PREISKEL & CO

Preiskel & Co LLP
4 King's Bench Walk
Temple
London EC4Y 7DL
United Kingdom

[redacted]
www.preiskel.com

Competition and Markets Authority
The Cabot
25 Cabot Square
London
E14 4QZ

By email only
mobilesms@cma.gov.uk

Our Ref: TC/ADM838
3 March 2026

Dear CMA,

Re: Movement for an Open Web submission on the CMA's consultation of Google & Apple's proposed commitments relating to their Mobile Platform

We represent Movement for an Open Web ("**MOW**") in response to the consultation on commitments from Google & Apple.[1] MOW notes the CMA's 22 October 2025 designation of Google[2] and Apple[3] as having Strategic Market Status ("**SMS**") under the Digital Market, Competition and Consumers Act 2024 ("**DMCCA**").

MOW's prior filings to the CMA, and the CMA's own provisional decision report of 22 November 2024, establish that Apple and Google have caused three categories of harm to digital markets: (1) delaying innovation by rivals; (2) impairing UK economic growth; and (3) distorting competition in markets adjacent to their dominant mobile platforms. These harms are documented findings of the CMA, not allegations.

MOW's response can be summarised as follows:

(a) Given their non-compliance to date and the number of investigations and actions taken by the CMA and other authorities in relation to Apple and Google's anticompetitive behaviour that have failed to change behaviour, commitments are likely to be ineffective.

Google and Apple's actions have been the subject of numerous investigations by the CMA.[4] The CMA holds a considerable amount of evidence of non-compliance over a considerable time and is duty bound to take into account that evidence when making decisions about how to proceed. The factual background

[1] https://www.gov.uk/government/calls-for-evidence/proposed-commitments-from-apple-and-google-app-certainty-and-interoperable-access
[2] SMS decision notice 22 October 2025
[3] SMS decision notice 22 October 2025
[4] The Online Platforms and Digital Advertising Market Study (1 July 2020), which identified very "wide ranging and self-reinforcing" in these markets (including search, social media and digital advertising) but instead of making a market reference, the CMA recommended that a new regulatory approach was needed, which can tackle a range of concerns simultaneously, with powers to act swiftly.

The Mobile Ecosystems Market Study Final Report (10 June 2022), which listed the potential interventions but that many of the interventions are "well suited to the anticipated new pro-competition regulatory regime" for digital markets in the UK.

The Mobile Browsers & Cloud Gaming Final Report (12 March 2025), which found AECs in numerous markets[4] but recommended that the CMA Board should consider appropriate interventions under the DMCCA.

The CMA's opening of investigations under the Competition Act 1998 ("**CA98**") into Apple's and Google's respective app stores.

The DMCCA SMS decisions of Apple & Google's mobile platform (each dated 22 October 2025) where the CMA published a roadmap of remedies to address the issues found in the digital activities.

provoked investigations, and even after those investigations proceeded to conclusions, nothing changed in the behaviour of Apple and Google. Since neither organisation has sought to substantially change its behaviour and adopt a compliant position, it is irrational for the CMA to accept undertakings. In Annex 2, we provide evidence of recidivism and non-compliance.

(b) The factual history and context show that the businesses concerned have been aware of their non-compliance for many years, and have done nothing to change it, and the CMA has itself stated that it needed stronger legal powers to take on the task of controlling online behaviour.

See CMA statements in Annex 1 of this letter. In the light of this rationale and statements, commitments are legally an unacceptable alternative to the remedies available under the DMCCA.

(c) The CMA's acceptance of the SMS players' new process fails to discharge the obligations on the CMA to oversee and assess its own remedies.

This risks the CMA being unable to test and verify compliance in an open, transparent and fair process that takes into account the evidence of UK businesses affected by the platforms' actions. Those businesses are significantly affected and have legitimate expectations that require due process protection.

(d) Commitments are not contemplated by the DMCCA at this stage of the process.[5]

Departing from the clear obligations in that Act risks the CMA acting *ultra vires* its powers in law. It would also likely obstruct effective enforcement and set an improper precedent that undermines public trust at a time when the new regime is being tested for the first time. We note that the appointment of the CMA's new chair is also under scrutiny.[6]

(e) In addition to the undertaking being legally unacceptable, they also contain significant linguistic and technical deficiencies which make them unacceptable on their face.

We provide detailed commentary on these loopholes in Annex 3 of this letter.

Inconsistency with the aims and text of the DMCCA

The CMA being granted new powers to issue CRs under s.19 DMCCA and not utilise them is an unreasonable route to select, going against the principle of rationality:[7]

(a) commitments do not ensure that Google and Apple are unable to use their market power to continue their anti-competitive conduct,
(b) the CMA has no power in statute to enforce such commitments, and

[5] Under the DMCCA, commitments may only be accepted by the CMA (under s.36) where it has opened a conduct investigation into a suspected breach of a conduct requirement (under s.26). Such commitments are enforceable (as the undertaking "must comply with it at all times" (s.36(3)(a)) and the CMA must keep under review compliance and the need for enforcement (s.37), including by imposing penalties for non-compliance (s.85) and director disqualification (s.99).
[6] See Committee concerns on role of CMA Chair requiring risk mitigations from ministers and the pre-appointment report (26 February 2026) at https://committees.parliament.uk/work/9625/appointment-of-doug-gurr-as-chair-of-the-competition-and%E2%80%A6.
[7] Principles of reasonableness as set out in *Mandalia v Secretary of State for the Home Department* [2015] UKSC 59.

(c) this denies third parties the statutory protections and rights afforded to them under the DMCCA, e.g. to seek damages under s.101 for breach of a conduct requirement.

Inconsistency with the CMA's previous representations

Previous representations of the CMA have shown an intention to use powers under the DMCCA to impose legally binding CRs, or PCIs, on Apple and Google in relation to their app store platforms.

The CMA's closure statements in the investigations into Apple's App Store and Google's Play Store under the Competition Act 1998 ("**CA 1998**") contained dedicated sections to the 'new, more effective tools' that the CMA has under the DMCCA[8]. In both statements, only CRs and PCIs were referred to as a part of that toolkit. Similarly, in the CMA's final report of its mobile ecosystems market study in 2022[9], which included app stores, it was concluded that Apple and Google 'have a stranglehold'[10] over those key gateways. After recognising the need to prevent Apple and Google from exploiting this power[11], the envisaged powers of CRs and PCIs under the 'proposed digital regime'[12] were labelled as potentially the most appropriate mechanism to take those actions forward due to speed and their flexibility.

The CMA explains in its call for evidence that proposed commitments are a first step and that in the event of non-compliance, CRs could be adopted later. In other words, the commitments may be the start of a lengthy process and cause even further delay for remedies. This position is inconsistent with the previous representations of the CMA, which have created legitimate expectations for third parties.[13] The CMA made those statements clearly so the market is reasonably expecting either CRs and/or PCIs.

The current pro-active action of both SMS players introducing commitments risks setting a precedent that is ineffective and runs contrary to the process expected by the DMCCA when it was proposed as a law (as a form of obstruction). MOW therefore submits that the proposed non-binding commitments are insufficient to secure genuine behavioural change, and that binding CRs that incorporate rigorous monitoring and enforcement mechanisms are the minimum standard to be achieved under the DMCCA powers.

Conduct Requirements that are independently monitored, externally audited, and subject to binding dispute resolution with reference to evidence from those affected and after hearing from those affected

[8] Case closure statement – Google case, page 2, Case closure statement – Apple case, page 3
[9] Final report summary
[10] Ibid. page 1
[11] Ibid. pages 13-14
[12] Ibid. page 21
[13] In *R (Osborn) v Parole Board* [2013] UKSC 61, Lord Reed speaks about the values served by the requirements about procedural fairness.

In discussing fairness, at [71], Lord Reed states: "The second value is the rule of law. Procedural requirements that decision-makers should listen to persons who have something relevant to say promote congruence between the actions of decision-makers and the law which should govern their actions (see eg Fuller, The Morality of Law, revised ed (1969), p 81, and Bingham, The Rule of Law (2010), chapter 6)."

Bingham's 8 principles of the rule of law are:
1. The law must be accessible and so far as possible intelligible, clear and predictable.
2. Questions of legal right and liability should ordinarily be resolved by application of the law and not the exercise of discretion.
3. The laws of the land should apply equally to all, save to the extent that objective differences justify differentiation.
4. Ministers and public officers at all levels must exercise the powers conferred on them in good faith, fairly, for the purpose for which the powers were conferred, without exceeding the limits of such powers and not unreasonably.
5. The law must afford adequate protection of fundamental human rights.
6. Means must be provided for resolving, without prohibitive cost or inordinate delay, bona fide civil disputes which the parties themselves are unable to resolve.
7. The adjudicative procedures provided by the state should be fair.
8. The rule of law requires compliance by the state with its obligations in international law as in national law.

in accordance with properly defined due processes, are likely to be the minimum necessary to restore competitive conditions in UK mobile ecosystems. However, in light of the extensive non-compliance to date, no commitments should be accepted without prior testing of their effectiveness, as the CMA itself pointed out in its DAMS market study of 2020.

This submission identifies six critical areas where Apple and Google's proposed commitments are in all events insufficient to remedy the documented harms and contain definitional ambiguities that would allow Apple and Google to circumvent them:

1. **Commitments provide no market certainty and cannot be trusted.** The CMA has clearly documented its concerns about dominant firms' conduct that is distorting digital markets in its Online Platforms (2020)[14] and Mobile Ecosystems Final Reports (2022).[15] Even more clearly, after six years of CMA investigations, the lack of substantive changes in both firms' commitments to meaningfully address these concerns highlight how these SMS firms are using all efforts to delay implementing actual remedies to the ongoing harms their conduct is causing on competition within digital markets.
2. **Adjacent business to business ("B2B") service coercion.** Apple and Google abuse their coordinated platform dominance to lock developers into services such as proprietary real-time communication standards, payment processing, advertising attribution, and analytics services. Remedies to these issues are vital.
3. **Interoperability must extend to use of the open web.** Both firms' interoperability commitments address only the request process. They continue to restrict use of the open web, especially for real-time communication that publishers and developers need for advertising.
4. **"Privacy" must be objectively defined under UK law.** Both Apple and Google have a long and well-documented history[16] of invoking undefined and overbroad "privacy" justifications for their restrictions on rivals that primarily serve commercial rather than data-protection purposes. Any remedy that leaves "privacy" and "security" undefined gives Apple and Google a self-issued licence to continue their anticompetitive conduct. The CMA's own provisional decision report identifies this circumvention risk as high.[17]
5. **Fair ranking must cover B2B service choice.** App ranking commitments must explicitly prohibit ranking signals, direct or through proxies, that advantage apps using Apple's or Google's own B2B services over apps using alternative, third-party equivalents.
6. **Monitoring must be output-based, independent, and continuous.** Bi-annual self-reported attestations and complaint-volume metrics will not detect or deter the identified harms. The CMA needs daily output data, an independent technical monitor, and a pre-implementation notification mechanism for material platform changes.

[14] CMA, Online Platforms Final Report (1 July 2020). https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report
[15] CMA, Mobile ecosystems market study final report (10 June 2022) https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report
[16] See for example the USA vs Apple DOJ pleading that refers to Apple's overbroad claims for privacy as an "elastic shield" that covers its activities for its commercial convenience and the DMA provisions which were debated in the EU parliament where the overbroad claims for undefined "privacy" protections were robustly rejected. Indeed the same approach to the one we see here was the first position of Google in its response to the CMA on its Privacy Sandbox case in early 2021 when Google sought to claim that undefined "privacy" should excuse a broad swath of its behaviour. It eventually acceded to GDPR as the basis for the definition of privacy in that case.
[17] SMS Proposed Decision into Apple's Mobile Platform (23 July 2025), Para 11.128, 11.203. https://assets.publishing.service.gov.uk/media/68811f9c3f77077624120561/Proposed_decision.pdf.

We thank the CMA for considering this submission.

We remain available should the CMA have any questions and would welcome a meeting to discuss the attached.

Yours faithfully,

Preiskel & Co LLP

(Annex 1 to 3 follow on the next page)

Annex 1 – Timeline of CMA Market Studies / Investigations

- **1 July 2020**: The Online Platforms and Digital Advertising Market Study
  - The problems identified in these markets are wide-ranging and self-reinforcing (including in search, social media and digital advertising).
  - Instead of making a market reference, the CMA recommended that a new regulatory approach was needed, which can tackle a range of concerns simultaneously, with powers to act swiftly.

- **3 March 2021:** The CMA opens investigation into Apple App Store under the Competition Act 1998 ("**CA98**").
  - The CMA can give directions as it considers appropriate to bring the infringement to an end (s. 33, CA98). Schedule 8, Enterprise Act 2002 lists the provisions that enforcement orders can contain.

- **15 June 2021:** The CMA launches a market study into mobile ecosystems within 4 broad themes (incl. mobile apps).

- **10 June 2022:** Mobile Ecosystems Market Study Final Report – See Chapter 8 – Potential Interventions.
  - There is "*a strong case for interventions*" to open up competition and address the harms.
  - Many of the interventions are "*well suited to the anticipated new pro-competition regulatory regime*" for digital markets in the UK. The CMA will continue to support the government in establishing the regime.
  - The CMA heard from many stakeholders about the "*wide-ranging benefits which would come from these market opening measures*".

- **10 June 2022:** The CMA opens investigation into Google's distribution of apps on Android devices in the UK under traditional competition rules.

- **21 August 2024:** The CMA closes the CA98 cases against Google and Apple.
  - *"The DMCC Act provides the CMA with new, more effective tools to address barriers to competition in digital markets."*
  - The CMA is mindful that:
    - enforcement under the Competition Act would, if progressed, potentially take a significant period of further time, involving the issuance of a statement of objections and consideration of representations from Apple before a final decision could be taken;
    - the directions at the end of the finding of infringement is limited to a specific conduct (cannot take into account Apple's wider activities in mobile ecosystem markets); and
    - the CMA will soon have the option to consider firms' conduct in digital markets under the DMCC Act framework instead.

- **12 March 2025:** the Mobile Browsers & Cloud Gaming Final Report

- Found AECs in numerous markets (see chapter 10) but recommended that the CMA Board should consider appropriate interventions under the DMCCA (see chapter 11 and Appendix D).

- **July 2025:** The CMA publishes a roadmap of remedies to address the issues found in Apple and Google's mobile platforms under the DMCCA.

- **22 October 2025:** The CMA designates Google & Apple as having strategic market status under the DMCCA **[1 year after the CA98 case closures].**
  - No remedies in force yet but the CMA provides an expectation of using powers of imposing conduct requirements:

    Para 4.157: the CMA considers *"that treating the four activities as a single digital activity will have benefits when the* ***CMA considers potential conduct requirements****, insofar as these might pursue an overarching goal of promoting greater competition such that UK app developers and innovators developing and distributing content via Apple's Mobile Platform are able to innovate and grow their businesses."*

- **10 February 2026:** The CMA consults on Apple & Google's proposed commitments under the DMCCA.
  - The "*CMA has moved swiftly to secure a package of commitments from Apple and Google*" (see press release).
  - It is clear from the CMA's 'Call for evidence' that the proposed commitments are not legally binding. Non-compliance itself does not carry legal consequences.
  - Commitments are not available at this stage of the process under the DMCCA. The CMA has not used the powers available under the DMCCA.

Annex 2 – History of Google & Apple's non-compliance

[redacted] As a result, a precedent of regulators using commitments to secure compliance, only for them to fail, is well-established.

Google

In particular, Google has been characterised as a multi-recidivist in an open debate at the European Parliament,[18] by Valentina Palmisano MEP and Stéphanie Yon-Courti MEP. This pattern of deliberate non-compliance is evidenced, among other instances, by Google's behaviour in the *Google Shopping proceedings*, where it failed to adhere to remedies imposed by the European Commission.[19]

This pattern of deliberate non-compliance and evasion is also evident in United States litigation, where Google is regularly accused of violations in relation to the disclosure of evidence and the creation of an "environment of concealment".[20]

By way of example:

- It has to be appreciated that Google is now one of the world's most fined companies for non-compliance with antitrust law, with EU fines only being available for deliberate breach of the law and amounting to over €9 billion.[21]

- In *Epic Games v. Google,*[22] Judge James Donato described Google's actions in relation to evidence suppression and destruction as "*a frontal assault on the fair administration of justice*"[23] and "*the most serious and disturbing evidence I have ever seen … with respect to a party intentionally suppressing relevant evidence*,"[24] highlighting its systematic obstruction of due process.

- In *USA v Google (AdTech) [2023],*[25] Judge Leonie Brinkema observed that "*Google's systematic disregard of the evidentiary rules regarding spoliation of evidence and its misuse of*

[18] "Multirécidiviste": Valentina Palmisano and Stéphanie Yon-Courtin – European Parliament 20 October 2025

[19] In the European Commission's Google Shopping investigation (Case AT.39740), Google was required to give rival comparison shopping services equal treatment in search results, including unbiased presentation and fair participation mechanisms. Despite these formal obligations, Google implemented an opt-in auction system and subtle interface changes that technically complied with the remedies but continued to favour its own services, preserving its market advantage. This episode exemplifies Google's pattern of circumventing regulatory obligations by adhering to the letter of imposed requirements while undermining their intended effect, demonstrating the risk that Conduct Requirements without robust monitoring and enforcement may fail to produce genuine behavioural change.: Connexity and others v Google – Judgment (Preliminary Issues) see also https://techcrunch.com/2024/11/20/duckduckgo-calls-for-eu-to-widen-its-digital-markets-act-probe-of-google/

[20] How Google Spent 15 Years Creating a Culture of Concealment – The New York Times

[21] The European Commission has fined Google in Google Shopping (€2.42 billion fine), Android (€4.34 to €4.12 billion), AdSense (€1.49 billion) (although this case is currently under appeal to the European Court of Justice) and Ad Tech (€2.95 billion)

[22] *Epic Games, Inc. v. Google LLC*, No. 24-6256 (9th Cir. July 31, 2025)

[23] The curious case of Epic Games: how the developer beat Google but not Apple - The Guardian; Federal judge vows to investigate Google for intentionally destroying chats - The Verg; Judge deciding Google's fate in Epic case is antitrust veteran - Reuters

[24] *Ibid.*

[25] *United States et al. v. Google LLC*, No. 1:23-cv-00108 (E.D. Va. Jan. 24, 2023).

the attorney-client privilege may well be sanctionable"[26], emphasising that Google's document-management practices undermined trust in its representations.

