point in time, and they can be found easily on and routed over the open internet.

39. Given widespread availability of IP addresses and their ability to provide a somewhat stable signal over some amount of time, they are often used by advertisers, publishers and ad tech providers in conjunction with other identifiers

[34] Documentation for User-Agent Client Hints can be found at the GitHub page here (accessed on 3 February 2022).
[35] In relation to Privacy Budget, see paragraphs 44–45 below of this Appendix 3.
[36] Final Commitments, footnote 3.
[37] More detail on the deprecation trial proposed is set out here (accessed on 3 February 2022), with the design document available here (accessed on 3 February 2022).

to identify and track users across sites. When used in combination with additional geolocation software, can also be used to determine the approximate geographic position of a user's device for localised advertising. IP addresses are important identifiers in the enablement of cross-device tracking,[38] and are also used by websites to combat fraud and abuse.

40. The Gnatcatcher proposal has the goal of reducing the amount of information available in a given IP address that websites see during network address translation ('**NAT**').[39] The Gnatcatcher proposal combines two previous proposals 'Near-Path NAT' and 'Willful IP Blindness'.

41. The Near-Path NAT proposal allows a browser to forward its HTTP traffic through a server that masks IP address, utilising the end-to-end encryption of TLS.[40] This would mask a user's original IP address from other third-party organisations, by allowing users to send their traffic through the same server, so it appears to originate from the same pool of IP addresses.[41] This service, applied across Chrome, would operate similarly to services that already exist in market for consumers wishing to hide their IP address when using the internet (ie Virtual Private Network services or like a traditional NAT).

42. The Willful IP Blindness proposal would give sites the option to self-certify that their servers are masking IP addresses from the application layer when transferring information on the serving infrastructure layer. This could be implemented, for example, by use of a HTTP header. The intention behind this is to make IP addresses an active surface, that can be accounted for in the Privacy Budget, rather than a passive one.[42] Under the proposal, the policy could be enforced by introducing audits and spot-checks (accounted for in the Privacy Budget). Parties who do not opt into Willful IP Blindness may be subject to the Near-Path NAT – or both could be implemented across the board.

43. The Willful IP Blindness proposal acknowledges the need for high amounts of entropy for certain fraud and abuse detection use cases and has proposed some principles to guide how and when IP address might be able to be used.[43] It is

[38] Cross-device tracking is discussed in the Market Study, Appendix G, paragraphs 14-47.
[39] More detail is set out in the Gnatcatcher GitHub 'explainer' on the GitHub page here (accessed on 3 February 2022). The GitHub 'explainers' for both previous proposals can be found on the GitHub pages here (for Near-Path NAT; accessed on 3 February 2022) and here (for Willful IP Blindness; accessed on 3 February 2022). Network address translation ('**NAT**') is the method of translating (mapping) between one IP address space and another by putting information in IP header of packets while in transit.
[40] Transport Layer Security ('**TLS**') is a cryptographic protocol to encrypt communications over a computer network. It is used as the main network security mechanism for the application layer of network communication on the web, and is what puts the 'S' in 'HTTPS'.
[41] Routing traffic through a proxy-server causes all traffic to appear to originate from the same pool of IP addresses.
[42] More detail on passive fingerprinting surfaces is set out in the Privacy Budget repository on the GitHub page here (accessed on 3 February 2022).
[43] More detail on this is available at the GitHub page here (accessed on 3 February 2022).

currently unclear how governance of such use cases will work, but the CMA is comfortable that the commitments are a suitable framework within which to oversee the development of this proposal.

Privacy Budget

44. Privacy Budget is a proposal to tackle fingerprinting and other workarounds to cross-site tracking after TPCs are deprecated. Under the Privacy Budget proposal, Chrome will assign an information budget to each website and monitor the information provided to each website.[44] When a website has used up its budget, Chrome will stop sending correct information, substituting it with imprecise or noisy results or a generic result that does not vary between users. Budget increases for specific information can be requested.

45. The Privacy Budget proposal is still under development, and is forecasted to be rolled out, at the very earliest, in 2023.[45] As a stepping stone, before Privacy Budget can be enforced, many of the tracking surfaces that are 'passive' may first need to be turned into 'active' surfaces. Passive surfaces are those which are information streams by default (eg IP address, user-agent string). By contrast, active requesting requires sites (notionally on behalf of users) to actively harvest the information (eg cookies, or JavaScript) and is thus detectable on the client (browser).[46] For example, user-agent string moving to User-Agent Client Hints turns it from a passive to an active surface. Because only active surfaces are detectable by the client, Privacy Budget depends on other proposals in the Privacy Sandbox that turn passive surfaces to active ones, and is therefore expected to be enforced later relative to other proposals.

Shared Storage and storage partitioning

46. To prevent various storages being used for cross-site tracking, Chrome is partitioning storages by domain/party as part of the Privacy Sandbox changes.

---

[44] Privacy Budget may be measured in bits as done in information theory. Bits are the units of entropy and self-information, which are measures of information content. To illustrate, suppose an identifier X can only take one of two values (A or B) with equal probability (0.5). If we learn for an individual that the value of the identifier is A, then the 'self-information' of this particular outcome is 1 bit. The entropy is the expected value of the self-information of all possible outcomes and indicates how 'informative' or 'surprising' learning the value of that identifier would be on average. 33 bits of identifying information would be enough to uniquely identify a single person out of 7.8 billion people. Crucially, in practice, the amount of entropy of an identifier depends on context and what else is already known. For example, if an individual's postcode is known, the added information of their city gives no additional bits of information. Additionally, measures of k-anonymity (where k is the number of users with identical information) and differential privacy measures may be used.

[45] Google, Privacy Sandbox Timeline (accessed on 3 February 2022; 'Last update: January 2022').