- In *USA v Google (Search) [2020],*[27] Judge Amit P. Mehta observed that "*Google…trained its employees, rather effectively, not to create "bad" evidence*."[28] He noted that "*the court is taken aback by the lengths to which Google goes to avoid creating a paper trail for regulators and litigants*"[29] and "*as a result of Google's chat deletion policy, "years' worth of chats—likely full of relevant information—were destroyed" and thus never subject to regulatory scrutiny*."[30]

- In the same *USA v Google (Search) [2020]* case, in a memorandum in support of the plaintiffs' motion to sanction Google and compel disclosure of documents which Google unjustifiably claimed were attorney-client privileged: "*As part of Google's larger efforts to shield documents from production, Google employees were expressly directed to add artificial indicia of privilege on all written communications relating to the exclusionary search-distribution agreements at the heart of Google's monopolies." Google's employees followed the Communicate-with-Care training, routinely adding in-house counsel to business communications, affixing privilege labels, and including pretextual requests for legal advice when no advice was actually needed, sought, or thereafter received. In these email chains, the attorney frequently remains silent, underscoring that these communications are not genuine requests for legal advice but rather an effort to hide potential evidence.*"[31]

- In France, after ordering interim measures in the form of injunctions in April 2020 (Decision 20-MC-01 of 9 April 2020)[32], the *Autorité* found that Google had not complied with these injunctions and imposed a fine of €500 million, as well as ordering Google to comply, under penalty payment, with the initial injunctions (Decision 21-D-17 of 12 July 2021).[33]

- In 2010, in the UK, the UK data protection authority, the Information Commissioner's Office ("**ICO**") ordered Google to delete personal data obtained from its Street View cards from open WiFi networks. Google later admitted that it did not erase the data by mistake, data which could include millions of emails and passwords. Google did not comment regarding the moment when they realised they had not deleted all the data. Nick Pickles, director of privacy at the pressure group Big Brother Watch, said: "*Given that Google failed to respect people's privacy in the first place and subsequently failed to adhere to its agreement with the information commissioner, serious questions need to be asked to understand why Google seemingly sees itself as above the law*."[34]

---

[26] Ibid. Memorandum Opinion. Page 114
[27] *United States v. Google LLC*, No. 20-cv-3010, 2024 WL 3647498 (D.D.C. Aug. 5, 2024).
[28] Ibid. Page 275
[29] Ibid pg. 275
[30] Ibid pg. 273
[31] Memorandum In Support Of Plaintiffs' Motion To Sanction Google And Compel Disclosure Of Documents Unjustifiably Claimed By Google As Attorney-Client Privileged (21 March 2022) available at https://www.justice.gov/atr/case-document/file/1577876/dl?inline. See also Sidley Austin's release on this at https://www.sidley.com/en/insights/newsupdates/2022/04/doj-accuses-google-of-intentionally-misusing-privilege-to-hide-sensitive-documents
[32] https://www.autoritedelaconcurrence.fr/en/decision/requests-interim-measures-syndicat-des-editeurs-de-la-presse-magazine-alliance-de-la
[33] https://www.autoritedelaconcurrence.fr/en/decision/compliance-injunctions-issued-against-google-decision-20-mc-01-9-april-2020
[34] https://www.standard.co.uk/panewsfeeds/google-ordered-to-hand-over-data-7982341.html

- In the EU *Google Shopping* case, Google was permitted to propose a remedy under Article 9. The resulting design relied on auction mechanisms that, on paper, appeared neutral and non-discriminatory. However, in practice, the remedy failed and is now under investigation for non-compliance under the Digital Markets Act 2022 self-preferencing obligations.[35] Independent evaluations found that the auction design imposed additional costs on rivals, while Google's own services benefited from structural advantages in traffic, brand recognition, and integration with general search. Organic demotion of competitors persisted, traffic flows did not shift meaningfully, and no meaningful competitive entry occurred.

- Google often resists any disclosure or searching of documents from senior executives and their document repositories. In one of the UK private actions against Google further to the *Google Shopping* case, the claimants highlighted that many documents refer to the strategy of demoting comparative shopping sites, but the strategy document itself is not disclosed nor any documents from senior executives have been searched / included in the disclosure.[36]

- Google protects all disclosure by creating image files that are difficult to search but then claims that it has technically complied with the disclosure orders and the provision of searchable documents being visible for inspection.[37] It uses a combination of image and TIFF and text files to prevent parties from being able to effectively inspect evidence.

- Google often uses "GoogleSpeak" that confuses non-Googlers. Internal documents reference project codenames (often Star Wars related such as "Project Jedi" after Jedi Blue) or with a tangential relationship to a subject. Product names are also changed regularly which makes tracking them over time difficult in terms of search terms or for document investigations spanning different product time periods.

- In the EU *Android* case, to address foreclosure arising from preinstallation and default search settings, Google introduced a "choice screen" intended to allow users to select alternative search engines. Empirical assessments, however, showed that the intervention produced less than a one percent shift in market share.

- More recent experience can be seen from the EU's Digital Markets Act 2022. Under Article 6(11), Google was required to share search click, query, ranking and view data with competitors. Google implemented this obligation by imposing thresholds that excluded over 99 percent of queries from the shared dataset. At a remedies workshop, DuckDuckGo tested these thresholds on its own data and extrapolated the effect to Google's scale, concluding that the resulting dataset would be commercially useless. As one participant summarised: "*We see Google trying to make sure whatever they put forward is as useless as possible for competitors*."

- The Digital Markets Act 2022 documents these dynamics step by step, demonstrating how Google preserves disproportionate advantages "*in the structure, design, function, and manner of operation*" of operating systems and app distribution layers. Crucially, these practices are

[35] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_811
[36] See Kelkoo & Others v Google UK Ltd & Others case management conference of 26 July 2023, in particular, page 61
[37] Skimbit Ltd & Others v Google & Others in the UK Competition Appeal Tribunal regarding damages following Google Shopping. See transcript of case management conference dated 18 July 2025 where references are made to Google's hyperlinks in documents not working and thus lacking the relevant document metadata (see pages 50 to 52) and that Google discloses documents in TIFF format for security reasons in all worldwide proceedings in this format (see page 45)

often compatible with a literal reading of the obligations, while clearly violating their economic intent. As a result, significant non-compliance investigations were opened within months of the DMA's entry into force.

[redacted] Whether before regulators or courts, Google's approach to compliance has been marked by concealment, selective disclosure, and the calculated erosion of oversight mechanisms. This entrenched behaviour demonstrates that formal undertakings alone are insufficient to secure genuine compliance. Any regulatory framework must therefore be designed on the assumption that Google will seek to circumvent its obligations unless subject to continuous and independently verifiable enforcement.

Apple

In terms of cases against Apple, despite the requirement on the gatekeeper to ensure compliance, the European Commission found Apple to be in breach of the Digital Markets Act regarding Apple's steering terms (one of the first non-compliance decisions under the DMA).[38] In the *USA v Apple* proceedings, Apple has substantially delayed document production, seeking multiple-month extensions.[39]

Conclusions

Within the proposed commitments, the 'complaints mechanisms'[40], 'public reporting'[41], and 'reporting to the CMA'[42] mechanisms are controlled and conducted by Apple and Google themselves, and therefore lack the necessary independence. To secure tangible behavioural change from Apple and Google, legally binding CRs that incorporate independent monitoring, verification, and enforcement mechanisms must replace the proposed non-binding commitments. To do any less would leave the CMA at risk of adding to the precedent of non-compliance. MOW therefore submits that non-binding commitments will be insufficient to account for the repeated recidivism of these dominant platforms.

[38] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085
[39] For example, see joint letter dated 12 December 2025 where Apple seeks an extension for document production from 26 January 2026 to 15 June 2026 https://storage.courtlistener.com/recap/gov.uscourts.njd.544402/gov.uscourts.njd.544402.351.0_1.pdf
[40] Call for evidence paragraph 48
[41] Call for evidence paragraph 50
[42] Call for evidence paragraph 56

PREISKEL & CO

Annex 3 – Detailed comments on the proposed Commitments and the Loopholes

Table of Contents

Part 1: Market Context: The Anti-Competitive Harms the Commitments Must Remedy

1.1 The DMCC Act and the SMS Designation

The Digital Markets, Competition and Consumers Act 2024 ("**DMCC Act**") represents the most significant expansion of the Competition and Markets Authority's powers in a generation. For the first time, the CMA has statutory authority to designate specific firms as having Strategic Market Status ("**SMS**") in specific digital activities, and to impose Conduct Requirements ("**CRs**") with the force of law, enforceable by financial penalties of up to 10% of global annual turnover and by direct CMA intervention, rather than relying on undertakings that depend on the designated firm's continued goodwill.

Both Apple and Google have been designated as SMS firms in relation to mobile ecosystems: Apple in respect of iOS and iPadOS, and Google in respect of Android and the Google Play Store. The CMA's Roadmap, published July 2025, identified a portfolio of concerns spanning app distribution, browser engine restrictions, payment systems, interoperability, real-time communication, and emerging AI services. These are not new concerns. Versions of them have occupied regulators in the EU, United States, Japan, South Korea, and Australia for the better part of a decade. In each jurisdiction, remedies have proven inadequate to restore competitive conditions.

The DMCC Act gives the CMA the tools to do better. The question this submission addresses is whether the commitments offered by Apple and Google represent an adequate substitute for the enforceable CRs the Act empowers the CMA to impose, or whether accepting those commitments would squander the most important regulatory opportunity the UK digital sector has seen.

10% *of global turnover max DMCC Act penalty per breach*	**95%+** *of UK smartphones run iOS or Android — the designated platforms*	**£1.5tn+** *combined estimated market cap of Apple and Google*	**7+** *jurisdictions where mobile remedies in the form of "commitments" proved insufficient*

1.2 The Revenue-Sharing Duopoly and Its Effect on Competition

The CMA's provisional decision report finds that Apple and Google hold a "*de facto duopoly*" in mobile operating systems[43] and that both firms hold dominant shares in mobile browsers exceeding 90%: Safari at 88% on iOS and Chrome at 74% on Android.[44] This position is maintained not merely through alleged product "quality" but through interlocking commercial arrangements that suppress competition.

The single most consequential commercial arrangement is the revenue-sharing agreement (known as the "**ISA**") between Apple and Google, under which Google pays Apple >$20 billion annually to be the default search provider on iOS. The CMA found this sum to be a "*significant percentage of its net advertising revenue from traffic that takes place via Safari and Chrome.*"[45] Critically, the CMA found

[43] https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report/interim-report
[44] Mobile ecosystems Market study final report (10 June 2022), Table 5.2: 2021 UK mobile browser and browser engine share of supply by operating system.
https://assets.publishing.service.gov.uk/media/63f61bc0d3bf7f62e8c34a02/Mobile_Ecosystems_Final_Report_amended_2.pdf
[45] SMS Proposed Decision into Apple's Mobile Platform (23 July 2025), Para 6.50.
https://assets.publishing.service.gov.uk/media/68811f9c3f77077624120561/Proposed_decision.pdf

the scale of this revenue sharing "significantly limits the financial incentives for Apple and Google to compete" with each other, while simultaneously meaning that rival browser vendors "*state that the agreements that allow Google to achieve default status are not financially viable for them*."

CMA Finding: CMA, Provisional Decision Report (22 November 2024), paragraphs 30–31 and 9.4: The revenue-sharing agreements between Apple and Google are "so large" as to limit their "financial incentives to compete." Rivals cannot afford to pay for equivalent default status and pre-installation thereby largely foreclosing distribution access.

This revenue-sharing arrangement is not incidental to the CMA's competition concerns. This is central to it. Apple and Google senior executives have privately described their commercial relationship as working "*as if we are one company*." This coordination is the commercial foundation on which all of the other restrictive policies identified in this submission rest.

1.3 Mobile Platform Scope and Bundling of Business Services

The CMA's scope of "Mobile Platforms" includes: operating systems, native app distribution, mobile browsers and mobile engines. Yet, there are adjacent products and services that rely on the supporting framework and hardware access of this Mobile Platform. We are concerned that the CMA does not fully take into account Apple and Google's anticompetitive bundling of their adjacent services into the operating system or browser platforms in ways that are not intrinsic to the OS's core purpose of facilitating software-hardware interaction and the impact of this conduct on rival content and service providers.[46]

The adjacent product and services (e.g., payment processing, advertising solutions like attribution, and broader generative AI services) could be provided separately and would benefit from competition. Apple's and Google's exclusionary preinstallation of defaults harms competition. It prevents and limits the opportunity for consumers to have a choice and restricts rivals from this cost-effective channel of distribution.

The CMA should recall that the underlying rationale for imposing obligations on any business under the DMCCA is that technology platforms, like telecoms networks, generate increased market power through their broad economies of scale, scope and network externalities. This means that any short-term efficiency savings for consumers from platforms enhancing their products can contribute to the enhancement of monopoly and the entrenchment of the platform's market power. In making the assessment of consumer benefit to be gained from claimed efficiencies for the platform, the CMA needs to assess the harm to the market that would have arisen in the counterfactual. For example, where a platform proposes that its bundling of products creates convenience, the CMA needs to consider the significant harm to innovation and competition that arises from the suppression of competition and the market. It is theoretically obvious that innovation losses from bundled products are very significant economically. Innovation over a single product that is integrated into a platform, and which precludes the hundreds or thousands of other products that could address the same or similar needs, manifestly reduces choice, competition and innovation by rivals.[47] An innovation theory of harm has been accepted.

[46] CMA's Proposed Decision on Strategic Market Status Investigation into Apple's Mobile Platform, page 33-34, para 4.38-4.33. https://assets.publishing.service.gov.uk/media/68811f9c3f77077624120561/Proposed_decision.pdf

[47] CMA, Provisional Decision Report (22 November 2024), paragraph 3.71. https://assets.publishing.service.gov.uk/media/67406fe502bf39539bdee865/Provisional_decision_report2.pdf

The CMA correctly identifies that Apple and Google have used their control over mobile operating systems and browsers to disadvantage rival developers, content producers and B2B solution providers. The mechanism of harm is not only directed to pre-installation and defaults. Instead, it is the systematic use of platform policies and technical restrictions to shift developers' and publishers' commercial relationships from open web standards to Apple's and Google's proprietary ecosystems, where they become subject to mandatory commercial terms they would not accept in a competitive market.

The CMA's provisional report noted that "*the benefit of building a web app or website as opposed to a native app was that developers only had to build once, rather than build separate apps in separate code for different Apple and Android devices.*"[48] Apple's restrictions on alternative browser engines, its limitations on web app functionality, and its interference with open web standard communication have systematically degraded this competitive alternative, unfairly funnelling developers and publishers into Apple's App Store and its associated mandatory payment processing commission of up to 30%.

CMA Finding: CMA, Provisional Decision Report (22 November 2024), paragraph 4.78: "*Web developers have raised that, as a result of Apple's control of the iOS operating system, it is able to hold back the development of web apps as a method of users accessing content, meaning that developers are less likely to focus their efforts on developing web apps compared to native apps through the Apple App Store.*"

Part 2: The Proposed Commitments Are Insufficient

2.1 Apple's and Google's Commitments Emphasize Process Without Outcomes

Apple's commitments, dated 10 February 2026, address four areas:

1) App Review process,
2) App Store search results,
3) Apple's use of third-party data collected through App Review, and
4) the transparency of its interoperability request process.

Each commitment is carefully drafted to appear substantive while remaining functionally self-referential. For example, Apple states it will ensure processes are "*fair, objective and transparent,*" but retains control over defining each of these terms and how Apple will choose to unilaterally evaluate its own conduct against them. Apple promises it will conduct internal evaluations and self-certify their outcomes. Its App Review Board, an Apple's controlled body, is offered as the only mechanism for appeals against Apple's unilateral decisions. Apple suggests it will review interoperability requests, but retains absolute discretion to refuse them all. Apple's commitment expressly states that receipt of a request creates no obligation to act.

The architecture of the Apple commitments is process without outcome, transparency without accountability, and consultation without obligation. Not one of the four areas addressed involves an external adjudicator, an independent technical audit, a binding decision timeline, or a substantive limit on Apple's freedom of action.

[48] This is the reason why basic competition law such as TFEU ART 102 outlaws bundling by dominant firms.

And the four areas discussed also represent only a fraction of the SMS concerns the CMA identified. App Store commissions, browser engine restrictions, alternative app distribution, anti-steering provisions, NFC access, digital wallets, AI integration, and choice architecture are entirely absent. Google's position is starker still: no commitments have been offered across any of the corresponding concern areas for Android and the Play Store.

The amended complaint in *USA v Apple* also observed this where Apple denies access to digital wallets, messaging apps, third party devices and super apps.[49] Apple proposes "interoperability" commitments but does not address these issues.

The table below illustrates a combined picture that is best characterised as strategically minimal. In areas where commitments were offered, they are self-policing. In the areas causing the greatest harm to competition - distribution monopoly, excessive payment extraction, browser engine control, anti-steering - both Apple and Google offered nothing or materially and substantively incomplete remedies to their ongoing abusive conduct.

Area of Concerns	Apple's Offered Commitments	Google's Offered Commitments
Distribution & Discovery		
App Review / Play Store Listing	*Materially & Substantively Incomplete* "Fair and objective" is self-evaluated with self-certified compliance. No external audit of review decisions. No firewall as all staff remain Apple employees incentivized to maximize Apple revenues and competitive success over rivals. Reporting is self-prepared; the CMA cannot independently verify. Guideline changes can take effect on the same day they are announced (no advance transition period).	*Materially & Substantively Incomplete* "Fair and objective" is self-evaluated with self-certified compliance. No external audit of review decisions. Reporting is self-prepared; the CMA cannot independently verify. A CEDR mediation outcome is not binding on Google.
Browser Engine Restrictions	*Silent & no commitment offered.* WebKit requirement (App Review Guideline 2.5.6) forces all iOS browsers to use Apple's rendering engine, eliminating genuine browser competition. For example, Chrome on iOS remains WebKit with Chrome's UI, not Chrome's engine. The CMA's Roadmap listed browser engine interoperability as a Category 1, first-half of2026 priority intervention.	*Materially & Substantively Incomplete* Although Google allows other browser engines in Android, Chrome's dominance through pre-installation and GMS bundling on Android devices is not addressed. The advantage of Chrome's deep Android integration is left untouched.