[46] For an explanation of passive vs active fingerprinting see W3C, Fingerprinting Guidance, September 2021 (accessed on 3 February 2022).

This includes storage partitioning,[47] network state/HTTP cache partitioning,[48] and Cookies Having Independent State ('**CHIPS**').[49] Recognising that shared storage across sites can have legitimate use cases, Google is proposing a new Shared Storage API.[50]

47. The Shared Storage API will be unpartitioned and allow origins to write to it from their own contexts on any page. To prevent cross-site tracking, data in Shared Storage may only be read in a secure environment with carefully constructed output gates. Some legitimate use cases for which output gates will be supported include: simple A/B experiments; or cross-site reach measurement of an ad campaign. The Shared Storage API is dependent on fenced frames, and the aggregate reporting API.

Federated Credential Management

48. With the deprecation of TPCs and limitation of other forms of cross site tracking which Google is undertaking, the use case of federated log-in is impacted.[51] The Federated Credential Management ('**FedCM**') proposal aims to prevent federated log-in being used for cross-site tracking, while preserving its intended functionality.[52] At this stage, Google has explored three variations of potential solutions, and it is not yet clear which form the proposal will ultimately take. It could mean that the browser adds more friction (eg in the form of permission prompts) or takes control of choice architecture around the use of federated log-in. It could also mean that website federated log-in systems could delegate a log-in to the browser, effectively making the browser a delegated representative of the identity provider. More information on FCM can be found in Google's explainer.[53]

[47] Google, Storage Partitioning (accessed on 3 February 2022).
[48] Google, HTTP Cache Partitioning and Network Stage Partitioning (each as accessed on 3 February 2022).
[49] Google, CHIPS (accessed on 3 February 2022).
[50] Google, Shared Storage explainer (accessed on 3 February 2022).
[51] Federated log-in allows users to use a single method of authentication (eg username and password) to access multiple websites, rather than creating a new username and password for each website. This is commonly experienced by users as 'log in with identity provider X to website Y'. Another common application is to log in to enterprise accounts in one place and be signed-in in many places thereafter, although this is more precisely referred to as 'single sign-on'.
[52] This is done by breaking federated log-in related tracking into two subproblems, the identity provider ('**IDP**') tracking the user and the relaying parties ('**RP**') tracking them. The RP tracking problem is addressed by making global identification directed. The IDP tracking problem is addressed by unbundling the issuing and the presentation of credentials. For more on the proposal, see the GitHub page here (accessed on 3 February 2022).
[53] Google, Federated Credential Management explainer (accessed on 3 February 2022).

Appendix 4: Implementation of the commitments

1. This appendix sets out more detail on how the CMA envisages certain aspects of the Final Commitments will be implemented. It covers:

   (a) the CMA's approach to assessing the effectiveness of the Privacy Sandbox Proposals, including through involvement in Google's testing and trials;

   (b) monitoring and the role of the Monitoring Trustee; and

   (c) involvement of third parties, including Google's obligations to respond to concerns raised and how the CMA plans to facilitate third-party engagement.

2. It is important to note that the CMA's approach to implementation may evolve over time, in response to changing circumstances and as the CMA gains more experience of how the commitments operate in practice.

Testing and assessment of effectiveness of the Privacy Sandbox tools

3. Google has committed not to remove TPCs before the expiry of the Standstill Period, during which the CMA will consider whether the development and implementation of the Privacy Sandbox addresses the competition concerns identified by the CMA. The assessment of whether the CMA's concerns have been met will depend on the effectiveness of the Privacy Sandbox tools in relation to the Development and Implementation Criteria,[1] namely:

   (a) impact on privacy outcomes and compliance with data protection principles as set out in the applicable data Protection legislation;

   (b) impact on competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants;

   (c) impact on publishers (including in particular the ability of publishers to generate revenue from advertising inventory) and advertisers (including in particular the ability of advertisers to obtain cost-effective advertising);

   (d) impact on user experience, including the relevance of advertising, transparency over how personal data is used for advertising purposes, and user control; and

   (e) technical feasibility, complexity and cost involved in Google designing, developing and implementing the Privacy Sandbox.

---

[1] Final Commitments, paragraph 8.

4. The CMA anticipates that this assessment will combine quantitative and broader qualitative analysis, as described in more detail below.

CMA's involvement in development of the Privacy Sandbox Proposals

5. Section E of the Final Commitments provides for the close involvement of the CMA in the development of the Privacy Sandbox Proposals. As provided in paragraph 17, Google and the CMA will seek to agree on the design of quantitative tests (including how and what to test), noting that the CMA may decide to take action pursuant to section 31B(4) of the Act should Google fail to carry out a test according to the CMA's preferred parameters.[2] There will be regular meetings and reports between Google and the CMA, with a view to ensuring that the Purpose of the Commitments is achieved.

6. Google will be undertaking quantitative testing[3] (as agreed with the CMA) of the effectiveness of the Privacy Sandbox tools individually, as well as in combination. It will also make the Privacy Sandbox tools available for market participants to conduct their own testing.

7. Google will send to the CMA the results, as well as data and explanations, of all significant tests it carries out. In addition, the results of each test, as agreed with the CMA, will be published by Google. Google will update the CMA on plans for user controls at least once a quarter. Further, under paragraph 17.c.iv. of the Final Commitments, should the CMA wish Google to carry out a test according to the CMA's preferred parameters, Google must do so within 20 Working Days (unless extended by mutual consent), failing which the CMA may decide to take action pursuant to section 31B(4) of the Act.

Outline of proposed approach to testing and trialling

8. This section provides an overview of the CMA's current plans for the implementation of Section E of the Final Commitments, and how these fit with Google's proposed testing programme. In keeping with the iterative nature of the dialogue envisaged in Section E, the CMA's plans regarding the testing of Privacy Sandbox may evolve over time.

9. The aim of testing and trialling is to contribute to the assessment of whether the development and implementation of the Privacy Sandbox tools addresses the CMA's competition concerns. Testing and trialling involves evaluating the impact of the Privacy Sandbox changes and measuring the outcomes on key parameters – for example, publisher and advertiser revenues, and

---

[2] Final Commitments, paragraph 17.c.iv.
[3] See the defined term 'Quantitative Testing' in Section B of the Final Commitments.

differences in impacts between Google and competitors.

10. In practice, the CMA anticipates that the CMA's main involvement in relation to Google's testing activities will be in:

    (a) designing the programme of testing with Google to ensure that (i) all the relevant tools and potential competition concerns are being examined, and (ii) appropriate data collection processes and metrics are in place, to be able to measure effectiveness against the Development and Implementation Criteria;

    (b) potentially facilitating and coordinating testing activities with Google and third parties (for example, where third parties need to supply data needed for evaluating impacts on them, or where third parties need additional technical resources or support from Google to be able to conduct their own testing);

    (c) evaluating the results of tests carried out by Google;

    (d) ensuring that results of tests, where these are material to evaluating effectiveness of the Privacy Sandbox tools, are published and amenable to scrutiny by third parties;

    (e) discussing (as appropriate) with Google the results of testing by third parties that are made available to the CMA; and

    (f) using the findings and results from testing by Google, as well as any additional views and evidence provided by third parties, to conduct an overall assessment of the Privacy Sandbox against the Development and Implementation Criteria during the Standstill Period.

11. The CMA also expects to involve the ICO in its engagement with Google on testing the Privacy Sandbox Proposals, particularly given that one of the Development and Implementation Criteria relates to the impact on privacy outcomes and compliance with data protection principles.

12. In testing and trialling of the Privacy Sandbox tools, Google will consider three broad use cases, and further use cases within each:

    (a) targeting – including the Topics API[4] and FLEDGE API, being developed to support interest-based advertising and remarketing respectively. One notable sub-use case is that of brand safety, where FLEDGE will be tested in combination with Fenced Frames API;

    (b) measurement and attribution – including the Attribution Reporting API, broadly aiming at measuring when a user's interaction with an ad leads to a conversion on an advertiser's website; and

---

[4] In January 2022, Google announced that it was replacing FLoC with Topics, an API that will provide interest-based topic categories. See Appendix 3 to this Decision, paragraphs 8 to 11.

(c) boundary cases – including Privacy Sandbox Proposals introduced to limit data collection and combat fingerprinting. Use cases include fraud prevention, defining first-party boundaries, and tailoring content to geo-location.

13. Google has indicated that it will carry out or support two main types of testing:

(a) functional testing – testing that the new tools and APIs actually work as designed and intended, for a range of use cases, and without major unforeseen side-effects; and

(b) effectiveness testing – measuring the impact of the new tools and APIs on market participants and outcomes, and assessing their effectiveness by reference to the Development and Implementation Criteria.

14. Functional testing will be organised around individual tools and APIs, whereas effectiveness testing is likely to involve both (i) testing the impact of certain tools/APIs individually, and (ii) testing the impact of several tools/APIs in combination for certain use cases. Eventually, as anticipated in the Final Commitments, before triggering the Standstill Period, Google will test the effectiveness of all Privacy Sandbox Proposals together.

15. For both functional and effectiveness testing, the following two basic approaches could be used:

(a) 'real world' experiments – where the developer (which might be Google or a third party) would run an experiment using the relevant Privacy Sandbox tool for a subset of users[5] and measures impacts and market outcomes, relative to a control group keeping existing technologies (similar to the Google TPCs randomised control trial that the CMA analysed in the Market Study);[6] and

(b) simulations – where it is not possible to run a 'real world' experiment (eg where certain market impacts are not measurable whilst TPCs are still available as an alternative) or where there is likely to be insufficient data available, the developer (Google or a third party) would supplement the available evidence by modelling and simulating the impact on a group of users, without these outcomes being observed in the real world.[7]

16. 'Real world' experiments and other testing by developers (including Google's Ads business as well as third parties) often take place in the context of

---

[5] Subject to users having opted in, in their user settings, to personalised advertising and trials of new Privacy Sandbox tools.
[6] Market Study, Appendix F.
[7] Testing may also combine elements of 'real world' experimentation and simulation. For example, Google's Ads business has previously run an experiment using real world traffic in combination with its own simulation of FLoC (that is, it created its own algorithm based on FLoC principles and used this in the experiment).

'Origin Trials'. These involve Google's Chrome business making the new tool or feature available to developers, who can self-select into participating and test it with a small subset of Chrome traffic, but where the developer may choose whether to share feedback with Google (Chrome) or not.

17. The CMA recognises the importance of the involvement of market participants in the design, implementation and evaluation of tests. In particular:

    (a) the CMA will want to understand market participants' views about policies underpinning a number of Privacy Sandbox Proposals;

    (b) the CMA will give due consideration to the results of market participants' own independent tests and trials; and

    (c) the CMA's ability to measure the impact of Privacy Sandbox Proposals on rival ad tech providers will be limited without their cooperation. The CMA is considering whether it might request metrics from other ad tech providers, such as DSP win rates in Google Ad Manager, volume of activity on rival exchanges, and other metrics; or take other steps to help coordinate market participants' experimentation.

18. Further to this, recognising the need for independent assessment, and to supplement the CMA's own technical expertise, the CMA is also considering involving one or more external expert(s) in the assessment of the effectiveness of Privacy Sandbox Proposals.