[49] https://www.justice.gov/atr/case/us-and-plaintiff-states-v-apple-inc

Alternative Distribution / Sideloading	*Silent & no commitment offered.* Apple's App Store retains a complete monopoly over iOS app distribution under these commitments. The Core Technology Fee ("**CTF**"), a per-install charge deterring alternative marketplace operators, is not addressed. The CMA's Roadmap identified alternative distribution as a Category 1 concern. Apple's DMA "compliance" response in the EU deployed the CTF as a deterrent; the CMA receives no commitment that equivalent deterrence will not be used in the UK.	*Silent & no commitment offered.* Google's commitments are scoped entirely to the Play Store and do not address alternative app distribution or sideloading policies. Android technically permits sideloading, but Google's GMS licensing terms and OEM agreements create barriers that affect market structure. Google imposes friction on sideloading (warnings, permission flows) that are not addressed.
Commissions and Revenue Share	*Silent & no commitment offered.* Apple's mandatory IAP at up to 30% commission is the single largest B2B coercion mechanism identified by the CMA — entirely unaddressed. The Competition Appeal Tribunal found Apple's commission rates excessive and anti-steering restrictions unlawful (October 2024 judgment, under appeal). The Apple-Google ISA — worth >$20bn annually — which the CMA found 'significantly limits financial incentives to compete' receives no commitment.	*Silent & no commitment offered.* No commitment offered on commission rates, revenue share, or the terms of Google Play Billing as a condition of app distribution. The ISA, by which Google pays to Apple a material portion of Apple's net revenue, is the commercial foundation of the mobile duopoly. The CMA found it forecloses rival search engines from default status. There is no commitment from Google to limit or cap these payments.
Anti-Steering Provisions	*Silent & no commitment offered.* Developers remain prohibited from: using alternative, third-party in-app payment processors; communicating that lower prices are available elsewhere; including links to their own websites for purchases; and telling users App Store prices include Apple's commission. The EC found Apple non-compliant under the DMA on anti-steering. The US District Court in *Epic v. Apple* (April 2025) required Apple to permit external purchase links. Apple's UK commitments are entirely silent.	*Silent & no commitment offered.* No commitment offered. Google's policies restricting developers from directing users to alternative payment methods or disclosing pricing differentials are not addressed.
Search / Algorithmic Neutrality	*Materially & Substantively Incomplete* No prohibition on ranking signals correlated with adoption of Apple's own B2B services (Apple Search Ads/SKAdNetwork, IAP, Apple Pay). "Quality" is left undefined and is self-assessed. No independent algorithm audit, and bi-annual reports are self-prepared.	*Materially & Substantively Incomplete* Self-assessed; no independent audit. No independent algorithm audit. "Quality", "relevance", and "user experience" are undefined and self-assessed. No prohibition on ranking signals correlated with adoption of Google's own B2B services (Firebase, Google Ads, Play

	One week's advance notice only is provided for "major" changes, which is also self-defined by Apple. Algorithm weighting and logic are not required to be disclosed. No obligation to disclose whether Apple Search Ads spend influences organic ranking. No external auditor with access to training data or algorithm.	Billing). "*Ad spend is not a criterion*" does not address whether Firebase analytics adoption or Google Ads usage correlates with ranking outcomes. No obligation to disclose algorithm weighting.
Interoperability		
Interoperability Requests	*Materially & Substantively Incomplete* Receiving a request "*will not create any obligation or expectation that Apple will commit to building a specific requested feature*." Apple retains absolute discretion to refuse all requests. Assessment criteria include "alignment with Apple's platform priorities" and "impact on Apple's intellectual property rights"' - both of which are Apple-emphasized veto conditions. Scope is limited to process transparency. No independent appeals panel. Status "update" is not a substantive decision and there is no expectation on any decision deadlines. Scope of appeal is offered to a restricted set of developers, excluding many global developers who supply UK residents and businesses with valuable services. No commitment on supporting open web standards as alternatives to Apple's proprietary real-time communication protocols.	*Silent & no commitment offered.* No commitment on supporting open web standards as alternatives to Google's proprietary real-time communication protocols. GMS licensing and the mandatory bundling of Google services (Chrome, Search, Maps, Play) with Android OEM access creates interoperability barriers. Third-party services requiring GMS API access are entirely dependent on Google's goodwill. No commitment to a formal interoperability request channel, published criteria, or independent assessment.
NFC / Contactless Payment Access	*Silent & no commitment offered.* The European Commission reached a commitments decision with Apple on NFC access in 2024 following a finding of abuse of dominance. The CMA Roadmap identified digital wallets and NFC access as a priority intervention area. Apple's commitments do not address NFC access, Secure Element access, or Host Card Emulation access for third-party payment and wallet apps. UK developers remain entirely dependent on Apple's (lack of) goodwill.	*Materially & Substantively Incomplete* Unlike Apple, Android's NFC stack is more open by design, but Google Pay / Google Wallet enjoy structural advantages through deep OS integration and GMS bundling. Google's commitments do not address whether Google Wallet's integration leads to an advantage over alternative, third-party digital wallets, which constitutes preferencing.

AI / Voice Assistant Integration	*Silent & no commitment offered.* Siri's deep iOS integration and default routing to Apple first-party apps (Maps, Music, Messages, Wallet) disadvantages rival apps in the same categories. Apple Intelligence on-device AI processing and notification summarisation applies preferentially to Apple's own services. The CMA flagged AI as a forward-looking concern area in its Roadmap. Apple's commitments are entirely silent.	*Materially & Substantively Incomplete* Google's broader Generative AI services (e.g., Assistant and Gemini) enjoy deep Android OS-level integration unavailable to rival AI assistants on equivalent terms. Default voice assistant settings, intent routing, and Android's AI feature stack (on-device Gemini Nano) structurally discriminates and advantages Google's own AI services. The CMA flagged AI as a forward-looking concern area. Google offers nothing.
Data Use		
Market and Rivals' Data Protections	*Materially & Substantively Incomplete* Scope limited to only "*data submitted as part of App Review*", excluding necessary coverage for broader App Store operational data (transactional data, user behaviour, commercial intelligence) used to inform Apple's first-party product strategy. "Legal review" is conducted by Apple's own compliance personnel with no independent data auditor. No self-reporting obligation to the CMA upon discovery of a breach. No remediation protocol for affected developers. DPLA Section 9.3 is retained; only a negative obligation not to misuse it.	*Materially & Substantively Incomplete* All controls are internal with no independent data auditor with system access. No obligation to self-report breaches to CMA upon discovery. "Non-public Play data" is narrowly scoped to app review and Play operation data; does not explicitly cover commercial intelligence derived from Play Store transaction patterns or user behaviour across Google's integrated services. Annual attestation is self-prepared. The CMA cannot independently verify access logs.

2.2 Why Commitments Cannot Restore Competition

The inadequacy of both firms' commitments is not primarily a matter of missing detail. It is fundamental. A commitment made by a firm with SMS operates under a central tension: the firm is asked to constrain its own exercise of the market power the SMS designation has found it holds. The incentive to defect from any genuinely constraining commitment is proportionate to the commercial value of the power at stake. For Apple, App Store commission revenues alone are estimated to exceed $20 billion annually. For Google, Play Store revenues and the advertising dependency created by Android's default-setting architecture represent comparable commercial significance.

Against that economic backdrop, three central deficiencies make commitments inherently insufficient in SMS contexts, regardless of drafting quality.

First: self-definition and certification of compliance. Both Apple's and Google's commitments define the substantive obligations against which their own conduct is to be assessed, their App Review Guidelines and Play Policies respectively, using language that they control and can amend unilaterally. A commitment to comply with one's own rules, applied by one's own staff, reviewed by one's own appeal board, and summarised in one's own annual self-certification, is not a constraint.

Second: the absence of any independent verification. Across all commitments offered by both firms, there is no independent monitor with access to internal systems, no external technical audit of algorithmic outputs, no independent adjudicator for developer disputes, no obligation to report breaches, and no external source of evidence such as impact on competition or competitors against which the effectiveness of remedies can be adjudicated by the party that is responsible for making that assessment, which is the CMA. The CMA's assessment is limited to reviewing reports prepared by the firms themselves — creating a significant problem where compliance cannot be distinguished from non-disclosure.

Third: scope capture. By offering commitments on peripheral process questions (e.g., App Review transparency, request process reporting rather than outcome reporting), both firms have proposed these commitments are adequate to rectify the totality of the CMA's identified concerns. This seeks to prevent the CMA from adopting real remedies in meaningful timeframes. The firms' commercial interests are greatly served by such a deferral. The ongoing competitive harm to developers, consumers, and the broader digital economy accrues throughout it.

Circumvention risk: The EU's experience under the Digital Markets Act is instructive: Apple's initial DMA implementation on alternative app distribution was arguably formally compliant but practically defective, deploying a Core Technology Fee and contractual burdens that neutralised any competitive effect. The CMA must draft CRs that close the implementation gap, not merely the headline prohibition.

The CMA faces a binary choice. If it were to now accept commitments as an adequate response to the SMS designations, nothing will change in the UK. UK businesses will continue to be adversely affected and abused. Those in the EU will be protected by EU enforcement actions; see for example the enforcement that is taking place in France[50].

A MOW Counter proposal?

We propose an alternative approach: Proposed Conduct Requirements set out, in legally precise and technically grounded terms, what effective CRs in each of the fifteen principal concern areas should contain. They are offered as a framework for the CMA's own CR development, with the aim of ensuring that the UK's flagship digital markets legislation delivers, in practice, the competitive conditions its passage promised.

Part 3: Apple and Google's Bundling of Business Services Remain Unaddressed by Commitments

Beyond the gaps in the areas they nominally address, both firms' commitments are entirely silent on the coercion of digital market players via their default bundling of business services. Apple and Google use coordinated platform dominance to lock developers into proprietary communication protocols, payment processing, advertising attribution, and analytics services. The mechanism is the systematic use of platform policies and technical restrictions to make open web standards commercially unviable, forcing developers to accept Apple's and Google's mandatory commercial terms.

[50] https://techcrunch.com/2024/03/20/google-hit-with-270m-fine-in-france-as-authority-finds-news-publishers-data-was-used-for-gemini/#:~:text=GenAI%20training%20in%20the%20frame.%20Today's%20enforcement,or%20the%20Authority%2C%E2%80%9D%20per%20its%20press%20release.

3.1 Apple's In-App Payment Mandatory Commission

Apple's App Store Guideline 3.1.1 requires that any app offering digital goods, content, or subscriptions to UK consumers must use Apple's own In-App Purchase ("**IAP**") system. Apple levies a commission of up to 30% on all transactions processed through IAP.

Alternative payment processors, which would reduce developer costs and could offer consumers better pricing, are not permitted on equal terms. Publishers such as Spotify, who built their audience relationships via web browsers, have been progressively coerced into the App Store ecosystem and its mandatory fees because Apple's deliberate degradation of open standard web communication functionality on iOS made the alternative open web interaction with their visitors commercially unviable.

CMA Finding: CMA, Provisional Decision Report (22 November 2024), paragraphs 12.98 and 12.100 confirms: "*Apple also requires the use of its IAP system for in-app transactions… Apple's Guideline 3.1.1 requires [cloud gaming service providers] use Apple's IAP system (with a ban on alternative payment systems) and pay a commission to Apple on in-app payments.*"

The CMA's report acknowledges this concern extends beyond cloud gaming to any app publisher competing with Apple's apps. The proposed commitments contain no obligation that addresses this abusive restriction of competition.

3.2 Advertising Attribution and Measurement: Apple's ITP, ATT and SKAdNetwork

Publisher apps often rely on ad revenue for their business model. Data is the key input for targeted digital advertising. Over the years, Apple has released features into its mobile platform, which diminish publishers' ability to earn ad revenue. Two of the features are Intelligent Tracking Prevention ("**ITP**") and App Tracking Transparency ("**ATT**"), which are not addressed in these commitments.

Apple's App Tracking Transparency ("**ATT**") framework, introduced in 2021, was presented publicly as a consumer privacy protection measure. However, the US DOJ described Apple's privacy claims as "an elastic shield that can stretch or contract to serve Apple's financial and business interests."[51] Apple also faces a fine from the French competition authority regarding Apple's abuse of dominance through its implementation of the ATT framework and that it went beyond what is necessary and proportionate for protecting personal data. The CMA similarly found that Apple's ATT distorted user choice[52], making it harder for app developers to find consumers and to monetise their apps.

The CMA's own provisional findings note that "Apple is not applying the same standards to itself as to third parties forced to show the ATT prompt when it comes to seeking opt-in from consumers for personalised advertising." Specifically, Apple exempted Google from the requirement to show the ATT prompt, likely as a result of the commercial relationship between the two companies, while requiring the prompt for all other third-party advertisers.

The effect of ATT is that Apple's own SKAdNetwork ("**SKAN**") attribution system, used by Apple Search Ads, is exempt from the consent requirements that ATT imposes on third-party mobile measurement partners ("**MMPs**"). Apps advertising through Apple Search Ads receive more granular,

[51] https://www.justice.gov/atr/media/1344606/dl?inline, *USA v Apple* Complaint (21 March 2024), see para 16
[52] See the CMA Mobile ecosystems market study final report (10 June 2022), page 181 and pages 227 to 244

real-time attribution data than apps using rival ad networks and independent MMPs under the ATT consent regime. This creates a feedback loop: better attribution data enables more efficient ad spend optimisation, which drives higher app download velocity, which improves organic App Store ranking. Apps relying on third-party attribution are discriminated against and disadvantaged throughout this chain.

We note that the CMA has included a provision in its roadmap[53] that they will address these features in another category of remedies. However, these restrictions from Apple have been in place since 2017 (for ITP) and 2021 (for ATT). More urgent intervention is needed to address these.

Circumvention risk: Neither Apple's proposed commitments on app review nor on app ranking contains any prohibition on using ranking signals correlated with the use of Apple's own advertising and attribution infrastructure. A commitment to non-discriminatory ranking framed solely in terms of "first-party vs. third-party app status" will not capture this supply chain structural service advantage.

3.3 Google's Android: GAID, Privacy Sandbox, and Chrome Integration

Google's Android platform provides access to device-level advertising signals through the Google Advertising ID ("**GAID**") via Google Mobile Services ("**GMS**"). Third-party ad networks and measurement providers depend on GAID or equivalent signals. Google's Privacy Sandbox initiative, its programme to deprecate interoperable identifiers stored in cookie files and GAID while replacing both with Google-controlled alternatives, was presented as a cross-industry standardisation effort. However, the CMA is aware from its separate Privacy Sandbox investigation that Google's disclosures to consumers "overstate the privacy benefits" and the ICO has called out Google for using misleading and leading questions in its user-facing prompts.

Google has also delayed or given partial responses to a direct CMA question, repeatedly posed over four years, as to whether it will commit not to use search ranking based on publishers' decisions to use Google's own ad systems (such as Topics or the Protected Audiences API) or solutions from rival providers. Google's responses have carefully stated that *opting out* will not be used as a factor, while remaining silent on whether *opting in* confers a ranking advantage. This deliberate ambiguity is itself a competition harm. Similarly, when asked whether Google's proprietary APIs would add latency for rivals, Google initially stated to the CMA that the additional latency it imposed would be minor; while under further questioning, it emerged that the latency had been measured only within the browser itself, rather than the commercially critical measure of the time between publisher and advertiser bidding technology, which adds orders of magnitude more latency to real-time bidding and as a result materially impairs rivals' auction revenue. In other words, Google's measurement of latency to be the time within the browser itself was misleading and in actuality, the impact on latency overall between publisher and advertiser was higher than Google made it seem.

Google's exclusive bundling of its B2B ad systems with its dominant Android OS and Chrome browser is another form of self-preferencing. The CMA's provisional findings acknowledge concerns raised by mobile browser vendors relating to "the integration of Chrome with other Google services or products." The proposed Google commitments do not address this.

[53] https://assets.publishing.service.gov.uk/media/687f893cf2ecaeb756d0e1e6/Roadmap__Apple_.pdf

Proposed Requirement:
The CMA must impose Conduct Requirements, not commitments, that: (1) prohibit Apple from requiring use of IAP as a condition of app distribution to UK consumers, and require Apple to permit alternative payment processors on technically and commercially equivalent terms; (2) require Apple to provide third-party MMPs with equivalent access to input data used for attribution processing as those available to Apple Search Ads via SKAdNetwork, without imposing a different consent requirement for that use which does not apply to Apple Search Ads itself; and (3) require Google to provide third-party ad networks and MMPs with equivalent access to device-level advertising signals (GAID or equivalent) as those available to Google Ads and Google Analytics for Firebase, and to commit unambiguously that no ranking signal in Google Search or Play Store will vary based on the publisher's or developer's decision to adopt Google's own ad systems or those of rivals.

Part 4: App Store Fair Ranking Must Prohibit B2B Service Adoption as a Ranking Signal

4.1 The Scope of the Non-Discrimination Commitment Is Too Narrow

Apple's proposed commitment states that its algorithm "*prioritises user engagement, app quality and delivering users the most relevant results, and does not self-preference Apple's own first-party apps.*" Google similarly commits that Play's app ranking will be based on "*user relevance, app quality, and user experience*," applied non-discriminatorily to first-party and alternative apps.

These commitments define non-discrimination exclusively in terms of "first-party" versus "third-party" app status. These terms are self-serving as they reinforce the major players massive end user base advantages over rivals and have no basis in law. They do not address a more subtle and commercially damaging form of discrimination: the use of metrics that are correlated with adoption of the platform's own B2B services as ranking signals.

Moreover, by including the undefined factor of "quality" in their decision making they leave a critical loophole by which they can continue to discriminate against rivals whose "quality" is different (but not objectively worse) than their own apps and adjacent B2B services (e.g., payment processing, advertising solutions like attribution, broader generative AI services) in the provision of a consumer-facing OS or browser.

4.2 How B2B Service Adoption Operates as a Disguised Ranking Signal

Because Apple and Google both design the ranking algorithm and supply the B2B services whose adoption influences the metrics that feed into ranking, conflicts of interest arise that produce discriminatory ranking outcomes without any explicit instruction to do so:

- **Payment conversion:** Apple and Google ranking algorithms weight user engagement and conversion metrics. IAP and Google Play Billing are deeply integrated into the platform UX, producing higher conversion rates for technically equivalent in-app purchases made through the platform's own checkout compared to an alternative processor with a less integrated flow. If conversion rate feeds into ranking, IAP adoption creates a ranking advantage not captured by any framing based on "first-party" and "third-party" definitions.
- **Attribution feedback loops:** App Store ranking incorporates download velocity and user retention signals. Apps using Apple Search Ads benefit from SKAdNetwork's richer, more timely input data for attribution under the ATT regime. Apple's discriminatory restrictions on

data only for rivals' solutions enables more precise ad-spend optimisation, driving higher download velocity, which in turn improves organic ranking. Apps using only third-party ad networks and MMPs cannot access equivalent attribution signals and are therefore disadvantaged in this feedback loop, not because their apps are of lower quality, but because they do not use Apple's commercial B2B services.

- **Analytics and engagement signals:** Google's Play Store ranking incorporates user engagement data. Apps that integrate Google Analytics for Firebase provide Google's ranking infrastructure with richer behavioural signals than apps using alternative providers' analytics. Google's ranking algorithm is trained on this data. Even without any deliberate instruction to favour Firebase users, the algorithm will infer that Firebase-integrated apps have better-understood engagement patterns and will weight them accordingly.

Apple & Google's "objective, transparent and non-discriminatory" app review – Internal policies are not a fair way of reviewing apps

The criteria that Apple & Google may use for the app review is not detailed in the commitments. The criteria must be fair, not only consistent.

Criteria that discriminate against rivals and favour Google's or Apple's infrastructure, even if applied consistently, are not objective in the competition law sense. The most significant example is latency, where Google operates one of the world's largest content delivery networks. It can engineer latency advantages for content hosted on its infrastructure in ways that appear formally neutral but are discriminatory, such as using page load speed, server response time, or Core Web Vitals metrics in ways that systematically advantage publishers who use Google Cloud or Google's CDN.

Using such an artificial threshold as a ranking signal cannot be justified as serving users' interests and should be treated as a proxy for preferencing Google's or Apple's adjacent businesses and infrastructure.

The correct test is whether a criterion serves consumer interests. Where a criterion has the effect of systematically shifting volume to Google's or Apple's own properties, the SMS players must bear the burden of demonstrating that the shift is an unavoidable consequence of pursuing consumer interests rather than a discriminatory design choice.

Circumvention risk: An algorithm trained on metrics correlated with platform B2B service adoption will produce discriminatory ranking outcomes while formally complying with a commitment framed only in first-party/third-party terms. The CMA must require that the non-discrimination obligation cover any ranking signal whose effect is to systematically advantage apps that use Apple's or Google's own B2B services.

4.3 Editorial and Curated Placement Must Also Be Covered

Google's proposed commitment extends non-discrimination obligations to curated collections. Apple's commitments are silent on editorial app placement: "Editor's Choice", "App of the Day"' and similar featured positions. Editorial placement is a significant organic discovery channel. If Apple's editorial selection favours apps that integrate Apple Pay, use Apple Search Ads, or participate in Apple's

advertising platform, this leverages platform control into adjacent B2B services markets without being captured by any algorithmic ranking obligation.