19. The CMA acknowledges that there are pros and cons associated with both quantitative and qualitative assessments. The benefits of quantitative testing include that (i) specific outcomes can be isolated and measured, and (ii) the outputs of different tests can be in the same units, which aids comparison and evaluation. The limitations of quantitative testing include that (i) it is only possible to observe short-term impacts of changes in the Privacy Sandbox tools, not the long-run impact once users have adjusted their behaviour, and (ii) in the case of testing undertaken by Google, Google's ability to test for quantitative impacts on competitors may be limited by the data they have access to.

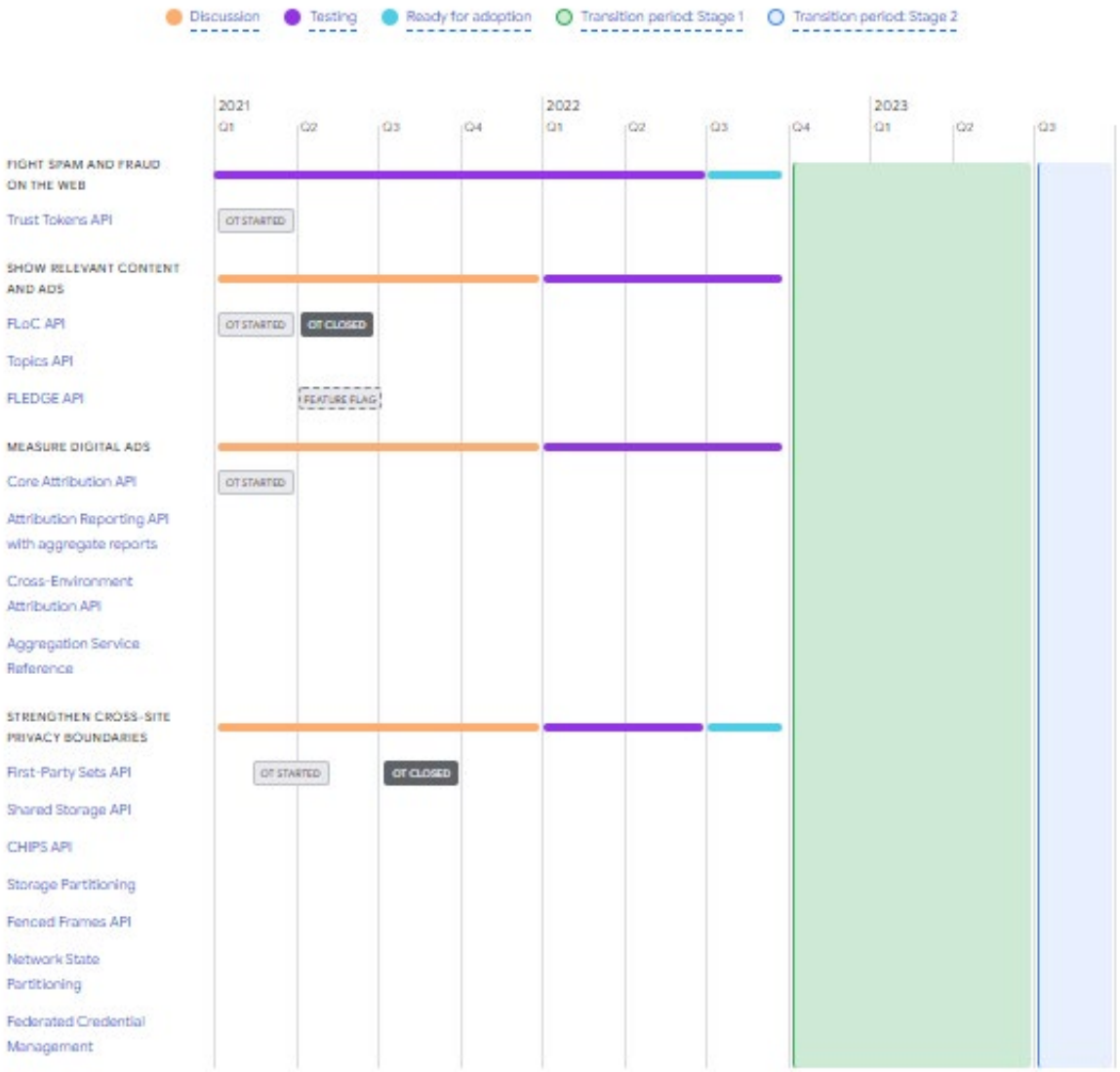
20. Qualitative assessment can take into account longer run effects and a broader range of outcomes, though it is usually underpinned by assumptions. There is thus a role for qualitative assessment, as well as quantitative evidence from third parties alongside the quantitative testing undertaken by Google, as it can supplement and enhance the evaluation of outcomes.

21. Google has published, and regularly updates, a timeline for the Privacy Sandbox, describing stages from testing of new Privacy Sandbox tools to

phase out of TPCs in Q3 2023.[8] The current version of this timeline (as notified to the CMA by Google on 4 February 2022) is reproduced below as Figure 1. It shows on a quarterly basis when APIs are expected to move from the 'Discussion' phase, in which limited testing may take place to assist discussions, to a full 'Testing' phase, when all technologies for the use case are available for developers to test and may be refined based on results. Within the 'Testing' phase reproduced below at Figure 1, Google envisages implementing the steps discussed in paragraphs 14 to 15 above (functional and effectiveness testing; testing APIs individually, testing groups of APIs for use cases, and finally testing all proposals in combination). The timing of these various steps has not yet been determined, and the CMA will expect updates (as applicable) to be provided to the CMA and publicly as they become available.

[8] Google, The Privacy Sandbox Timeline (accessed on 3 February 2022; 'Last update: January 2022').

Figure 1: Google's provisional outline timeline for quantitative testing



- *Google defines 'Transition Period: Stage 1' as 'all technologies for each use case are launched in Chrome and ready for scaled use across the web. Chrome will monitor adoption and feedback carefully before moving to the next stage.'*
- *For 'Transition Period: Stage 2', Google's timeline states 'Chrome will phase out support for third-party cookies over a three-month period finishing in late 2023.'*
- *In the process of assessing the effectiveness of Google's Privacy Sandbox Proposals, the CMA will consider the APIs on this timeline, as well as other Privacy Sandbox Proposals not captured here but which are listed in Annex 1 of the Final Commitments. In particular, the CMA will consider the effectiveness of Gnatcatcher, User-Agent Reduction and Privacy Budget. As stated in the Final Commitments, Privacy Budget will not be implemented before the Removal of TPCs. The CMA will want to assess the effectiveness of all Privacy Sandbox Proposals except Privacy Budget, separately and in combination, by the end of the Standstill Period. The Standstill Period maps onto the end of 'Transition period Stage 1' in this diagram.*

Monitoring and the role of the Monitoring Trustee

22. Alongside assessing the effectiveness of the Privacy Sandbox Proposals, the CMA will monitor and enforce compliance with the wider commitments agreed with Google.

23. Commitments relating to the implementation process, the design of the Privacy Sandbox Proposals and engagement with third parties will be monitored directly by the CMA. Commitments requiring operational changes relating to the use of data and self-preferencing will be monitored by a Monitoring Trustee, working with the CMA.

24. This section sets out the CMA's views on the role of the Monitoring Trustee including the skills and expertise required, and briefly describes how the CMA intends to monitor compliance with the broader commitments which are not subject to Monitoring Trustee oversight.

Role of the Monitoring Trustee

25. In its November Notice,[9] the CMA welcomed the proposal by Google to appoint a Monitoring Trustee. A Monitoring Trustee is an independent person or firm which is appointed to review and report on the compliance with orders or undertakings. In this case, the Monitoring Trustee would be reporting to the CMA on Google's compliance with the operational aspects of the Final Commitments where the CMA might otherwise be unable to effectively monitor what actions Google has taken to ensure that it complies with the Final Commitments.

26. The Final Commitments provide for the appointment of a Monitoring Trustee with the role to monitor compliance with paragraphs 25 to 27, 30 and 31 and, with respect to those provisions, compliance with paragraph 33 which requires Google not to circumvent any of the Final Commitments. The Monitoring Trustee will provide the CMA with a quarterly Monitoring Statement within three Working Days of the end of each three-calendar-month period following the Effective Date.

27. An outline of the contents of the Monitoring Trustee's reporting is set out in Annex 3 to the Final Commitments. In summary, this will involve the following.

    (a) For paragraphs 25 to 27 of the Final Commitments, the Monitoring Trustee will review and provide to the CMA: a description of the technical data separation mechanisms for compliance with the requirements of the

[9] Notice of intention to accept modified commitments offered by Google in relation to its Privacy Sandbox Proposals, 26 November 2021.

Final Commitments; a summary of the Monitoring Trustee's review of the relevant logs detailing the access history of any datasets within Google that contain data relevant to the Final Commitments; and a description of training on permissible data access Google has carried out and the attendees of such training.

(b) For paragraphs 30 to 31 of the Final Commitments, the Monitoring Trustee will provide: a description of various processes, procedures and other actions taken by Google and specified in Annex 3 to the Final Commitments; and a summary of the Monitoring Trustee's review of their implementation.

(c) For paragraph 33 of the Final Commitments, the Monitoring Trustee will provide a summary of the steps it has undertaken to provide a review of any putative circumvention of paragraphs 25 to 27, 30 and 31 of the Final Commitments.

28. Responses to the Second Consultation were generally supportive of the appointment of a Monitoring Trustee as a way of supporting effective monitoring and compliance of any commitments offered by Google. Consultation responses on the role of the Monitoring Trustee largely fell into the following categories:

(a) responses relating to the criteria for selection of a Monitoring Trustee; and

(b) responses relating to the way in which the CMA and third parties should engage with the Monitoring Trustee in support of the effective disposal of the Monitoring Trustee's role.

Criteria for selection of the Monitoring Trustee

29. In the November Notice, the CMA set out its view that the appointment of a Monitoring Trustee would be welcome, and described the role of that Monitoring Trustee. A number of respondents to the Second Consultation commented on how the Monitoring Trustee should be appointed, in order to be effective in its role. The main points raised were as set out below.

(a) The criteria for the appointment of a Monitoring Trustee should be clarified, and how reporting and compliance criteria will be determined.

(b) The Monitoring Trustee must be impartial and independent of Google.

(c) The Monitoring Trustee would require a deep understanding of the relevant aspects of Google's business. Examples given included: an understanding of the ad tech business and Google's ad tech suite in particular; data governance; the development and execution of training programs; software development and system design; and source code.

(d) The Monitoring Trustee should also possess wider skills, such as legal and compliance monitoring.

(e) The CMA should have a prominent role in the selection process of the Monitoring Trustee.

30. In this section, the CMA provides further clarification of how the CMA proposes to ensure that the terms of appointment of the Monitoring Trustee are consistent with the objectives of appointment of a Monitoring Trustee, as set out in the consultation.

31. As background, the Final Commitments state that appointment of the Monitoring Trustee is subject to the ongoing approval of the CMA, liaising with the ICO to ensure that the Monitoring Trustee has the appropriate level of privacy and data protection expertise. In order to give approval, the CMA will need to be satisfied both that the Monitoring Trustee has the capability to effectively dispose of the roles outlined in the Final Commitments, and that the terms of appointment of the Monitoring Trustee are consistent with the requirements specified in the Final Commitments.