Proposed Requirement:

Non-discrimination obligations in both Apple and Google ranking commitments must be extended to:(1) expressly prohibit any direct or proxy ranking signal systematically correlated with adoption of the platform's own B2B services for payment processing, advertising, attribution, or analytics, with Apple and Google bearing the burden of demonstrating that any identified correlation is an unavoidable consequence of best serving consumer interests; (2) require Apple to extend its non-discrimination commitment explicitly to editorial and curated app placement decisions, prohibiting B2B service adoption as an express or implied editorial selection criterion; and (3) require Apple and Google to report to the CMA, in their confidential monitoring reports, the correlation (in anonymised aggregate form) between app ranking position and adoption of each major platform B2B service, updated at least quarterly.

Part 5: Interoperability Commitments Must Deliver Substantive Open-Standards Access

5.1 Apple's Interoperability Commitment Is Process Transparency Without Substantive Outcome

Apple's proposed commitments improve only marginally the process for handling interoperability requests, namely: a dedicated feedback channel, published assessment criteria, a four-week status update, and outcome notifications, if they are complied with. These process improvements are welcome. However, in isolation they do not address the substantive access to real-time open web interoperable communications that developers need to compete with Apple's rival proprietary services. Moreover, Apple's published assessment criteria contain five conditions that Apple can use to decline any commercially inconvenient request, enabling it to abuse its dominance in mobile ecosystems.

As has been the *modus operandi* of Big Tech for some time, Google has framed restrictions on rivals' continued ability to rely on open web standards for real-time communication as an alleged "privacy" protection measure. Apple too relies on pretextual "privacy" claims to restrict rivals' ability to rely on open web standards for real-time communication. These firms then exempt their own continued reliance on real-time communication under the so-called "First Party" exemption. However, data protection regulations are concerned with the protection of personal data, not whether the data is "first" or "third party" data. Regulators have repeatedly held that privacy concerns hinge on what data is being collected and processed, rather than the discriminatory labels of "first" and "third" party recipients which are used by Apple and Google. Indeed, the aim of framing messaging around "first" and "third party" is to heighten concerns about third parties or open web businesses and reduce concerns about the big platforms who have first party relationships. Apple and Google have used this language to mislead and misdirect enquiry away from their own privacy practices. This issue is likely to be central to the forthcoming case between Texas and a range of US states taken against Google, in which coordination of lobbying to prevent privacy protections has been a feature of the conduct of the major tech platforms.[54]

[54] See *In re Google Digital Advertising Antitrust*, para 170: For example, in a closed-door meeting on August 6, 2019 between the five Big Tech companies, including Facebook, Apple, and Microsoft, Google discussed forestalling consumer privacy efforts. In a July 31, 2019

We remind the CMA of its joint statement with the ICO that data protection regulations must not be interpreted to view vertically-integrated "first party" handling differently than transfers of data among independently-owned third-party businesses, as well as to ensure the focus is on whether the data exchanged is personal or non-personal data.[55]

CMA Finding: CMA & Joint Statement (19 May 2021), paragraphs 76ff (emphasis added): *"there is a risk of data protection law being interpreted by large integrated digital businesses in a way that leads to negative outcomes in respect of competition. For example,... an interpretation of data protection law in which transfers of personal data between different businesses owned by a single corporate entity – such as a large platform company – are in principle viewed as acceptable from a privacy perspective, while transfers of personal data between independently-owned businesses are not, even if these businesses are functionally equivalent to those of the platform and the data is processed on the same basis and according to the same standards.*
If implemented in practice, such an interpretation would clearly be problematic for competition, as it would provide strong incentives for companies to integrate horizontally and vertically in order to be able to process more personal data. It would also undermine the ability of challenger or new entrant firms that are not vertically integrated, including small start-ups, to compete in digital markets....
It is important to note, therefore, that neither competition nor data protection regulation allows for a 'rule of thumb' approach, where intra-group transfers of personal data are permitted while extra-group transfers are not."

5.2 The Assessment Criteria Are Exploitable Vetoes

Apple's criteria for assessing interoperability requests include: (i) expected user and developer uptake; (ii) alignment with Apple's platform priorities; (iii) potential implementation costs; (iv) impact on user experience, performance, security, safety, privacy, integrity, and accessibility; and (v) impact on Apple's intellectual property rights. Each of these conditions is exploitable by Apple:

- **Criterion (i) Expected uptake:** Apple controls the definition of expected uptake and the data used to measure it. A developer cannot demonstrate expected uptake for functionality they cannot yet build because access is denied. This criterion creates a circular bar to entry.
- **Criterion (ii) Platform priorities:** This is a wholly subjective criterion that Apple defines unilaterally. Any request for functionality that competes with Apple's own services (such as payments via NFC, real-time messaging via a non-APNs route, browser engine alternatives) can always be characterised as not aligning with Apple's platform priorities.

---

document prepared in advance of the meeting, Google memorialized: "*we have been successful in slowing down and delaying the [ePrivacy Regulation] process and have been working behind the scenes hand in hand with the other companies*" and para 224: "*The companies also have been working together to improve Facebook's ability to recognize users using browsers with blocked cookies, on Apple devices, and on Apple's Safari browser, thereby circumventing one Big Tech company's efforts to compete by offering users better privacy.*" https://www.courtlistener.com/docket/60149069/152/in-re-google-digital-advertising-antitrust-litigation

[55] ICO and CMA Joint Statement (19 May 2021): "*The boundaries between first and third-party data according to the above definition are not always clear, particularly when large companies own a variety of businesses, some of which have a relationship with the user and some of which do not. Both first-party and third-party data as defined above can include personal and non-personal data. Whether information is personal data depends on whether it relates to an identified or identifiable individual. There is no explicit reference to the distinction between first-party and third-party data in data protection law*".
Appendix G of the CMA 2020 report currently refers to the fact that the same cookie data is contained in cookie files and the designation of first and third party merely relates to domain. As such it is the same data that is used by both Google and others. The issue that this creates for Google. With its extensive ability to reidentify end users, is a greater level of privacy risk than for third parties using the same data, where they do not have the means or capability to reidentify the individuals. The CJEU has recently clarified the legal position in Case T-557/20 SRB v EDPS. https://assets.publishing.service.gov.uk/media/60a3c893d3bf7f288aaa5c9b/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf

- **Criterion (iii) Implementation costs:** Apple could lower its implementation costs by standardising its APIs and adopting open-standard communication protocols. Such an approach would enable the use of a single, unified set of mechanisms for accessing hardware functionalities across its mobile operating system and browser platforms, instead of maintaining two distinct and discriminatory systems that hinder (and often foreclose) competition by creating asymmetries in information and functionality.
- **Criterion (iv) Privacy and security:** These are legitimate considerations. However, the DOJ described Apple's use of privacy justifications as an "*elastic shield*" that Apple "*selectively compromises when doing so is in Apple's financial interest*."[56] The CMA's provisional decision confirms "the risk of Apple's attempt at circumvention is high, given Apple's continuous self-preferencing definitions of these terms." Without an objective and legally grounded definition of "privacy" and an independent technical assessor, this criterion is an unconstrained veto (see Part 5 below).
- **Criterion (v) Apple's intellectual property:** As drafted, any request that could be characterised as affecting Apple's IP can be declined. The scope of what "affects Apple's IP" is potentially unlimited and cannot be a standalone ground for refusal where an interoperability obligation arises from a finding of market power.

5.3 Five Categories of Interoperability the Commitments Must Deliver

Browser engine interoperability

Apple's restriction on alternative browser engines on iOS (the WebKit requirement) means that all browsers on iOS, regardless of consumer-facing brand, must use Apple's WebKit engine. This means Apple's decisions about which web platform features to support directly constrains the capabilities available to all browser users on iOS, regardless of which browser consumers have chosen.

The CMA's provisional decision identifies Apple's conduct as causing a negative impact on "*security, privacy, performance, and feature support for browsers on iOS.*"[57]As Mozilla submitted, the failure to support web compatibility standards causes consumers to shift to alternative methods of interacting with web content, accelerating the shift from the open web to proprietary App Store.

The CMA's roadmap flagged browser engine interoperability as a priority intervention for the first half of 2026. The current commitments do not deliver it.

NFC access and contactless payment interoperability

Apple's restriction of NFC access to Apple Pay directly prevents competing digital wallet and payment services from operating on equivalent terms on iOS. The European Commission reached a commitments decision with Apple on NFC access in 2024.

The CMA has identified digital wallets as a priority intervention area. The current commitments do not deliver NFC interoperability.

Push notifications and real-time communications (APNs)

Third-party apps requiring real-time push notifications on iOS must route through Apple's Push Notification Service ("**APNs**"). There are no documented, enforceable, publicly available specifications permitting competing real-time communications infrastructure to operate on equivalent terms. This

[56] *USA v Apple* Complaint (21 March 2024), see para 16. https://www.justice.gov/atr/media/1344606/dl?inline
[57] Para 4.71, CMA Mobile Browsers and Cloud Gaming Provisional decision report (22 November 2024)

dependency affects the commercial competitiveness of all third-party messaging, notification, and real-time services on iOS. It discriminates against rivals and advantages Apple's own messaging infrastructure, iMessage and FaceTime, while disadvantaging every competing communications service.

Technically, maintaining state and interoperability across systems requires a common match key. MOW recommends that Apple's deidentified "random identifier," which Apple itself uses and promotes as a privacy-preserving mechanism, be made available to other solution providers to support real-time interoperability, with explicit prohibitions on any recipient's reidentification of a specific individual. This approach is technically feasible and aligns well with data protection obligations as highlighted in the SRB decision.

VoIP and CallKit Integration

Third-party VoIP and communications apps require equivalent access to CallKit and telephony integration frameworks to compete with Apple's FaceTime. Apple's first-party communications apps benefit from lock-screen integration, Siri, CarPlay, and system audio routing that are not available on equivalent terms to rivals. Apple's commitments are silent on this.

iMessage Interoperability and RCS Support

Third-party messaging apps cannot interoperate with iMessage, preventing users from receiving and responding to iMessage contacts without leaving their chosen app. Apple's implementation of RCS must not disadvantage third-party RCS-capable messaging apps relative to iMessage. Apple's commitments are silent on messaging interoperability.

5.4 Standards Bodies: Apple and Google Must Not Continue to Act as Quasi-Regulators

MOW has made multiple submissions about Apple and Google's abuse of their dominance to technical standards bodies including W3C, IAB Tech Lab, and IAB UK. Both companies have sought to legitimise their anticompetitive conduct by shaping standards under the banner of allegedly neutral trade bodies. The CMA's provisional findings acknowledge concerns that Apple and Google "slow innovation and investment in web businesses, by dominating committees that set standards to restrict competition."

The remedies must ensure that Apple and Google are not permitted to use standards body processes as a mechanism for circumventing the obligations the CMA imposes. Specifically, any proposal Apple or Google submits to a technical standards body that would restrict rivals' access to functionality previously available under open web standards must be accompanied by a published competition impact assessment, reviewed and approved by the CMA before implementation. The CMA's own investigations confirm that platforms should not be quasi-regulators of the markets in which they compete.

Proposed Requirement:

The CMA must impose formal Conduct Requirements, not commitments: (1) Apple must permit alternative browser engines on iOS/iPadOS, subject only to objectively assessed security requirements verified by an independent technical expert (not Apple); (2) Apple must provide third-party payment apps with technically and commercially equivalent NFC access to that available to Apple Pay; (3) Apple must provide open, documented, FRAND interoperability specifications for APNs or permit competing

real-time communications infrastructure on equivalent terms; (4) interoperability assessment criteria must remove "alignment with Apple's platform priorities" as a standalone criterion, and any proposed "security" or "privacy" justification for declining a request must be assessed by an independent technical expert against the objective privacy definitions set out in Part 5; and (5) Apple and Google must publish a competition impact assessment for any proposal they submit to a standards body that would restrict rivals' functionality access, reviewed by the CMA before implementation.

Part 6: 'Privacy' and 'Security' Must Be Objectively Defined to Prevent Circumvention

6.1 The Circumvention Risk Is Already Documented

The CMA's provisional decision report confirms that the risk of Apple's attempt at circumvention is high, given Apple's continuous self-preferencing definitions of privacy and security terms in the past. The CMA itself recognises that any remedy that permits Apple to impose "*minimum security and privacy requirements*" without defining those terms "*objectively… and proportionate to mitigate the risks*" causes a high risk of being used by Apple as a loophole.[58]

Moreover, the US DOJ's complaint in United States v. Apple describes this with precision: "*Apple wraps itself in a cloak of privacy, security, and consumer preferences to justify its anticompetitive conduct. Apple selectively compromises privacy and security interests when doing so is in Apple's own financial interest.*"[59]

Google's record is equally documented. The CMA has found that Google's consumer disclosures "*overstate the privacy benefits to Users*." The CMA has called out Google on three separate occasions for using leading questions in its consumer-facing prompts and instructed Google to "*avoid such leading questions in the future*."

These companies' activities are coordinated. Google and Apple, together with other large technology companies, engaged in a closed-door meeting in 2019 at which they discussed forestalling consumer privacy laws and "*had been working behind the scenes hand in hand with the other companies"* to *"successfully slow down and delay*" the EU ePrivacy Regulation process.

Definitions of "security" and "privacy"

A definition regarding the meaning of privacy and security should be clarified by the CMA. We note that in the consumer survey table regarding technical use and behaviour on the CMA's case page,[60] the CMA defines them as follows:

> "*Security features (e.g. virus protection, protection from hacking)*"
> "*Privacy features to control how my private information is used or tracked by companies when using apps or websites*"

These definitions are overly broad and risk being exploited by Apple and Google. With respect to security features, there should first be a distinction regarding the type of data that needs to be kept

[58] CMA, Provisional Decision Report (22 November 2024), paragraph 11.123.
[59] https://www.justice.gov/atr/media/1344606/dl?inline, *USA v Apple* Complaint (21 March 2024), see para 16
[60] https://assets.publishing.service.gov.uk/media/6880a676fdc190fb6b846917/Consumer_survey_data_tables_-_technical_use_and_behaviour.xlsx

secure. If it does not relate to personal data, the foreclosure of rivals becomes disproportionate on these grounds.

"Security" can be defined as preventing unauthorised access.[61] However, this definition raises who is empowered to provide appropriate authorisation. When the business data in question is neither Personal Data nor sensitive information, then it seems reasonable that the business controlling that data ought to determine which partners can access it. Having Apple and Google indiscriminately block such interoperable exchanges and sharing causes grave competition concerns, which is at the heart of concerns regarding Apple's ITP and ATT as well as Google's Privacy Sandbox.

On numerous occasions, Google and Apple's justifications for restrictions on the basis of privacy and security have been rejected. In *Kent v Apple*, which found that Apple had incorporated restrictions in its App Store functionality that led to it charging excessive prices[62], Apple's security and privacy defence for the exclusion of third parties from its iOS were found to be unnecessary and disproportionate. The specific criteria for these bases needs to be assessed by the CMA, rather than Apple.

With respect to "privacy" features, as the CMA is aware, a common misconception that major platforms utilise to their advantage is the artificial "labelling" of technology and processing, obfuscating any risk-based analysis of the sensitivity of data in question or risk mitigation aspects recognized by data protection regulations. In response to the Privacy and Electronic Communications Regulations ("**PECR**"), the ICO issued guidance that merely labelling storage and access technologies doesn't impact whether Regulation 6 of PECR applies.

The ICO lists the following typical labels that do not aid in identifying the risk of what data is being used or for which *use and purpose*:

- 'first-party' or 'third-party';
- 'session' or 'persistent'; and
- 'client-side' or 'server-side'.[63]

MOW agrees with the ICO that the key consideration is the purposes (or uses) to which such technology is applied. MOW is pleased with the clarity the ICO has made by summarizing this policy:
"Ultimately, whether a storage and access technology is classed as 'first-party' or 'third-party' is not the main consideration for data protection and privacy purposes. Instead, what's primarily relevant is:

- *who is responsible for the storage or access on terminal equipment — which in most cases is the service provider; and*
- *the purpose(s) of the storage / access"*[64]

The crucial aspect for the analysis of any risks of privacy is not *where* the processing occurs, but rather *what* data is being collected and processed and for which uses. Clarity on this within Conduct Requirements from the CMA will assist with future enforcement.

---

[61] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 4.130.
[62] https://www.catribunal.org.uk/sites/cat/files/2025-12/14037721%20Dr.%20Rachael%20Kent%20v%20Apple%20Inc.%20and%20Apple%20Distribution%20International%20Ltd%20-%20%20Judgment%20%5B2025%5D%20CAT%2067%2023%20Oct%202025.pdf
[63] ICO (2025). https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/#using_storage_and_access_technologies_in_different_contexts
[64] ICO (2025), https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/#using_storage_and_access_technologies_in_different_contexts

The lack of evidence-based risk assessments has led to a disproportionate restriction of functionality that has distorted competition, by shifting online consumer behaviour away from free access to online websites to accessing the identical content and services via Google and Apple's proprietary app stores. The harm to consumers is the extortion of fees associated with any online payment that would not exist if that same individual were to interact with that same online business via a browser. Businesses must both pass these costs along to consumers in terms of higher prices, but also increasingly prompt consumers to pay to access their property or increase the ad load in their websites to make up for the reduced monetisation ability given Apple's interference with cookie storage.[65]

CMA Finding: CMA, Provisional Decision Report (22 November 2024), paragraph 11.123: Apple can impose "*minimum security and privacy requirements*" but "*those requirements would need to be objectively required and proportionate to mitigate the evidence-based risks highlighted above.*" The CMA acknowledges that without an objective definition, circumvention is reasonably foreseeable.

6.2 The Key Distinctions Apple and Google Deliberately Conflate

The core definitional problem is that Apple and Google consistently conflate two distinct categories of data and two distinct categories of risk in order to justify overbroad restrictions on rivals:

- **Personal Data versus deidentified data:** Courts have held that data, including IP addresses, cannot be presumed to be personal. The ICO's guidance is clear: information that is "effectively anonymised is not personal data and data protection law does not apply." Apple itself, in its own marketing and filings to the CMA, distinguishes between Personal Data and deidentified data, referring to its own "random identifiers" as privacy-preserving. Apple's restrictions on rivals, however, apply indiscriminately to both categories. When the data being exchanged is deidentified, prohibiting the linkage to any specific individual, Apple cannot rely on "privacy" to restrict rivals' access to it, because the privacy risk that justifies the restriction does not exist in relation to that data.
- **"Tracking" versus "interoperability":** Google and Apple both rely on the ICO's rejected premise that "third-party" data is inherently less safe than "first-party" data, whether stored in cookies or on servers. The ICO and CMA have both repeatedly confirmed that "first party" versus "third party" distinctions have no relevance to privacy protection. What matters is (1) whether the data in question is linked to a specific individual in the hands of the recipient; and (2) whether the use of that data poses a high likelihood of severe risk to those individuals. When these conditions are not met, as is the case for deidentified business data used for real-time bidding, audience measurement, and contextual advertising, Apple and Google's overbroad restrictions on rivals' real-time interoperability are not privacy measures but commercial restrictions that distort competition. Tracking must not be confused with interoperability.
- **Security risks versus competition restrictions:** "Security" is properly defined as preventing unauthorised access. However, when the business data in question is neither Personal Data nor sensitive information, the question of authorisation is for the business controlling that data, not for Apple or Google. Apple and Google's application of "site isolation" and analogous security measures to ***all*** **data**, rather than only to the sensitive data those measures were designed to protect, is an overbroad application that causes grave competition concerns.