32. Given that the monitoring will start shortly following acceptance of the Final Commitments, the CMA has already been in discussions with Google about the appointment of a Monitoring Trustee, and envisages that an appointment will be made upon (or shortly after) the issuance of the CMA's decision to accept commitments in this case. The criteria discussed below have been applied in the current process for the appointment of a Monitoring Trustee, and the CMA would expect them to be applied again, should a new Monitoring Trustee need to be appointed.

33. First, with regard to the suggestion that the Monitoring Trustee must be impartial and independent of Google, the CMA agrees. As such, part of the process for appointment will be a conflict check to ensure that the appointed business does not have any business relationships which would threaten its actual or perceived impartiality in performing the role of Monitoring Trustee. The CMA will ensure that the Monitoring Trustee complies with best practice in managing and mitigating any potential conflicts of interest.

34. With regard to the suggestion that the Monitoring Trustee would require a deep understanding of the relevant aspects of Google's business, the CMA agrees. The CMA also considers that it would unnecessarily limit the pool of potential Monitoring Trustees to require that one body must have all these skills in-house. The CMA therefore expects that the Monitoring Trustee – if not able to offer all these skills in-house – should be expected to work with an independent technical expert or technical experts who do have such skills. In that case, the role of the Monitoring Trustee in respect of the technical aspects of monitoring compliance with the final commitments would be to ensure the technical experts were capable of doing each specific monitoring

job and collating their outputs.

35. In relation to the suggestion that the Monitoring Trustee should also possess wider skills, such as legal skills, the CMA agrees with the suggestion. This very much fits in with the model referred to above where the Monitoring Trustee sets a framework within which technical experts carry out checks for compliance. The Monitoring Trustee would provide a legal, project and auditing umbrella to support the technical experts. The CMA regularly works with Monitoring Trustees and is aware of the skills required to be an effective Monitoring Trustee. The CMA's approval of any appointment would be conditional on the relevant firm being able to demonstrate a suitably broad mix of skills to effectively complete its work.

36. As regards the suggestions that the CMA should have a prominent role in the process for selecting the Monitoring Trustee, the CMA agrees, and is in ongoing discussions in respect of Google's approach to each of the key stages in such process up to the final consent to appoint a Monitoring Trustee. This is necessary to ensure that the CMA has sufficient information to be able to confirm that Google's choice of Monitoring Trustee would be effective as required by the Final Commitments. Google has already discussed with the CMA or will consult with the CMA on the following:

    (a) the tendering process;

    (b) the process for assessing the proposed Monitoring Trustee from tendered options;

    (c) the relevant aspects of the terms of reference or instructions to the Monitoring Trustee, including:

        (i) agreeing criteria with Google for all the areas to be covered and examined by the Monitoring Trustee (separate criteria for audit and technology roles);

        (ii) the formal role and actions to be taken by the Monitoring Trustee (and any advisers) and access within Google to enable them;

        (iii) the reporting requirements;

        (iv) confirming that the proposals for remuneration of the Monitoring Trustee do not give rise to a conflict of interest; and

        (v) areas in which the Monitoring Trustee may appoint technical experts and the process for any such appointment, including satisfying the CMA as to the expertise and independence of any appointee as a condition of CMA approval of their appointment.

37. The CMA will consider all this evidence before approving the choice of

Monitoring Trustee. The CMA therefore considers that it has a sufficiently prominent role in the selection process of the Monitoring Trustee.

Interaction between the Monitoring Trustee and the CMA

38. Respondents to the Second Consultation said that Monitoring Trustee's role should include taking account of the views of third parties. This could include observing all developments around the Privacy Sandbox, for example monitoring relevant public forums.

39. As described above, the Monitoring Trustee is expected to appoint or work with a technical expert, including satisfying the CMA as to the expertise and independence of any appointee as a condition of CMA approval of their appointment. The CMA would expect that, between the Monitoring Trustee itself and the technical expert, there should be sufficient knowledge of developments around the Privacy Sandbox to be able to effectively meet the objectives for the Monitoring Trustee. The CMA does not envisage that the Monitoring Trustee would gain this knowledge directly through engagement with third parties in respect of monitoring. The CMA would expect the Monitoring Trustee to have access to the skills to properly assess compliance with the Final Commitments and to report to the CMA.

40. The CMA agrees with the recommendation made during the Second Consultation that the CMA should maintain a direct line of communication with the Monitoring Trustee (ie not through Google).

41. While Google will pay for the Monitoring Trustee (and any technical experts), the Monitoring Trustee will be working for the CMA. As such, the CMA will have an open line of communication to the Monitoring Trustee. The CMA will receive quarterly compliance reports directly from the Monitoring Trustee. The CMA will also be able to request any documents, data and data logs that are or may be relevant to matters of compliance with the Final Commitments from the Monitoring Trustee.

42. The CMA will be able to assess the Monitoring Trustee's performance, and direct it to carry out specific tasks where appropriate. In circumstances where the CMA has reason to believe that the Monitoring Trustee is not meeting the requirements of its role, the CMA will be able to request that Google dismiss and replace the Monitoring Trustee following the same process as before.

The CMA's monitoring role

43. As noted above, the Monitoring Trustee will have a role in monitoring only a subset of the commitments – those relating to Google's use of data and self-preferencing by Chrome. For the other commitments, the CMA will monitor Google's compliance directly.

44. The commitments envisage that monitoring will be based around a quarterly reporting cycle. Google and the Monitoring Trustee are each required to provide the CMA with quarterly reports on compliance with the commitments. As set out in paragraph 32.a. of the Final Commitments, Google's report must include an explanation of how it has dealt with third-party issues raised.

45. The CMA will also monitor on an ongoing basis Google's compliance with its other commitments, including those relating to transparency, such as publishing regular updates on progress of the Privacy Sandbox Proposals.

46. The CMA anticipates that an important part of the CMA's monitoring role will involve following up on issues raised by third parties. The following section sets out in more detail how the CMA expects to involve third parties in this process.

Transparency commitments and involvement of third parties

47. An important aim of the Final Commitments is to provide greater transparency to affected third parties (such as publishers, ad tech providers and other market participants), and to ensure that their concerns are taken into account by Google in the development of the Privacy Sandbox Proposals. The CMA is also keen to ensure that it has a good understanding of stakeholder views on Google's proposals, which can then inform its engagement with Google in the development and testing process, along with its overall assessment of effectiveness of the Privacy Sandbox Proposals.

48. The Final Commitments require Google to design a process for engaging directly with market participants (third parties), and facilitate the involvement of the CMA in the process, including in highlighting issues raised by third parties as part of Google's design, development and implementation of the Privacy Sandbox Proposals.

49. The purpose of this section is to clarify:

    (a) the CMA's expectations of Google's design and implementation of its process for engaging with third-party concerns; and

    (b) how the CMA intends to facilitate third-party engagement through a mix of formal and informal channels.

50. The remainder of this section sets out the obligations provided for in the Final Commitments, and thereafter the CMA's broad proposed approach to facilitating engagement of third parties as envisaged by the Final Commitments.

Google's commitments to respond to third-party views and suggestions

Obligations arising from the Final Commitments

51. Google has made a series of commitments, the purpose of which is to improve transparency and stakeholder confidence about its engagement with concerns raised about the development and implementation of the Privacy Sandbox Proposals.[10]

52. The Final Commitments include publishing a process for Google's stakeholder engagement in relation to the details of the design, development and implementation of the Privacy Sandbox Proposals.[11] As part of this process, Google must:[12]

    (a) consider reasonable views and suggestions expressed to it by publishers, advertisers and ad tech providers in relation to the Privacy Sandbox Proposals including testing, in order to better apply the Development and Implementation Criteria referred to in paragraph 8 of the Final Commitments;

    (b) report on that process publicly; and

    (c) report on the process quarterly to the CMA, including updated timing expectations and substantive explanations of how Google has taken into account observations made by the CMA and third parties.

Design and implementation of the stakeholder engagement process

53. Paragraph 12 of the Final Commitments describes the stakeholder engagement process to be designed and owned by Google as the developer of the Privacy Sandbox Proposals. The CMA expects that Google will engage with market participants constructively and in good faith as part of the development and implementation process. This expectation relates to both:

    (a) views and concerns about the design and implementation of Privacy Sandbox Proposals at a technical level; and

    (b) views and concerns about the design of testing and trialling of specific Privacy Sandbox Proposals.

54. Google has said that it will set out the stakeholder engagement process on a dedicated microsite (either on www.privacysandbox.com itself, or prominently

---

[10] These commitments include those set out in paragraphs 11, 12, 14 and 32 of the Final Commitments.
[11] As part of this process, Google must publicly disclose timing (and updates to reflect changes or increased certainty) of key Privacy Sandbox Proposals accessible from a single webpage, which may also be made across blink-dev discussion group; within W3C and/or in a blog post, dedicated microsite or equally prominently: Final Commitments, paragraph 11.
[12] Final Commitments, paragraphs 12 and 32.a.

signposted and linked to that site).[13] The process will include the following engagement channels.

(a) **Dedicated stakeholder feedback channels:** the dedicated microsite will include an explanation of the key ecosystem stakeholder feedback channels that are part of Chrome's multi-channel feedback process. These include relevant GitHub issues and developer repositories on individual Privacy Sandbox Proposals; blink-dev and Origin Trial mailing lists, and the relevant W3C groups[14] and other industry fora. Google will provide a short description of the purpose of each feedback channel, and will include links to dedicated public forums of each Privacy Sandbox API where stakeholders can view community discussions and provide direct feedback.[15]

(b) **Specific feedback form:** a new feedback form will be available on the dedicated microsite, enabling any stakeholder to submit suggested use cases and API feature requests, as well as sharing direct feedback with Google's Chrome team. Google will encourage stakeholders using the form to share their feedback also in public forums to allow for public discussion of any suggestions. The details and format of this feedback form are still under consideration.

55. The CMA expects that, as part of this process and in engaging with stakeholders, Google will explain to stakeholders how it is responding to suggestions and concerns raised. This includes through Google's public reporting and reporting to the CMA, as outlined further below.

56. The Final Commitments are clear that the onus is on Google to demonstrate to the CMA that Google takes account (and how it takes account) of concerns raised by market participants (eg in particular publishers, advertisers and ad tech providers) in order to comply with the obligations set out in the Final Commitments.

Transparency reporting to market participants and the CMA

57. The Final Commitments in paragraphs 12 and 32.a. oblige Google to report on the stakeholder engagement process publicly and to the CMA. The aim of these provisions is to keep market participants updated on Google's process, provide confidence that the stakeholder engagement process is being

---

[13] Google has told the CMA that the microsite will be published by no later than 28 February 2022.

[14] Currently these groups include, in particular: Improving Web Advertising Business Group; Privacy Advertising Technology Community Group; Privacy Community Group; and the Web Platform Incubator Community Group. (all accessed on 8 February 2022)

[15] Google will explain on the microsite that the input received through the feedback channels will: (i) inform the design, development and implementation of the Privacy Sandbox Proposals, including testing; and (ii) be reflected in the quarterly reports submitted to the CMA within the context of the commitments.

managed effectively and that market participants are being treated consistently, and ensure that stakeholder views are being taken into account in the development of the Privacy Sandbox Proposals.

Google's public reporting

58. To implement this commitment, Google has proposed to publish regular updates (at least quarterly) on the design and development process for each Privacy Sandbox API on the microsite. In particular, Google will publish a summary of common feedback themes in relation to the design and implementation of specific proposals arising from its overall stakeholder engagement.