[65] Online Platforms and Digital Advertising Final Report (1 July 2020), paragraph 5.326: In research conducted by the CMA it found UK publishers earn "around 70% less revenue overall" when unable to sell advertising using third party cookies. https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final report Digital ALT TEXT.pdf

6.3 The False Privacy Binary in Choice Architecture

Apple and Google both deploy choice architecture that gives consumers a false sense of security while concealing the commercial self-interest served by the design. The CMA's provisional report found that Apple's ATT prompts "*could unduly influence some consumers to refuse data sharing in a way that may be inconsistent with their preferences.*" This consent sludge manufactures privacy preferences that reflect Apple's commercial interests, not consumers' actual preferences.

Importantly, the CMA's own research confirms that only 8% of consumers selected privacy features as an important factor in browser choice, with 1% selecting it as the most important factor. The CMA's Mobile Ecosystems Market Study found "*only 29% of consumers on iOS and 22% on Android named security and privacy as a factor which was important to their smartphone decision.*"

Privacy is a legitimate and important concern for a minority of consumers, and that minority deserves genuine competitive choice. However, Apple and Google's current privacy frameworks do not serve that minority. Instead, both companies produce a false sense of security for privacy-concerned consumers while commercially disadvantaging all rivals who depend on safe exchanges of deidentified, business data.

6.4 Proposed Objective Definitions for the CMA's Order

To prevent circumvention, the CMA's order must incorporate the following objective definitions, drawn from Applicable Data Protection Legislation and relevant court decisions:

- **Definition of privacy risk:** A "privacy risk" for the purposes of any security or privacy justification offered by Apple or Google must be assessed by reference to: (a) whether the specific data in question constitutes Personal Data or Sensitive Data in the hands of the recipient (not the sender); (b) the likelihood, not the theoretical possibility, of harm to a specific identifiable individual; and (c) the severity of that harm. Restrictions based on mere potential privacy risks must be proportionate to evidence-based assessment of likelihood and severity. Apple and Google bear the burden of demonstrating this assessment with specific evidence for each restriction.
- **Personal Data versus deidentified data:** Data, including IP addresses, cannot be presumed to be personal. Personal Data in the hands of Apple or Google may be deidentified in the hands of the recipient. Any restriction imposed by Apple or Google on the basis of "privacy" must identify specifically whether the data in question is Personal Data or Sensitive Data in the hands of the recipient and must not apply to deidentified data.
- **Symmetry of obligations:** Any restriction Apple or Google imposes on rivals' use of data must apply on equivalent terms to Apple's and Google's own use of that data in their own adjacent and competing B2B services to the provision of a mobile OS or browser. Apple cannot lawfully restrict rivals' use of deidentified data while using deidentified "random identifiers" in its own advertising and analytics services. Google cannot restrict rivals' use of device signals for advertising while using equivalent signals through Google Ads and Google Analytics for Firebase.
- **Choice architecture:** Any consumer-facing prompt or choice screen presented by Apple or Google in connection with privacy or data permissions must be independently tested (including through the kind of consumer survey research the CMA commissioned from Verian) to ensure it does not use dark patterns, biased framing, consent sludge, or disproportionate visual hierarchy to steer consumers toward choices that serve Apple's or Google's commercial

interests. Prompts must use neutral language, equivalent visual weight for all options, and must fully and accurately describe the commercial consequences of each choice.

Proposed Requirement:

The CMA must incorporate the following into any order: (1) "Privacy" and "security" justifications offered by Apple or Google for restrictions on rivals' interoperability must be assessed against objective criteria anchored in Applicable Data Protection Legislation and relevant court decisions — not Apple's or Google's self-defined interpretations; (2) any restriction must identify specifically whether the data in question is Personal Data in the hands of the recipient (not the sender), the likelihood and severity of harm, and the proportionality of the restriction; (3) the same restrictions must apply on equivalent terms to Apple's and Google's own use of equivalent data in their own competing services; (4) any proposed new policy or technical restriction that Apple or Google presents as a "privacy" or "security" measure must be accompanied by a privacy risk assessment using these objective criteria, provided to the CMA for review before implementation, with a minimum 60-day notice period; and (5) any consumer-facing choice architecture relating to privacy or data permissions must be independently tested and approved by the CMA before deployment.

Part 7: Monitoring Must Be Output-Based, Independent, and Continuous

7.1 Lack of due process, testing and trialling

There is a lack of due process in the CMA's policing of commitments. The CMA is responsible for assessing and making sure its remedies are effective in addressing the anticompetitive practices that it has identified, not Google and Apple. The commitments focus on Google's and Apple's reporting and complaints process, which are a separate matter from the CMA's duty to secure an effective remedy.

The CMA has also overlooked the importance of trialling and testing remedies before they come into force. In the CMA's 2020 DAMS Report,[66] the CMA noted the importance of an ongoing trialling and testing monitoring regime. Excluding such a provision now risks being inconsistent and going against what is a legitimate expectation of third parties.

Also, reporting on bi-annual or annual instalments is not regular enough in tech markets that are fast moving. This should be amended so that the CMA can seek information and metrics from Google and Apple at any time during the SMS designation period depending on the issue at hand.

7.2 The Proposed Framework Measures Inputs, Not Outcomes

The CMA's proposed monitoring framework, bi-annual public reporting, annual self-attestations, complaint volumes, and supplementary confidential metrics, form an input and process measurement framework. It tells the CMA how many decisions Apple and Google made, not whether those decisions were fair or whether competition has been restored.

A developer whose app is systematically disadvantaged by ranking signals correlated with B2B service adoption, or whose interoperability request has been declined using a "platform priorities" veto, will not necessarily file a formal complaint. With unilaterally dictated platform policies, such competing

[66] https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

developers or content providers will commercially adapt to Apple's and Google's preferences, investing resources in platform conformity rather than in innovation.

Complaint volume is therefore an inverse indicator of the effectiveness of platform leverage. The more effectively Apple and Google use their market power to coerce commercial conformity, the lower the complaint rate. A monitoring framework that treats low complaint rates as evidence of compliance will systematically underestimate ongoing harm.

CMA Finding: CMA Call for Evidence, paragraph 9: Commitments are unlikely to be appropriate "where compliance is difficult to determine, observe or monitor" or "where measures can be easily circumvented." All of the B2B service coercion, ranking discrimination, and privacy circumvention risks identified in this submission satisfy these caution conditions.

7.3 The DMA Compliance Record Confirms the Circumvention Risk

Apple and Google's compliance record under the EU Digital Markets Act confirms that voluntary and self-reported compliance mechanisms are insufficient. DuckDuckGo has documented that Google has failed to comply with Article 6(11) (sharing anonymised click and query data with rivals), Article 6(3) (rolling out updated Android choice screens to all EU users), and Article 6(4) (allowing downloaded browser apps to prompt users to set search defaults). [redacted] Given this history, these same companies are extremely unlikely to self-report their non-compliance in the UK absent independent verification.

7.4 Specific Output Metrics the CMA Must Require

The CMA should require the following output-based measures, reported on a continuous basis to the CMA and, where consistent with commercial confidentiality, published:

- **App ranking distribution by B2B service adoption:** Apple and Google must report, in aggregate anonymised form, the correlation between app ranking position and adoption of platform B2B services (including IAP/Play Billing, Apple Search Ads/Google Ads, and Apple/Google analytics). This data must be reported daily to the CMA to enable detection of systematic patterns before they cause irreversible harm. Given the daily updates in Search ranking both companies currently provide in their app stores, this obligation is commercially feasible and can ensure swift attention to new discriminatory conduct.
- **Interoperability request outcomes by functional category:** For Apple's interoperability channel, the CMA should receive monthly data on: the nature of each request by functional category (payments, notifications, browser engine, communications); the outcome; and the stated justification for each declined request. The CMA should publish a quarterly summary of declined requests by category so that patterns of systematic refusal can be identified.
- **Attribution signal parity:** Apple must report quarterly on the differential in attribution data granularity available to Apple Search Ads via SKAdNetwork versus that available to third-party MMPs under the ATT consent framework. Google must report quarterly on any changes to GAID availability and Privacy Sandbox API specifications that affect third-party advertising solution providers and MMPs.
- **Privacy assessment records:** Any alleged "privacy" or "security" justification offered by Apple or Google for a restriction on rivals' interoperability must be included in confidential reporting to the CMA, together with the specific evidence base for the assessed likelihood and

severity of privacy risk based on the ICO's definitions of privacy, not these platforms. The CMA's independent technical monitor (see below) must have access to these assessments.

- **CMA can also monitor compliance:** The CMA can assess the outputs of the ranking and whether the results being displayed are fair by conducting their own investigation of the results rendered in response to searches in Apple and Google's respective app stores (output-based assessment). If any discriminatory results appear, then the burden is on the SMS player to advance an objective justification, which the CMA needs to assess.

7.5 An Independent Technical Monitor Is Required

Due process requires independent adjudication (not by Google and Apple) of evidence from both Google's compliance systems and from third parties. Any justification of a defendant's position is a burden borne by the defendant and must be subject to evidence testing and scrutiny by the CMA before being accepted.

Such process would be one where the CMA can hear evidence from rivals within a time frame laid down for a fast-track resolution of any disagreement that Google and Apple cannot game to their benefit.

The CMA should appoint an independent technical monitor, modelled on the monitoring trustee regime used in UK merger control, with the following remit:

- Access to Apple's and Google's ranking algorithms and training data, under appropriate confidentiality protections, sufficient to assess whether any ranking signal is systematically correlated with platform B2B service adoption;
- Authority to commission algorithmic audits at intervals determined by the CMA, using methodologies comparable to those used by the European Commission in DMA proceedings;
- Authority to review Apple's interoperability request decisions and assess whether the stated privacy and security justifications are technically credible, proportionate, and consistent with the objective definitions required under Part 5;
- Authority to review Apple's and Google's consumer-facing choice architecture for compliance with the dark-pattern prohibition; and
- Authority to publish findings to the CMA and, in summary form, publicly, thereby providing accountability and deterrence that self-reported attestations cannot deliver.

7.6 Pre-Implementation Notification Requirement

The proposed commitments do not include any obligation on Apple or Google to notify the CMA in advance of material changes to platform policies, payment processing terms, advertising frameworks, attribution APIs, or interoperability assessment criteria. This means that by the time harm is identified, it will already have been caused. Such conduct potentially irreversibly harms developers who have invested in product strategies that a platform policy change renders commercially unviable.

Proposed Requirement:

The CMA must require: (1) an independent technical monitor appointed by the CMA with the remit set out above; (2) daily or weekly CMA access to aggregate output data on app ranking distributions by B2B service adoption category; (3) an anonymous developer reporting channel for concerns about

ranking discrimination and B2B service coercion, with the CMA committing to investigate systemic patterns without identifying individual complainants to Apple or Google; (4) a mandatory 60-day pre-implementation notification requirement for any material change to: payment processing policies; advertising identifier frameworks; attribution APIs; interoperability assessment criteria; or consumer-facing choice architecture — with a CMA right to pause implementation pending review; and (5) regular CMA-initiated market engagement with UK app developers on a structured non-complaint basis, to identify emerging concerns before they crystallise into formal complaints.

Part 8: Substantive Issues with Apple's Commitments (10 February 2026)

Apple has offered commitments to the CMA regarding:

1) "*Apple's App Review process;*
2) *App Store search results;*
3) *Apple's use of third-party data collected through its operation of the App Store and during App Review; and*
4) *the transparency of Apple's process for considering requests for interoperable access to functionality in iOS and iPadOS.*"[67]

8.1 Apple's discriminatory review process for rival apps

Apple claims that its review process is dedicated to maintaining "*a safe, secure, and high-quality experience*" for consumers and that its reviews of software are "*objective, fair, and transparent.*"[68] Both claims are misleading.

Loophole-AR1: Apple's claim of "fair, objective and transparent" reviews is self-defined and self-assessed.

The commitment in paragraph 1 is that Apple will conduct App Review "*on the basis of the Guidelines*" and "*will not preference Apple's competitive interests*." But the Guidelines themselves are written, maintained and updated exclusively by Apple. There is no independent verification that the Guidelines are substantively fair, only that Apple applies them consistently. A commitment to apply biased rules consistently is not a commitment to fairness. The commitment lacks any mechanism for independent review of the Guidelines' content.

Apple's pretextual claim that its own software is safer that rivals' software, specifically related to "privacy" claims, is refuted by court records.[69] The court in *Kent* rejected Apple's reliance on privacy and security to justify tying in-app purchasing to its proprietary API, finding the conduct abusive and the justification unsupported by evidence. The court stated:

> *"**783.** We also accept that there is evidence that some users value safety, security and privacy…*
> ***784.** However, that does not necessarily mean that that group of users (or indeed, the wider user population) need or want an integrated and centralised service for iOS app distribution and in-app payment services…*
> ***785.** In the security counterfactual, iOS device users will get the benefit of App Review and the application of the Guidelines in any event… it seems difficult to say that there is any material*

[67] Apple Commitments (10 February 2026), page 1, paragraph 1.
https://assets.publishing.service.gov.uk/media/69899adbd3f57710b50a9b86/apple_proposed_commitments.pdf
[68] Apple Commitments (10 February 2026), page 2.
https://assets.publishing.service.gov.uk/media/69899adbd3f57710b50a9b86/apple_proposed_commitments.pdf
[69] 51403/7/7/21 Dr. Rachael Kent v Apple Inc. and Apple Distribution International Ltd.

reduction, in such a counterfactual, in the benefits which an iOS device user who is concerned about safety, security and privacy will receive."

The court accepted that Apple's privacy and security justifications could be presented in general terms but found them insufficient to justify the tying, as the same benefits could be achieved without the restrictive conduct. They are disproportionate.

This is consistent with the long-accepted principle of competition law that an objective justification for anti-competitive action must be proportionate.[70] The court clarified that any claim for privacy or security benefit must be evidenced by a concrete, causal connection between the alleged risk and the restriction imposed and be proportionate to the outcome. No such evidence was produced in *Kent v Apple*.

This decision illustrates that assertions of objective justification, based primarily on alleged privacy considerations, cannot be accepted at face value or serve as a shield for dominant firms' practices that are otherwise anticompetitive.

The CMA should only accept Apple's use of App Review Guidelines once such guidelines have been rewritten to ensure they achieve the conduct requirement changes from Apple necessary to restore competition.

Proposed Conduct Requirement App Review (CR AR-1):

Apple must not amend, introduce or remove any provision in the App Review Guidelines ("Guidelines") without first submitting the proposed change, together with its stated rationale, to the Independent Monitor appointed for review (see CR AR-6).

The Independent Monitor shall assess whether the proposed change: (i) is objectively justified by reference to user safety, privacy, security, platform integrity, or a legitimate technical constraint; (ii) is proportionate to that objective; and (iii) does not discriminate between Apple first-party apps and equivalent third-party apps. The Independent Monitor shall provide a written opinion within 20 Business Days of receipt.

Apple may implement the proposed change only after receiving a non-adverse opinion from the Independent Monitor, or, in the case of an adverse opinion, following resolution by the CMA pursuant to the dispute procedure detailed under this Conduct Requirements package. In cases of genuine emergency (imminent threat to security), Apple may implement a change immediately and must notify the Independent Monitor and the CMA on the same day, with the change subject to retrospective review within 10 Business Days.

[70] see Whish, R. and Bailey, D., *Competition Law*, 7th edn (Oxford University Press, 2018), p. 211, Objective Justification, "The language of objective justification can be found in many judgments and decisions coupled with the proposition that, to be objectively justifiable the conduct in question must be proportionate." See also: Case 311/84 [1985] ECR 3261. [1986] 2 CMLR 558 *Centre Belge d'Etudes de Marché Télémarketing v CLT,* BBI/Boosey and Hawkes OJ [1987] L 286/36, [1988] 4 CMLR 67; BPB Industries plc OJ [1989] L 10/50, [1990] 4 CMLR 464, para 132, upheld on appeal Case T-65/89 *BPB Industries plc and British Gypsum v Commission* [1993] ECR II-389, [1993] 5 CMLR 32 and further on appeal to the Court of Justice Case C-310/93 *P BPB Industries plc and British Gypsum v Commission* [1995] ECR I-865, [1997] 4 CMLR 238; *Napier Brown – British Sugar* OJ [1988] L 284/41, [1990] 4 CMLR 196, paras 64 and 70; *NDC Health/IMS Health: Interim Measures* OJ [2002] L 59/18, [2002] 4 CMLR 111, paras 167–174; *Portuguese Airports* OJ [1999] L 69/31, [1999] 5 CMLR 103, para 29; *Prokent-Tomra* Commission decision of 29 March 2006, paras 347–390.

Loophole-AR2: Apple's Claim of Independence of the App Review team is not guaranteed.

Paragraph 2 commits to App Review personnel operating "*independently from teams responsible for Apple's apps and services*" within Apple's internal structure. However, all App Review staff remain Apple employees, subject to Apple's performance management, culture, and incentive structures. The commitment contains no firewall mechanism, no external oversight body, and no requirement that the organisational separation be verified by anyone outside Apple. The annual self-certification in paragraph 8(b), that App Review "*continues to operate independently*", is a statement Apple makes about itself.

Proposed Conduct Requirement App Review (CR AR-2):

Apple must implement and maintain a firewall between the App Review function and any Apple team responsible for developing, marketing, or monetising Apple first-party apps or services. The firewall must include, at minimum:

(i) Separate reporting lines to a distinct senior executive (Vice-President level or above) for App Review staff and non-app review staff respectively, with no common superior below the level of Chief Executive Officer;

(ii) Information barriers preventing App Review personnel from receiving real-time or prospective information about unreleased Apple first-party app features or Apple product strategy;

(iii) Information barriers preventing App Review personnel from sending information about unreleased app features or non-Apple products under review to non-app review staff;

(iv) A prohibition on performance evaluation metrics for App Review personnel that incorporate, directly or indirectly, the commercial performance of any Apple first-party app or service;

(v) Annual mandatory attestation by each App Review team member confirming compliance with the firewall requirements, with copies of attestations submitted to the Independent Monitor.

The Independent Monitor shall conduct an annual audit of the firewall, including confidential interviews with App Review personnel, and shall report findings to the CMA.

Loophole-AR3: Apple's Commitment contains no substantive right of appeal on the merits.

Paragraph 6(c) grants developers a right of appeal to the "App Review Board." But the App Review Board is itself an Apple body. There is no right of appeal to any independent arbiter, and no defined standard of review on appeal. Apple retains absolute discretion over the outcome. This differs materially from a right of challenge to the CMA or another external body, which would be the meaningful protection competition law would ordinarily contemplate.

Proposed Conduct Requirement App Review (CR AR-3):

Apple must make available to developers an external independent appeal mechanism for all final App Review rejection and removal decisions. This external independent appeal mechanism shall:

(i) Be administered by an independent adjudicator approved by the CMA, who shall not be an Apple employee, contractor, or otherwise financially dependent on Apple;

(ii) Apply a standard of review asking whether Apple's decision was: (i) consistent with the Guidelines; (ii) applied consistently with decisions on equivalent Apple first-party apps or services; and (iii) not a disguised exercise of Apple's circumvention of its Conduct Requirement obligations;

(iii) Issue a binding decision within 30 Business Days of referral, which Apple must implement within 5 Business Days;

(iv) Have access to, and Apple must provide, all internal App Review records, communications, and decision logs relating to the appealed decision.