59. As part of this commitment, the CMA would expect Google to provide insight to market participants and the CMA on how it addresses concerns that have been raised with it.

60. The CMA expects that such public reporting would give an indication of the weight of different views or suggestions made (for example, which of the issues were raised by a larger number of stakeholders). It would also include a broader description of how Google has taken account of concerns raised by stakeholders in relation to specific proposals, including explaining where it disagrees with a commonly raised suggestion.

Google's reporting to the CMA

61. Google has also committed as part of its reporting requirements to provide the following information to the CMA.

    (a) For each API (or use case, if more than one API is involved), a summary of aggregated feedback themes and a list of common feature suggestions, based on public discussions and comments on GitHub and via the W3C (or other fora).

    (b) For each API (or use case, if more than one API is involved), a summary of feedback themes and a list of common feature suggestions, based on 1:1 consultations and relevant partner discussions as well as on input to the feedback form on the dedicated microsite.

62. The CMA expects that this reporting will include whether Google has or has not incorporated specific common feature suggestions, whether they are under consideration, as well as general explanations as to why Google has rejected certain proposals.

63. More generally, paragraph 32.a. of the Final Commitments sets out the requirement on Google to provide a quarterly update to the CMA, covering points including those outlined above. The CMA expects that a non-

confidential version of these reports would be published in order to provide greater transparency to external stakeholders.

CMA's role in relation to third-party involvement

Obligations arising from the Final Commitments

64. Google has also made a series of commitments to engage with the CMA in an open, constructive and continuous dialogue. This includes facilitating engagement via the W3C and other fora.[16] The Final Commitments in practice involve the following components:

    (a) Monthly meetings between the CMA and Google up to the removal of TPCs, and at regular intervals thereafter, to discuss progress on the Privacy Sandbox Proposals.[17]

    (b) Google to proactively identify material changes to the Privacy Sandbox Proposals and without delay seek to resolve concerns raised and address comments made by the CMA with a view to achieving the Purpose of the Commitments.[18]

    (c) A power for the CMA to continue its investigation where Google does not resolve the CMA's concerns within 20 Working Days (unless extended by mutual consent).[19]

    (d) For Google to update on its plans for user controls at least quarterly, including default options and choice architecture.[20] Google will take account of any observations the CMA makes in relation to this obligation with a view to achieving the Purpose of the Commitments.[21]

CMA expectations and proposed approach to monitoring compliance with these obligations

65. The CMA envisages taking an active role in monitoring and safeguarding the effectiveness of Google's third-party stakeholder engagement, as part of the broader Privacy Sandbox development and implementation process. As noted above, the CMA sees engagement with third parties as playing an important role in informing the CMA's approach to the Privacy Sandbox development and testing, and the CMA's overall assessment of effectiveness

---

[16] Final Commitments, paragraphs 13 and 17.
[17] Final Commitments, paragraph 17.b.
[18] Final Commitments, paragraph 17.a.i.
[19] Final Commitments, paragraph 17.a.iii.
[20] This commitment also includes an obligation on Google to share any user research and testing which underpins for its decisions on user controls.
[21] Final Commitments, paragraph 17.d.

of the Privacy Sandbox tools.

66. The CMA expects that its engagement with other market participants will complement the engagement envisaged via Google's published stakeholder engagement process. This will likely involve a mix of formal and informal channels of engagement throughout. Both the CMA and Google will review their processes for stakeholder engagement on a regular basis.

Pre-standstill engagement (development)

67. Before the Standstill Period, where Google's Privacy Sandbox Proposals are being discussed and tested with market participants via relevant fora, the CMA will provide for a dedicated email inbox for stakeholders to provide their views. The intention is that this route should be available to market participants primarily for two purposes:

    (a) informing the CMA about the technical operation, or specific concerns about potential unintended consequences of, a specific proposal that could inform the CMA's ongoing assessment of proposals against the Development and Implementation Criteria; and

    (b) alerting the CMA to any failure of Google to follow its own stakeholder engagement process or take into account concerns about a specific proposal.

68. The CMA will not necessarily take action in response to each individual concern raised with it. However, it will use such evidence to identify concerns about the effectiveness of the process that should be raised with Google.

69. Where the CMA identifies any such concerns it will raise them at the next available status meeting and follow up with a notification of its concerns in writing. If Google and the CMA thereafter cannot reach mutual agreement or resolve the concerns within the period of 20 Working Days set out in paragraph 17.a. of the Final Commitments (unless extended), then the CMA may take action pursuant to section 31B(4) of the Act.

Standstill Period engagement (assessment)

70. The Standstill Period provided for in Section F of the Final Commitments offers an opportunity for the CMA to assess the effectiveness of the Privacy Sandbox Proposals individually as well as in the round against the Development and Implementation Criteria.

71. The CMA envisages that engagement with market participants during this period will likely include a range of routes to inform the CMA's overall assessment. The CMA considers that at a minimum this will involve:

    (a) consulting on Google's Privacy Sandbox Proposals to seek views from

relevant market participants; and

(b) discussions with market participants, via follow-up meetings or broader stakeholder roundtables, that respond to any CMA consultation.

72. In relation to those discussions with market participants and broader stakeholder roundtables, the CMA would seek to test evidence (both qualitative and quantitative) provided to the CMA as part of the public consultation, as well as hear views about the degree to which Google has engaged with a sufficiently broad and representative sample of likely affected stakeholders.

Post-standstill engagement (implementation)

73. If Google proceeds with removing TPCs and introducing the Privacy Sandbox Proposals following the Standstill Period, the CMA envisages that its engagement with market participants will continue to take a similar form as before the Standstill Period. This will be reviewed in light of the CMA's experience and the operational readiness of the DMU and the regime relating to competition in digital markets.