An internal App Review Board may remain available as a first-stage option but shall not constitute a bar to referral to the external independent appeal mechanism. Developers may proceed directly to the independent appeal mechanism following any initial rejection.

Loophole-AR4: Apple's Commitment states its Guideline changes can become effective on the same day they are announced.

Paragraph 7(b) says Apple will "*announce any material changes to the Guidelines to developers on the same day such changes become effective*." One week's advance notice is only committed for App Store search algorithm changes (see below), not for Guideline changes. Developers may therefore face immediate compliance obligations on revised rules with no transition period. This is a notable asymmetry of information necessary for rivals to maintain compatibility with Apple's mobile OS.

Proposed Conduct Requirement App Review (CR AR-4):

Apple must provide developers with a minimum transition period before any amendment to the Guidelines (other than emergency changes under CR AR-1) takes effect. The transition periods are:

(i) For amendments that increase compliance obligations or restrict app functionality previously permitted: no less than 30 calendar days from the date of announcement;

(ii) For amendments that introduce new categories of app, feature type, or business model into scope of the Guidelines: no less than 60 calendar days from the date of announcement;

(iii) For amendments that reduce compliance obligations or expand permissions for app features: no minimum period, but must be effective no earlier than the date of announcement;

During any transition period, Apple must continue to process submissions under both the old and new Guidelines and must accept submissions made under either, notifying the developer which version was applied. Apps rejected solely for non-compliance with a new Guideline provision during the transition period must be given a grace period extension equivalent to the unexpired portion of the transition period.

Loophole-AR5: Apple Commitments propose providing metrics that are aggregated and unreasonably limited in scope, rather than developer-specific to all impacted developers.

Annual metrics under paragraph 9 are published at an aggregated level for "*UK-based app developers*." As the CMA has noted in its SMS Search designation of Google, the appropriate geographic scope is

for UK residents using Apple mobile OS devices, rather than only UK-based app developers, content owners or rival service providers. Given Apple does not consider its own apps as being coded by a UK-based app developer, it would be unfair on rivals to limit protections to only the subset of firms that would be classified as "UK-based app developers." The proper definition of impacted developers is any developer whose apps are listed on the UK App Store storefront.

Moreover, Apple's Commitments propose that Apple not be required to provide any developer with information about their own relative rejection or approval rate compared to Apple first-party apps or competitor apps. Detecting discriminatory patterns from aggregated statistics alone is and would be practically very difficult.

Proposed Conduct Requirement App Review (CR AR-5):

In addition to the aggregated annual metrics published under Apple's commitments, Apple must publish and provide to the Independent Monitor the following disaggregated data, updated on a quarterly basis:

(i) Rejection rates by app category (using Apple's own category taxonomy), including for each category the equivalent rate for Apple first-party apps in the same category;

(ii) Mean and median review time by app category and by whether the app competes with an identified Apple first-party service;

(iii) Distribution of Guideline provisions cited in rejections, enabling identification of provisions that are disproportionately applied to categories where Apple has first-party competitive interests;

(iv) External independent appeal mechanism appeal outcomes by app category and by Apple vs. third-party equivalent;

The Independent Monitor shall independently analyse this data annually and report to the CMA any statistically significant differential treatment between Apple first-party and third-party apps in equivalent categories.

Loophole-AR6: Apple offers no commitment on the substantive content of rejection reasons.

Paragraph 6(b) requires Apple to "*provide the developer with an explanation of how its submission contravenes the Guidelines*." This is a process obligation, not a substantive one. Apple may cite a Guideline provision without explaining the underlying reasoning in any depth. There is no requirement that explanations be sufficient to enable meaningful challenge or that they be reviewed for adequacy. Apple's proposed commitments request CMA blessing to cement its unilateral decision-making to reject or revoke developer accounts, apps, or even entire alternative app marketplaces without a fair appeal process to an independent authority or CMA oversight. This allows de facto blocking of rivals (e.g., sideloading Epic or Meta stores), undermining open distribution.

Proposed Conduct Requirement App Review (CR AR-6):

The CMA shall appoint an Independent Monitor for App Review within 90 days of these CRs taking effect. The Independent Monitor shall have:

(i) Full, unescorted access to Apple's App Review systems, internal documentation, training materials, and personnel records on reasonable notice;

(ii) The power to conduct confidential interviews with App Review staff, App Review Board members, and Apple senior management;

(iii) Authority to commission independent technical testing of App Review consistency, including submission of test apps designed to probe potential differential treatment.

Apple must bear the reasonable costs of the Independent Monitor, paid through a mechanism that does not create any financial relationship between the Independent Monitor and Apple that could compromise independence. The Independent Monitor shall report annually to the CMA and publish a public summary.

8.2 Apple's discriminatory search results process is self-policed with no objective benchmarks

Apple includes mentions a "self-preferencing" prohibition, which is only self-policed with no objective benchmark.

Loophole-SR1: Apple's Commitments claim it will disclose any self-preferencing conduct.

Paragraph 1 commits Apple not to "*self-preference Apple's own first-party apps*" in search. Yet Apple both trains the algorithm and assesses whether training reflects self-preferencing. There is no independent audit of search outputs against a non-Apple-designed standard. The commitment that human assessors operate "*independently from teams responsible for Apple's apps and services*" (paragraph 2(a)) does not prevent Apple from designing the assessment rubric in a way that systematically advantages Apple apps without any overt instruction to do so.

Proposed Conduct Requirement Search Results (CR SR-1):

Apple must engage, at its cost, a technically qualified independent auditor approved by the CMA, to conduct a bi-annual audit of the App Store search algorithm and presentation of results. Each audit must:

(i) Submit a standardised battery of test queries across at least 20 app categories, including categories where Apple operates a competing first-party app, and compare organic search rankings for Apple first-party and equivalent third-party apps;

(ii) Assess whether statistical evidence of self-preferencing exists, applying a significance threshold to be agreed with the CMA;

(iii) Assess whether any correlation exists between a developer's App Store Search Ad spend and that developer's organic search ranking for equivalent queries;

(iv) Review the training data and human assessor instructions used to train the algorithm and assess whether any features of those instructions systematically favour Apple first-party apps;

The independent auditor's report shall be delivered simultaneously to Apple and the CMA. The CMA shall publish a non-confidential summary. Apple may provide factual corrections within 10 Business Days.

Loophole-SR2: No meaningful advanced notice on even changes intentionally designed to self-preference Apple's competing solutions.

Apple's mention of advance notice for algorithm changes is only "***approximately** one week*" and applies narrowly. Paragraph 3(b) commits to approximately one week's notice only for "*major changes*" to inputs or presentation. What constitutes a "major" change is unilaterally determined by Apple. Moreover, intentional incremental algorithmic drift, which could progressively disadvantage third-party developers without any single "major" change, will as such require no notice at all.

Proposed Conduct Requirement Search Results (CR SR-2):

Apple must disclose to the CMA, on a confidential basis and updated annually, a sufficiently detailed technical description of the App Store search algorithm to enable meaningful independent assessment of self-preferencing risk. This disclosure must include:

(i) The relative weighting or ordering of priority assigned to each disclosed factor (text relevance, customer behaviour, ratings, engagement signals, etc.) used in the organic ranking model;

(ii) A description of any separate ranking layer, boost, or filter applied to Apple first-party apps, including any feature that uses Apple's identity as a signal;

(iii) A description of the mechanism, if any, by which App Store Search Ad spend influences organic ranking signals, including any shared feature pipeline.

Apple may apply for CMA confidentiality protection for commercially sensitive elements of this disclosure; the CMA shall not publish the detailed disclosure but shall make it available to the independent auditor.

Loophole-SR3: No transparency as to how substantively compete in search rankings.

Apple offers no commitments to disclose its algorithm's actual weighting or logic. Paragraph 3(a) commits to publishing "*key factors*" bearing on relevance, but the weighting assigned to those factors is not required to be disclosed. Knowing that "*text relevance*" and "*customer behaviour*" are factors does not tell developers how they are balanced, or how new signals like paid advertising interact with organic search. Moreover, Apple does not offer any obligation to disclose whether and how participation and spend with its Apple Ads will be used to influence organic rankings.

Proposed Conduct Requirement Search Results (CR SR-3):

Apple must ensure that a developer's expenditure on App Store Search Ads does not, directly or indirectly, influence that developer's organic search ranking for equivalent queries. In particular:

(i) Apple must maintain strict separation between the features and signals used to determine paid placement and those used to determine organic ranking;

(ii) Apple must not apply any engagement signal derived from paid ad impressions or clicks to the organic ranking model;

(iii) Apple must clearly and persistently label all paid placements in search results in a manner that a user of ordinary attention would recognise as advertising, distinguishing paid from organic results.

This obligation applies with equal force to Apple's own use of any equivalent to Search Ads for its first-party apps.

Loophole-SR4: Paid App Store advertising is not addressed.

Apple limits its commitments to address only organic search. Apple generates significant revenue from Search Ads, which appear at the top of App Store search results. The relationship between paid placement and organic ranking, or whether high advertising spend correlates with improved organic visibility, is omitted from any obligations within the scope of Apple's proposed commitments. This is a significant gap given the CMA's concern about leveraging.

Proposed Conduct Requirement Search Results (CR SR-4):

Apple must notify the CMA and the independent Algorithm Auditor of any planned change to the App Store search algorithm that satisfies any of the following objective criteria, regardless of whether Apple characterises the change as "major":

(i) Any change to the relative weighting of organic ranking factors that alters the weight of any single factor by more than 10 percentage points;

(ii) Any introduction of a new ranking signal or feature category not previously disclosed;

(iii) Any change to the mechanism by which paid advertising interacts with organic signals;

(iv) Any change to the human assessor instructions that modifies the criteria by which app quality or relevance is assessed.

Notification must be provided at least 20 Business Days before implementation. The Algorithm Auditor may request a targeted interim review within that period. Changes subject to this obligation must not be implemented until notification obligations have been satisfied.

Loophole-SR5: The bi-annual confidential reports are not subject to independent audit.

Apple proposes in Paragraph 5 to submit bi-annual confidential reports to the CMA. However, these reports are prepared by Apple and there is no commitment to allow the CMA or an independent expert to run counter-tests on the algorithm results or to audit algorithmic outputs directly. The CMA's ability to monitor depends entirely on what Apple chooses to report. A more reasonable approach is for Apple to make transparent to developers whose apps are listed in the UK App Store storefront with the information necessary to adjust their solutions to be discovered and accessible by UK residents who select devices that rely on iOS.

Proposed Conduct Requirement Search Results (CR SR-1):

Apple must provide developers whose apps are listed on the UK App Store storefront with access to analytics that enable the developer to:

(i) Identify the search queries for which their app appears in organic results and their ranking position for each query;

(ii) Track ranking position over time and receive notification when their ranking changes by more than a defined threshold for a material search query;

(iii) Understand, at a category level, how their app's ranking compares to the mean ranking for apps in the same category.

This analytics access must be no less granular than the equivalent analytics access enjoyed by Apple's own first-party app teams.

8.3 Apple's discriminatory restrictions on Data Use

Loophole-DU1: Apple's Commitments covers only "data submitted as part of App Review," not operational App Store data more broadly.

Paragraph 1 restricts its scope to data submitted during App Review. The CMA's SMS investigation was concerned with a wider category of data use, namely, Apple's use of data collected "through its operation of the App Store." Fair access and use of this commercial data, market intelligence, and behavioural data derived from running the App Store platform is critical to restoring competition in digital markets. That broader concern is acknowledged in the Introduction (paragraph 1(3)) but the substantive commitments in section III cover only App Review submission data. Apple omits to constrain its use of App Store transactional or commercial data and competitive intelligence to inform its own product strategy and product developments.

Proposed Conduct Requirement on Data Use (CR DU-1):

The prohibitions and safeguards set out in these CRs shall apply to all non-public third-party data that Apple receives or stores by virtue of its operation of the App Store, including but not limited to:

(i) Developer data submitted as part of App Review;

(ii) Commercial and financial data generated by developer transactions through the App Store, including revenue data, pricing data, and subscriber metrics not publicly disclosed by the developer;

(iii) Behavioural and engagement data concerning user interaction with third-party apps within the App Store environment, including search queries leading to third-party app downloads, conversion data, and user review data before public publication;

(iv) Strategic or market intelligence data generated through Apple's operation of the App Store, including emerging category demand signals, developer pipeline information, and unreleased feature data submitted in test builds.

For the avoidance of doubt, this CR does not restrict Apple's use of data in aggregated, anonymised form for the purpose of improving App Store infrastructure, provided that such data (i) cannot reasonably be used to derive commercially sensitive insights about any identifiable developer and (2) is not communicated to teams involved in developing, marketing, or monetising Apple first-party apps or services.

Loophole-DU2: Section 9.3 DPLA carve-out is weak.

Apple states in Paragraph 2 that it will not apply Developer Program License Agreement Section 9.3 in any way that "*would undermine*" the protections for market players' data in its proposed commitments. This is a negative obligation. Apple retains the contractual clause, and the commitment merely promises not to use it against the stated data protections. It does not require Apple to amend or remove Section 9.3, meaning Apple retains the contractual right to rely on it for purposes outside the narrow scope of these commitments.

Proposed Conduct Requirement on Data Use (CR DU-2):

Apple must not use any non-public third-party data, whether directly or indirectly, to:

(i) Inform the development, feature prioritisation, or commercial strategy of any Apple first-party app or service;

(ii) Inform any pricing or commercial decision by Apple in relation to its own app, service, or hardware products;

(i) Inform any decision by Apple to enter, expand into, or withdraw from any product category in which a third-party developer operates.

This prohibition applies regardless of whether the data is processed directly or is fed into a machine learning model, algorithmic system, or other intermediate process used in Apple product development

Loophole-DU3: "Legal review" of data access is internal.

Paragraph 1(b) provides that access to tagged developer data requires "*legal review to confirm the business purpose*." That legal review is conducted by Apple's own legal compliance personnel. There is no external validation, no independent compliance officer, and no requirement to report access events to the CMA in real time. The adequacy of Apple's internal access controls is unverifiable from outside.

Proposed Conduct Requirement on Data Use (CR DU-3):

Within 60 days of these CRs taking effect, Apple must amend the Developer Program License Agreement (DPLA) to:

(i) Expressly prohibit Apple from using data submitted in connection with App Review for competitive intelligence purposes consistent with CR DU-2;

(ii) Remove or modify any provision — including but not limited to Section 9.3 — that purports to grant Apple a licence to use developer confidential information in a manner inconsistent with these CRs;

(iii) Include an express covenant by Apple not to use App Store operational data for competitive purposes as defined in CR DU-2.

Apple must submit the amended DPLA to the CMA for review before publication. The CMA shall have 20 Business Days to raise objections. Apple must address any objections raised before the amended DPLA takes effect.

Loophole-DU4: No remediation obligation if a breach is discovered.

The commitments set out safeguards, training, and monitoring but contain no provision for what happens if Apple's own audit reveals that third-party data has been accessed for competitive purposes in breach of the commitments. There is no self-reporting obligation to the CMA upon discovery of a breach, no remediation protocol, and no commitment to notify affected developers.

Proposed Conduct Requirement on Data Use (CR DU-4):

Apple must appoint an Independent Data Auditor approved by the CMA to oversee access to any non-public third-party data. The auditor shall:

(i) Maintain daily real-time read access to Apple's Protected Data access logs;

(ii) Review a statistically representative sample of access requests on a quarterly basis to assess whether the business purpose stated is consistent with CR DU-2;

(iii) Have authority to require Apple to provide, within 5 Business Days, full documentation of any access event the auditor selects for detailed review;

(iv) Report any access event that, in the auditor's reasonable opinion, may constitute a breach of CR DU-2 to the CMA within 2 Business Days of forming that opinion.

Apple must cooperate fully with the auditor and may not restrict, delay, or condition the auditor's access. The auditor's reasonable costs shall be borne by Apple through a mechanism that preserves the auditor's independence.

8.4 Apple's omission on interoperability obligations

Loophole-I1: Apple omits any obligation to grant any interoperability request and Apple's proposed assessment criteria are heavily weighted in Apple's favour.

Paragraph 2(c) states explicitly that the receipt of a request "*will not create any obligation or expectation that Apple will commit to building a specific requested feature*." Apple retains complete discretion to refuse any and all requests. The commitment is purely procedural: a channel is created and criteria are published, but there is no substantive obligation to provide access to anything.

The CMA's Roadmap concern was that Apple would be *required* to "*fairly and objectively consider*" requests. In the proposed commitments, Apple provides a process for mere consideration but Apple remains the sole decision-maker on the outcome, with no appeal and no external review of whether a refusal is objectively justified.

The criteria in paragraph 2(b) include "*alignment with Apple's platform priorities*," "*potential impact on Apple's intellectual property rights*," and "*potential implementation costs*." These are criteria Apple scores on its own behalf. A request could satisfy genuine developer and user need but be refused because Apple determines it conflicts with its own priorities or IP, precisely the competitive self-preferencing concern the SMS designation exists to address.

Proposed Conduct Requirement on Interoperability (CR I-1):

Apple may refuse an interoperability request only where it can demonstrate, to the standard required by the CMA on a reasoned written assessment, that one or more of the following grounds applies and that the refusal is proportionate to the concern identified:

(i) Granting the request would create a material and evidence-based risk to consumer safety, device security, or privacy that cannot be addressed through reasonable technical or organizational mitigation;

(ii) Granting the request is technically infeasible given current iOS/iPadOS architecture, with Apple providing a technical assessment to the CMA;

(iii) Granting the request would require Apple to redesign core OS functionality in a manner disproportionate to any reasonable estimate of developer or consumer benefit;

The following grounds shall NOT constitute a valid basis for refusal: (i) "alignment with Apple's platform priorities"; (ii) impact on Apple's competitive position in a market where Apple operates a competing service; (iii) the possibility that granting access would reduce developer dependency on

Apple's ecosystem. Apple's commercial interests shall not be counted as a factor in the proportionality assessment.

Loophole-I2: Apple limits its scope to "equivalent system and hardware functionality used by Apple services or accessories."

Paragraph 2(a) limits eligible requests to functionality Apple already exposes to its own services or accessories. This means developers cannot request access to capabilities that Apple has not already chosen to use itself, even if the underlying hardware and OS would support such access. The scope is thereby determined by Apple's prior choices, not by the reasonable needs of the developer ecosystem. Features Apple has deliberately left internal (to protect its competitive position) remain inaccessible regardless of their importance to third-party innovation.

Proposed Conduct Requirement on Interoperability (CR I-2):

The scope of eligible interoperability requests shall not be limited to functionality currently used by Apple's own products and services. Eligible requests shall include any request for access to:

(i) Hardware capabilities of Apple devices that are accessible to the iOS or iPadOS operating system layer, regardless of whether Apple has previously exposed them to third parties;

(ii) OS-level APIs, frameworks, or system services that are accessible to Apple's own apps, whether or not those apps are publicly available to consumers or developers;

(iii) Any functionality that the requesting developer can demonstrate is technically achievable on existing Apple hardware and iOS/iPadOS software without requiring Apple to develop new hardware capabilities.

Where a request falls outside this scope solely because Apple has elected not to expose a technically available capability to any party (including its own apps), Apple must explain in its reasoned refusal why the technical capability has been withheld from all third parties in conformity with the reasons in CR-I-1.

Loophole-I3: Apple offers no enforceable timeline for a substantive decision.

Paragraph 1(c) commits Apple to providing "*an update on the status*" of a request within four weeks. An "update on status" is not a substantive decision, it could simply be confirmation that the request is still under review. There is no deadline by which Apple must actually decide whether to grant or refuse a request, meaning requests can be indefinitely deferred.

Proposed Conduct Requirement on Interoperability (CR I-3):

Apple must issue a substantive written decision on each eligible interoperability request within the following periods from the date of receipt of a complete request:

(i) Standard requests: 8 weeks;

(ii) Complex requests (as designated by Apple in a written notification to the requesting developer within the first 4 weeks): 16 weeks;

(iii) Requests relating to real-time communication, push notifications, VoIP, NFC, or digital wallet functionality: 8 weeks.

A substantive decision must include: (i) an unambiguous grant or refusal; (ii) if a grant, a clear implementation timeline; (iii) if a refusal, a written justification by reference to the grounds in CR I-1. Failure to issue a decision within the applicable period shall be treated as a refusal, engaging the developer's right to appeal under CR I-4. Any unreasonable implementation timeline, especially for functionality Apple's own products and services rely on shall be treated as a refusal, engaging the developer's right to appeal under CR I-4.

Loophole-I4: Apple offers no independent process for any appeal.

Apple's Commitments fail to offer developers access to any independent appeals process for its unilateral decisions. Under Apple's proposal, it can reject requests without substantive justification or even accepts requests with timelines that exceed reasonable implementation needs. Moreover, there is no penalty to Apple to deny all requests purely on the basis that accepting them may compete with Apple's own products and services, and hence not align "with Apple's platform priorities," which is exactly the use case the SMS designation was specifically designed to address.

Proposed Conduct Requirement on Interoperability (CR I-4):

Developers whose interoperability requests are refused (expressly or by Apple's failure to decide within the applicable period in CR I-3) may appeal to an independent appeals panel appointed by the CMA. This panel shall:

(i) Include at minimum one independent technical expert in mobile platform architecture and one independent competition economist;

(ii) Have access to Apple's technical documentation, architecture diagrams, and internal assessments of the refused request;

(iii) Issue a recommendation within 30 Business Days, applying the grounds in CR I-1 and assessing whether Apple's stated justification is technically sound and proportionate;

(iv) Transmit the recommendation to the CMA, which may direct Apple to grant access if the panel's recommendation is that the refusal was not justified.

Apple must comply with any CMA direction to grant interoperability access within the timeframe specified by the CMA, which shall not exceed 3 months for standard functionality and 6 months for functionality requiring significant engineering work.

Loophole-I5: Apple unreasonably limits scope to "UK-only" developer eligibility.

Apple proposes that its feedback channel should be available to only Developer Program members registered in the UK. Yet many of the most significant interoperability barriers affect global app developers whose UK operations are registered elsewhere. The UK developer community is not the only party with a legitimate interest in iOS interoperability, and restricting the channel geographically limits the breadth and diversity of requests that inform the process.

Proposed Conduct Requirement on Interoperability (CR I-5):

Valid requests for interoperability may be made by any developers whose apps are listed on the UK App Store storefront or service providers that support such developers.

Loophole-I6: Apple's ongoing asymmetry of access to technical information required for fair competition.

Apple offers no commitments to share critical technical documentation, API specifications, or architectural information proactively to help developers formulate requests. Developers may not know what functionality exists or how to request it with sufficient specificity to qualify as an "eligible" request. The information asymmetry between Apple and third-party developers is a core barrier to effective interoperability, and the commitment does nothing to reduce it.

Proposed Conduct Requirement on Interoperability (CR I-6):

To reduce information asymmetry and enable developers to formulate meaningful interoperability requests, Apple must publish and maintain:

(i) A comprehensive register of all iOS/iPadOS APIs and system capabilities that are available to any Apple first-party app or supporting service but not currently exposed in the public SDK, updated at each major iOS release;

(ii) For each capability in the register, an indication of: (i) whether it is in principle eligible for third-party access; (ii) if not eligible, the specific justification by reference to the grounds in CR I-1;

(iii) Technical documentation for each eligible capability sufficient to enable a competent developer to formulate a specific and technically grounded interoperability request.

Publication of the register and documentation must be made to the CMA 30 days before public release to allow the CMA to comment on completeness.

8.5 Conduct Requirements necessary to restore real-time communication needed for effective competition

The following CRs address the specific interoperability gaps most critical to restoring competition on mobile platforms. The functionalities required for app developers and competing service providers to ensure regulators do not unduly favour vertically integrated firms include: real-time communication using open web-standards, open instant messaging support, payment processing, and web content rendering functionality. These are areas where the CMA's SMS investigation has identified active competitive harm from Apple's restrictions. All conduct requirements to restore real-time communication and supporting services that rely on this communication must be implemented by Apple within 6 months.

Conduct Requirement to restore competition by supporting Real-time Communication using open web standards

Apple's ability to abuse its dominance in Mobile Platforms is only possible by removing support for real-time communication using open web standards from both web content rendering engines and mobile apps. By removing rival market players' ability to use such standards for real-time communication, Apple coerces them to use its proprietary APIs that require compliance with its unilaterally dictated terms of services.

Requiring Apple to reestablish support for such real-time open web standards would allow other market players to compete with Apple's own products and services on a more level playing field.

Web standards including WebRTC, Web Push, WebAssembly, and Web Bluetooth/NFC underpin a generation of real-time communication and productivity applications that compete directly with Apple's native-app ecosystem. By controlling and restricting WebKit's pace of standards implementation and imposing iOS-specific sandboxing restrictions on web apps, Apple creates asymmetry. Apple's native apps benefit from full OS integration while web-based competitors face artificial capability ceilings.

The CMA has found that Apple's selective and delayed implementation of open web standards within WebKit has suppressed competition in Mobile Platforms and rival market players' services with those provided by Apple, including its native apps and business services.

Proposed Conduct Requirement on Real-time Communication (CR RTC-1):

Apple must ensure that WebKit on iOS and iPadOS implements, on a complete and non-discriminatory basis, the following web standards to the extent technically achievable on Apple hardware:

(i) WebRTC: Full implementation of the W3C WebRTC specification, including RTCPeerConnection, MediaDevices, getDisplayMedia, and insertable streams;

(ii) Web Push API: Full implementation on parity with desktop Safari, including background delivery without requiring the PWA to be foregrounded or the device unlocked, notification badges, silent push for background sync, and removal of any iOS-specific requirement that a user add a PWA to their home screen before Web Push is activated;

(iii) WebAssembly: Full support including SIMD, threads, and tail calls, consistent with the W3C WebAssembly specification;

(iv) WebTransport and WebSockets: Full support with no iOS-specific connection count restrictions or timeout policies that are more restrictive than those in desktop Safari;

(v) Web Bluetooth and Web NFC: Full implementation of the open standard specifications;

Apple must apply any privacy design choices equally to both on-device and cloud-based software and first-party and third-party software. Where Apple does not implement a web standard within 3 months of each finalised standard update, Apple must: (i) notify the independent monitor and the CMA 60 days before an equivalent Apple-proprietary native capability launches; (ii) provide a written technical justification for non-implementation; and (iii) submit to an independent appeals panel review within 30 days of a CMA request.

Conduct Requirement to restore competition by in web rendering engines

Apple requires all third-party browsers on iOS and iPadOS to use its WebKit rendering engine, enforced through App Review Guidelines section 2.5.6 and the Developer Program License Agreement. The consequence is that no browser on iOS, regardless of brand, feature set, or cross-platform capabilities can use Blink (available in Chrome on other operating systems) or Gecko (available in Firefox on other operating systems).

The CMA's SMS designation specifically encompasses Apple's mobile browser and browser engine. The WebKit restriction, which requires all iOS browsers to use Apple's rendering engine, is identified in the Roadmap as a Category 1 concern.

The CMA's SMS Designation identified this restriction as a Category 1 concern for three compounding reasons. First, it eliminates genuine browser competition. Chrome on iOS is WebKit with Chrome's UI, not Chrome's engine. Second, it denies rival browser engines the iOS scale and feedback data necessary

to compete with WebKit. Third, by controlling WebKit's pace of development, Apple restricts and controls the capability ceiling for all iOS browsers, entrenching Safari's advantage. A fourth concern is that WebKit engine restrictions suppress web app quality, reducing the competitive constraint web apps impose on native App Store apps, and therefore sustaining App Store commission dependency.

Apple's commitments say nothing about it. Third-party browsers remain locked into WebKit, meaning Apple retains complete control over what web technologies are available on iOS, constraining both browser competition and the viability of web apps as alternatives to native apps.

Proposed Conduct Requirement on Real-time Communication (CR RTC-2):

Apple must, within 12 months of these CRs taking effect, remove the requirement imposed through App Review Guidelines section 2.5.6 and any equivalent DPLA provision that third-party browsers must use the WebKit rendering engine. Following removal, Apple must:

(i) Permit browser developers to distribute browsers using any rendering engine (including Blink, Gecko, or any other) on the iOS and iPadOS App Store;

(ii) Not apply any App Review criterion that has the effect of requiring WebKit, or that imposes requirements technically achievable only by WebKit-based browsers;

(iii) Not apply any commission rate, revenue share, or App Store Terms less favourable to non-WebKit browsers than to WebKit browsers;

(iv) Provide browser developers using non-WebKit engines with access to the same iOS APIs, hardware accelerators, JIT compilation privileges, and sandboxing capabilities as are available to Safari and WebKit-based browsers, subject to CR WK-2;

General assertions that alternative engines are less secure than WebKit shall not constitute a valid justification for maintaining any restriction. Apple must identify the specific, evidence-based vulnerability in the alternative engine as deployed on iOS before any engine-specific restriction may be imposed.

Conduct Requirement to restore competition for Alternative App Stores

The CMA's designation encompasses native app distribution. The Roadmap explores requiring Apple to permit alternative app stores and sideloading. Apple's commitments are silent on alternative distribution entirely, meaning Apple's App Store retains its monopoly over iOS app distribution in the UK.

Proposed Conduct Requirement on Real-time Communication (CR RTC-1):
Apple must, within 12 months of these CRs taking effect, implement the technical and contractual changes necessary to permit alternative app store operators to distribute apps. Apple must:

(i) Provide a documented technical mechanism by which an alternative app store can distribute apps without those apps passing through Apple's App Store or App Review;

(ii) Enable iOS to install apps distributed through the alternative app store's installation mechanism, requiring only the user's affirmative consent at first installation of the alternative app store itself, not at each subsequent app install;

(iii) Provide alternative app store access to the same iOS APIs, background execution privileges, push notification access, and system integration as are available to Apple's App Store, including the ability to provide automatic app updates;

(iv) Not require any alternative app store to route user payments through Apple's payment systems, or pay Apple any per-transaction or per-install fee as a condition of marketplace operation, beyond a one-time annual certification fee that is cost-reflective, non-discriminatory, and CMA-approved;

(v) Not restrict the categories of apps an alternative app store may distribute.

Apple must publish full technical documentation for alternative marketplace integration within 6 months of these CRs taking effect.

Conduct Requirements to prohibit deterrence mechanisms for competitive service provider

Apple's imposition of its Core Technology Fee ("**CTF**") deters operations of rival app marketplaces, given the per-install fee scales massively for popular apps, pricing out competitors. Apple's own App Store can thus distribute apps more cheaply than rivals, creating asymmetric barriers the CMA flagged in its app distribution concerns.

Proposed Conduct Requirement on Real-time Communication (CR RTC-1):

Apple must not impose any fee, charge, technical restriction, or contractual obligation on alternative app store operators or on developers distributing through alternative marketplaces that has the purpose or effect of deterring establishment or use of alternative marketplaces. Apple must not:

(i) Impose any per-install, per-download, per-user, or per-transaction fee on apps distributed through alternative marketplaces unless an identical fee is charged on an equivalent per-install or per-transaction basis for App Store-distributed apps — and then only at the equivalent rate;

(ii) Require developers distributing through alternative marketplaces to maintain their app on the Apple App Store, or to offer equivalent or better pricing there;

(iii) Apply slower API access, system update access, or less favourable developer programme terms to developers distributing primarily through alternative marketplaces;

(iv) Present users with warning dialogs, friction screens, or consent flows when installing apps from a QMO that are more prominent or alarming than those presented for equivalent actions within the Apple App Store;

(v) Apply technical restrictions or limitations, including storage, background processing, or API access restrictions, to marketplace-installed apps that do not equally apply to equivalent App Store-installed apps;

The independent monitor shall monitor alternative marketplace take-up in the UK bi-annually and report to the CMA on whether any Apple conduct is having a deterrent effect.

Conduct Requirements to restore competition given Apple's excessive App Store commissions and unfair steering

The CMA's Roadmap identifies as a Category 1 (highest priority) intervention "*requiring that Apple allows app developers to direct their potential customers off the App Store*" to alternative payment channels. The CAT has found Apple's commissions to be excessive and unlawful.

None of these issues are addressed. Apple makes no commitment on commission levels, no commitment to allow out-of-app linking, and no commitment to permit developers to communicate pricing alternatives to users within their apps.

Apple charges developers 30% on in-app purchases and subscriptions processed through its mandatory In-App Purchase ("**IAP**") system (15% for qualifying small businesses and for the second year of a subscription). Developers are prohibited by the DPLA and App Review Guidelines from: (i) using a third-party in-app payment system; (ii) communicating within their app that lower prices are available elsewhere; (iii) including links to their own website for purchases; or (iv) telling users that App Store prices include Apple's commission.

The Competition Appeal Tribunal found in its October 2024 collective proceedings judgment that Apple's commission rates were excessive and its anti-steering restrictions unlawful. Apple has appealed, but the ongoing competition harm must be remedied during the appeals process. The CMA's SMS Designation Roadmap identified commission levels and anti-steering restrictions as Category 1 concerns. Apple's commitments of 10 February 2026 are entirely silent on both. These CRs address the commission structure and its associated anti-competitive restrictions together, as they are interdependent: the anti-steering rules are the mechanism by which Apple prevents competitive pressure from reducing its commission.

Proposed Conduct Requirement on Data Use (CR RTC-1):

Apple must, within 6 months of these CRs taking effect, remove all App Store Guidelines, DPLA provisions, and technical restrictions that prohibit or discourage developers from:

(i) Integrating a third-party in-app payment processor as an alternative to, or in addition to, Apple IAP;

(ii) Offering users the option to complete a purchase using a payment method of their choice, including browser-based checkout, third-party payment apps, or external payment links;

(iii) Displaying different prices based on the payment method chosen by the user, where pricing differences reflect genuine cost differences.

Where a developer uses Apple IAP, Apple may charge its commission on IAP-processed transactions. Where a developer uses a third-party processor or external purchase link, Apple may charge only a commission that is:

(i) **Cost-reflective**: reflecting only genuine incremental costs Apple incurs in distributing the app, excluding payment processing costs;

(ii) **Transparent**: set out in a publicly available schedule approved by the CMA;

(iii) **Non-excessive**: benchmarked by the CMA against cost-reflective rates charged by comparable payment processing services and adjusted if found to exceed a reasonable rate of return on Apple's distribution costs.

Apple must immediately remove from the App Store Guidelines and DPLA all provisions that:

(i) Prohibit or restrict a developer from including within their iOS app a link, button, or in-app message directing users to a webpage where a purchase can be completed at a different price from the App Store price;

(ii) Prohibit or restrict a developer from communicating to users within their app that: (i) a lower price is available through an alternative channel; (ii) the App Store price includes a commission charged by Apple; or (iii) equivalent functionality is available through the developer's website or another platform;

(iii) Require that the developer's App Store price be no higher than prices for equivalent content on any other platform or channel (most-favoured-nation clauses — addressed separately in CR COM-4);

(iv) Restrict the developer from providing promotional pricing, offers, or bundles to users who purchase through non-Apple channels that are not simultaneously available on the App Store;

During the implementation period, Apple must not enforce any existing anti-steering provision against any app developer whose apps are listed on the UK App Store storefront.

Conduct Requirement to restore competition for Push Notification

Proposed Conduct Requirement on Real-time Communication (CR RTC-1):

Apple must ensure that access to the Apple Push Notification Service ("**APNs**") is provided to all third-party messaging, communications, and notification-dependent apps on terms that are:

(vi) No less favourable in terms of latency, reliability, rate limits, and delivery guarantees than the terms on which APNs is made available to Apple's own first-party messaging and communications apps (including iMessage, FaceTime, and Mail);

(vii) Not subject to additional payload restrictions or content inspection requirements beyond those imposed on Apple first-party apps using the same infrastructure;

(viii) Not contingent on the third-party developer adopting any other Apple technology, framework, or service.

Apple must provide the independent monitor with APNs performance data for Apple first-party and third-party competing communications apps on a quarterly basis to enable monitoring of this obligation.

Conduct Requirement to restore competition for Video and VOIP Communication

Proposed Conduct Requirement on Real-time Communication (CR RTC-2):

Apple must ensure that CallKit and any successor or equivalent telephony integration framework is made available to third-party VoIP and communications apps on the following terms:

(i) Equivalent OS integration as enjoyed by Apple's own FaceTime, Phone, and first-party communications apps, including integration with the lock screen, Siri, CarPlay, and system audio routing;

(ii) Equivalent background processing privileges to maintain call state, receive incoming calls when the app is not in the foreground, and manage call handover;

(iii) Access to any new or enhanced telephony capability introduced in future iOS versions no later than the date Apple makes equivalent capability available to its own apps.

Any restriction on the above must be justified by specific, documented user safety or security grounds under CR I-1 and approved by the independent monitor before implementation.

Conduct Requirement to restore competition for Instant Messaging

Proposed Conduct Requirement on Real-time Communication (CR RTC-3):

Apple must implement technical interoperability between iMessage and third-party messaging apps operating on iOS that request access under this CR, such that:

(i) Users can receive and respond to messages from iMessage contacts without leaving a third-party messaging app of their choice, on a functionally equivalent basis to the iMessage native experience;

(ii) iMessage delivery receipts, read receipts, and typing indicators are made available to third-party apps using a documented API on equal terms; and

(iii) Apple does not apply preferential compression, encryption overhead, or delivery priority to iMessage traffic relative to third-party messaging traffic over equivalent network conditions on-device.

Apple must maintain RCS support consistent with industry standards and must not implement RCS features in a manner that disadvantages third-party RCS-capable messaging apps relative to iMessage. This obligation is without prejudice to Apple's right to offer iMessage-specific features that are technically dependent on the iMessage protocol.

Conduct Requirement to restore competition for Near Fear Communication (NFC) services

The CMA's Roadmap specifically contemplates addressing Apple's restrictions on digital wallets and NFC access, identified as an important FinTech concern. Apple's proposed commitments contain no provision on wallet access or NFC interoperability.

Proposed Conduct Requirement on Real-time Communication (CR RTC-4):

Apple must provide third-party apps (e.g., digital wallet, payment processing, and access control) with access to the mobile platform NFC controller on the following terms:

(i) Full NFC read/write capability, Host Card Emulation ("**HCE**"), and contactless payment card emulation (including EMV-mode emulation) equivalent to the functionality available to Apple Pay and Wallet;

(ii) Access to the Secure Element or an equivalent secure execution environment for cryptographic operations necessary for payment card and transit card emulation, on terms no less secure and no less convenient than Apple Pay's own access;

(iii) Express Mode functionality (tap-to-pay without device unlock) for third-party transit and access control apps on the same terms as Apple Wallet's Express Mode;

(iv) No fee charged to third-party wallet providers for NFC access.

Apple must publish and maintain complete NFC API documentation consistent with the technical disclosure obligation in CR I-6. Any restriction on NFC access must be justified under CR I-1 and reviewed by the independent panel within 30 days of the restriction taking effect.

Conduct Requirement to restore competition for broader generative AI services

The CMA explicitly flagged AI as a forward-looking area of concern, such as Apple Intelligence, Siri, and their relationships to third-party app developers, raising nascent but significant gatekeeper concerns. Apple's commitments are entirely silent on AI.

Proposed Conduct Requirement on Real-time Communication (CR RTC-5):

Apple must ensure that Siri's voice activation, intent routing, and on-device AI capabilities are available to third-party app categories that compete with Apple first-party services on the following terms:

(i) Third-party apps (e.g., messaging, VoIP, music, podcast, navigation, and payment apps) must be eligible to receive default Siri intent routing on user instruction, without requiring the user to explicitly invoke the third-party app by name for each query;

(ii) User-designated default apps in any Siri-supported category must receive equivalent Siri integration depth as Apple's own default apps in the same category, including proactive suggestions, contextual awareness, and lock screen access;

(iii) Where Apple Intelligence (or any successor Apple AI generative service) is used to summarise, prioritise, or present communications, notifications, or content from third-party apps, Apple must apply the same quality of on-device AI processing and data access to third-party app services as is made available to equivalent Apple's services.

This CR shall not require Apple to disclose proprietary model weights. It requires parity of outcome, not parity of technical implementation.

Conduct Requirement to restore competition by providing for Consumer Persistent Choice Architecture

The CMA's Roadmap contemplates requiring that "choice architecture in relation to digital wallets and browsers supports active user choice." Apple does not mention default settings, browser choice screens, or other default app selection flows anywhere in its proposed commitments.

Proposed Conduct Requirement on Real-time Communication (CR RTC-6):

Apple must implement and maintain user-facing default settings that enable genuine substitution of Apple first-party services with third-party alternatives:

(i) Users must be able to set a persistent system default for each of: messaging app, VoIP/calling app, digital wallet, navigation app, and email client; and that default must be respected by all OS-level features, including Siri, Spotlight, Share Sheets, lock screen shortcuts, and CarPlay;

(ii) The user must be presented with a choice screen for each of the above service categories on first setup and on each major iOS version upgrade, using neutral presentation that does not visually distinguish Apple first-party apps from third-party alternatives;

(iii) Apple must not revert user-selected third-party defaults to Apple first-party services following any iOS update without the user's affirmative selection of Apple's services when presented by Apple of its own and a non-discriminatory list of alternatives.

The independent monitor shall review the design of the choice screen and default settings interface annually and may direct Apple to make modifications if the interface employs dark patterns, consent sludge or unfair ranking that undermine genuine user choice.

8.6 Additional and Cross-Cutting Omissions

Notwithstanding the detailed deficiencies identified above, the most serious failing of Apple's and Google's proposed commitments is structural. Taken as a whole, the commitments do not engage with the core sources of market power identified by the CMA's SMS designations, nor do they address the conduct that gives that power its exclusionary effect. Instead, both firms have offered narrowly scoped, process-oriented assurances that leave intact the commercial mechanisms by which competition is foreclosed.

First, the commitments do not address monopoly control over app distribution and monetisation. Apple offers no commitments on alternative app distribution, alternative app stores, or sideloading, and makes no commitment to remove or neutralise deterrence mechanisms such as per-install fees, contractual restrictions, or asymmetric technical friction. Apple's mandatory In-App Purchase requirement, its excessive commissions, and its anti-steering provisions, identified by the CMA and the Competition Appeal Tribunal as among the most serious competition concerns, are entirely absent. Google likewise offers no commitments on Play Store commission levels, Play Billing requirements, or the barriers to market entry created by GMS licensing and OEM bundling. As a result, the single largest channel through which both firms extract rents from developers and suppress price competition remains wholly untouched.

Second, browser and web competition, the principal competitive constraint on native app ecosystems, remains unremedied. Apple offers no commitment to remove its WebKit browser engine restriction, despite the CMA identifying this as a Category 1 concern. Nor does Apple commit to parity in web standards implementation or to restoring the viability of websites and web apps as substitutes for native mobile apps. Google, while permitting alternative engines in principle, offers no commitments to address Chrome's entrenched advantage through default placement, deep OS integration, and service bundling on Android. The result is that the commitments preserve the discrimination against, and degradation of, the open web that has driven developers into proprietary app stores.

Third, adjacent B2B service coercion is entirely unaddressed. Neither firm offers commitments preventing the use of platform control to force adoption of proprietary payment systems, advertising services, attribution frameworks, analytics tools, real-time communication protocols, or AI services. The commitments do not prohibit the use of ranking signals, defaults, data asymmetries, or technical integration advantages that systematically favour a platform's own B2B services over functionally equivalent third-party alternatives. As a result, the central leveraging harm identified by the CMA—where dominance in the mobile platform is used to distort competition in adjacent markets—remains fully operative.

Fourth, interoperability commitments are limited to process transparency and confer no substantive rights. Apple's interoperability proposal creates a request channel but explicitly disclaims any obligation to grant access, imposes assessment criteria weighted toward Apple's own commercial interests, and offers no independent appeal or enforceable timelines. Google offers no corresponding interoperability commitments at all. In neither case is there any obligation to support open standards for real-time communication, payments, browser engines, or device capabilities. Interoperability is thus treated as a discretionary concession rather than a competition remedy.

Fifth, "privacy" and "security" are left undefined and self-judged, despite the CMA's explicit finding that the risk of circumvention through these justifications is high. The commitments do not impose objective, evidence-based definitions, do not require proportionality assessments, and do not ensure symmetry between restrictions imposed on rivals and the firms' own use of equivalent data or

capabilities. This preserves a well-documented loophole through which anticompetitive restrictions can be reframed as consumer protection measures without independent scrutiny.

Sixth, monitoring and enforcement remain fundamentally inadequate. Both firms rely on self-reporting, self-certification, and internally generated metrics. There is no independent technical monitor, no continuous output-based monitoring, no access to algorithms or training data, no binding dispute resolution for developers, and no meaningful pre-implementation notification requirement. The CMA would be required to infer compliance from information curated by the very firms whose incentives are to evade effective constraint.

Finally, Google's proposed response is materially incomplete in scope. While Apple has offered limited commitments in four peripheral areas, Google has offered no equivalent commitments across most SMS concern categories, including browser competition, app distribution, interoperability, payments, AI integration, and B2B service neutrality. Accepting Apple's commitments while Google offers none would entrench asymmetric and ineffective regulation of a coordinated duopoly.

In sum, the proposed commitments do not remedy the harms identified by the CMA's SMS designations. They leave untouched exclusive distribution, excessive commission extraction, browser engine control, anti-steering rules, B2B service leveraging, and the ability to invoke undefined privacy and security justifications to foreclose rivals. The commitments therefore risk delaying effective intervention while conferring regulatory legitimacy on conduct that continues to distort competition. For these reasons, commitments cannot substitute for enforceable, outcome-based Conduct Requirements imposed under the DMCC Act. Apple and Google have had a chance and more than enough time over the past six years to propose commitments that would address the CMA's concerns as to how it uses its dominance in mobile ecosystems to distort competition in digital markets. Both firms' proposed commitments fail to do this.

For these reasons, CMA conduct requirements would better ensure the necessary changes to Apple's and Google's conduct. In drafting such CRs, the CMA ought to apply the following principles:

(a) **Ensure they are substantive not merely procedural**: obligations must address the underlying competitive concern, not merely require Apple or Google to establish and self-assess their unilaterally defined and operated processes.

(b) **Enable independent verification**: compliance monitoring must involve a party with no financial dependence on Apple or Google, with access to their systems sufficient to conduct meaningful audits.

(c) **Monitor effectiveness of remedies**: breach of any CR must trigger a defined obligation: disclosure to the CMA, notification to affected developers, and, where appropriate, reinstatement or remediation.

(d) **Provide developer standing**: developers must have access to an externally administered dispute resolution mechanism, not merely Apple's or Google's internal complaints channels that leave both firms as unilateral decision makers on any outcome.

(e) **Temporal certainty for both these firms and other market participants**: all process obligations must carry hard deadlines; no obligation may be satisfied by an "endeavour" standard where a definite deadline is achievable.

From a UK competition law standpoint, Apple's and Google's proposed commitments represent carefully calibrated opening offers. For example, Apple can claim credit for addressing four legitimate but relatively peripheral concerns: process transparency in App Review and search, mentioning some data safeguards, and offering a request process for interoperability, while leaving completely intact the features of Apple's platform power that the CMA's SMS designation was primarily about:

1) exclusive distribution,
2) commission extraction,
3) browser engine restrictions, and
4) steering prohibitions.

Apple's proposed transparency and reporting obligations are largely self-referential, with Apple certifying its own compliance and preparing its own reports. The interoperability commitment, the most significant in principle, is in practice a promise to listen rather than to act.

For the CMA to accept these commitments as a substitute for formal conduct requirements on the four concerns it has raised, it would need to be satisfied that self-policed process reforms are sufficient to address the concerns that arose precisely because Apple's incentives are to exploit its gatekeeper position. The omitted issue - anti-steering provisions, WebKit restrictions, alternative distribution, and competing payment systems - will require formal CRs, and the adequacy of these commitments should be assessed in that context, not in isolation.

Part 9: Substantive Issues with Google's Commitments (5 February 2026)

Google has offered commitments to the CMA regarding:

1) Google's App Review process;
2) Google's ranking of rival apps in search results;
3) Google's use of third-party data collected through its PlayStore.[71]

As with Apple's commitments discussed in Part 8, the central question is not whether the stated aims (fairness, transparency, predictability) are desirable. They are. The question is whether the commitments are capable of restoring competition given the restrictions imposed by the SMS firm, and given (i) Google's incentives, (ii) the breadth of the CMA's identified competition concerns in its Mobile Platforms work, and (iii) the CMA's documented experience with Google (e.g., Privacy Sandbox) that ill and undefined measures can be difficult to monitor and easily circumvented when they rely on self-assessment.

9.1 Google's Play app review, listing and enforcement commitments remain self-defined and non-binding

Google claims its commitments will ensure Play's app review practices operate "*fairly, objectively, transparently… and on a non-discriminatory basis*," and that app review will be conducted by "*a team separate*" from teams responsible for Google's first-party apps.[72]

[71] Google Commitments (5 February 2026), page 1, paragraph 1.
https://assets.publishing.service.gov.uk/media/69899adb85bc7d6ba0fbc791/google_proposed_commitments.pdf
[72] Google Commitments (5 February 2026), page 2.

Google also proposes (i) an annual UK transparency report with attestations and aggregated metrics, (ii) a formal programme of engagement with UK developers, (iii) communications and "reasonable notice" around policy updates, and (iv) enhanced visibility of appeals and the existing P2B/CEDR alternative dispute resolution channel.

Loophole-GA1: "Fair, objective, transparent, and non-discriminatory" is still self-defined by reference to Google-controlled policies.

The commitment is to implement review practices "*on the basis of [Google's] published policies*." As with Apple's Guidelines in Part 8, the governing rules remain drafted, interpreted, updated, and operationalised by the SMS firm itself.

The annual report is built solely around self-attestations that Google has complied with its own standards, rather than independent verification against objective benchmarks.

Loophole-GA2: Organisational "separation" is not a firewall and is not independently audited.

Google states app review is conducted by a "*team separate from*" first-party teams. But the commitments (as drafted) do not establish a legally enforceable firewall (separate reporting lines, information barriers, incentive restrictions, and audit rights) comparable to remedies typically required where conflicts of interest are intrinsic to a vertically integrated dominant player who operates a choke-point strategic market service.

Loophole-GA3: Appeals are internal-first; the "independent" route is non-binding and can be refused.

Google maintains a "*robust internal appeals mechanism*," and then offers access to a P2B/CEDR mediation framework. However:

- Google states if a dispute proceeds to mediation, this body's outcomes are "not binding" on either party; and
- Google reserves discretion to refuse mediation, including on the basis the developer is "clearly not in compliance," or that the request is out of scope.

This leaves developers without a binding merits appeal to an independent adjudicator, precisely the deficiency Part 8 identifies as fatal in self-policed systems.

Loophole-GA4: "Reasonable notice" and "grace periods" are undefined, with no hard transition minima.

Google proposes "*reasonable notice*" for material policy updates and "*reasonable grace periods*," and notes developers may be able to request additional time for certain complex policies. Without minimum notice periods, minimum transition windows, and enforceable constraints on emergency exceptions, the commitments permit "policy drift" and rapid rule changes that developers must absorb under asymmetry of information that the CMA has identified as a competitive concern.

Loophole-GA5: Reporting is aggregated, unreasonably geographically restricted, and delayed, limiting ability to detect discrimination.

Google's annual UK transparency reporting is aggregated and anonymised, with reporting "*within three months following each… reporting period*." Google also specifies the first reporting cadence and delivery dates (e.g., first bi-annual metrics report by 30 September 2026 covering 1 April 2026 – 30 June 2026, and first annual report by 31 March 2027 covering 1 April 2026 – 31 December 2026).

The UK-only framing risks excluding many developers materially affected in the UK storefront but not "UK-based" (a concern similarly raised in Part 8 for Apple's unreasonable UK-developer restrictions).

Loophole-GA6: No enforceable performance commitments on review speed or error correction.

Google describes publicly that some reviews may take "*up to seven days or longer in exceptional cases*," while noting average review times are "*less than one day*." But there is no enforceable service-level requirement, nor any obligation to provide developer-specific comparative outcomes (needed to detect discriminatory treatment in practice).

9.2 Google's Play ranking / discovery commitments are process-forward and leave core discrimination vectors unaddressed

Google commits to rank apps "*fairly, objectively, transparently, and on a non-discriminatory basis*," and describes Play's ranking as based on three criteria: (1) user relevance, (2) app quality, and (3) user experience.

Google also states that ranking is algorithmic/rules-based, applies non-discriminatorily to first- and alternative third-party apps, and operates independently from teams responsible for Google's own apps. Google also proposes annual UK transparency reporting, developer engagement, developer resources, and enhanced visibility of complaints routes.

Loophole-GR1: "Quality" / "user experience" are undefined and can function as proxy discrimination.

As set out in this submission's earlier analysis (Part 4), discrimination can be implemented not only through explicit first-party preference but through ranking signals correlated with adoption of the platform's adjacent B2B services (payments, ads, analytics, attribution). Google's high-level criteria (relevance/quality/UX) are not objectively defined, and do not, as currently drafted, prohibit proxy signals that systematically advantage apps using Google's own B2B stack.

Loophole-GR2: No independent algorithm audit; no duty to disclose factor weightings or test outputs.

Google asserts ranking is rules-based and algorithmic, but its proposal, like Apple's in Part 8, relies on transparency reports and engagement rather than independent, technical verification of outcomes (e.g., audit access, query testing, statistical tests for self-preferencing).

Loophole-GR3: No explicit separation between paid promotion and organic ranking (and no parity duty).

The commitments text available here describes organic ranking criteria and process but does not, on its face, impose an enforceable obligation to separate paid promotion and other monetisation-linked signals from organic ranking outcomes, nor to provide parity of discovery conditions for apps that do not adopt Google monetisation or other B2B services.

9.3 Google's "use of data" safeguards remain internal-only, narrowly scoped, and hard to verify

Google's commitments package is explicitly within the scope of "*app review, app ranking and use of data*." However, per the earlier evaluation of Apple's insufficient commitments, Google's proposal suffers from the same imitations: internal controls, no independent data auditor, no self-reporting obligation upon breach discovery, and annual self-prepared attestation with monitoring that the CMA cannot independently verify (e.g., access logs).

Loophole-DU1: Internal controls without independent audit rights are not monitorable.

Where compliance is "*difficult to determine, observe or monitor*," and where measures can be "*easily circumvented*," self-policing frameworks are weak, particularly in vertically integrated gatekeepers with strong incentives to extract competitive intelligence.

Loophole-DU2: No breach self-reporting and no remediation process.

As identified earlier in this submission, the absence of mandatory breach notification (to the CMA and affected developers) and the absence of a remediation protocol materially reduces any deterrent effect from Google's proposed commitments.

Loophole-DU3: Scope ambiguity risk ("non-public Play data").

Where "non-public" data is not defined to include derived market intelligence and behavioural insights produced by platform operation, safeguards can be circumvented by using processed/derived datasets and model outputs rather than raw developer inputs—an issue MOW flags for both firms' approaches to data protections.

9.4 Interoperability and open standards access: Google offers no equivalent commitments (a substantive omission)

The CMA's February 2026 call for evidence describes Google's proposed commitments as "*in respect of app review, app ranking and use of data*," while stating that Apple's proposed commitments "*also enable developers to request interoperable access to key functionalities within Apple's mobile operating systems*." This underscores a material asymmetry in Google's proposal. Google does not provide even an interoperability "request" route nor substantive interoperability obligations comparable to those required for Apple.

This omission matters because the CMA's Mobile Platforms work and SMS designation concerns extend beyond the app store process to include interoperability and competition in the broader mobile platform stack (including browser competition and default-driven distribution power).

9.5 Cross-cutting omissions relative to the CMA's SMS concerns: the commitments do not address core monetisation and distribution constraints

Even within this submission's own comparison table, the most competition-significant sources of platform power—commissions/billing requirements, anti-steering constraints, alternative distribution constraints, and browser/default leverage—are identified as unremedied by Google's commitments (either silent or materially incomplete depending on the area).

In particular, the submission has already flagged that:

- Commitments framed around "fair and objective" processes risk remaining self-evaluated and non-audited.
- Payment and revenue-extraction mechanisms, anti-steering, and other leveraging pathways are not remedied by process transparency alone.

9.6 Monitoring remains input-based and retrospective; the CMA needs independent, continuous, output-based oversight

Google's commitments lean heavily on transparency reports, attestations, engagement programmes, and complaint/appeal channel visibility. As MOW explains in Part 7, these are **inputs** not **outcomes**:

they do not detect systematic discrimination where developers adapt rather than complain, and they do not deter circumvention absent continuous, independent monitoring of platform outputs.

Proposed Conduct Requirements for Google

The following CRs are drafted to convert Google's process statements into enforceable obligations with measurable outputs, independent verification, and binding dispute resolution.

A. App Review / Play Store Listing

Proposed Conduct Requirement App Review (CR GR-1): Policy change governance
Google must not amend, introduce, or remove any provision in Play's Developer Program Policy (DPP), Developer Distribution Agreement ("**DDA**"), or any review-enforcement guidance in a manner that materially affects developers without: (i) at least 30 days' advance notice (60 days for material monetisation/permissions changes); (ii) publication of objective justification; and (iii) submission of the change rationale and impact assessment to an Independent Monitor for review.

Proposed Conduct Requirement App Review (CR GR-2): firewall
Google must implement and maintain a firewall between app review/enforcement functions and teams responsible for developing, marketing, monetising, or measuring performance of Google first-party apps and services, with audit rights for an Independent Monitor.

Proposed Conduct Requirement App Review (CR GR-3): Binding external appeal
Google must provide developers with access to a binding external appeal mechanism for final enforcement decisions. The existing P2B/CEDR mediation process may remain available but shall not substitute for binding adjudication, given that mediation outcomes are not binding and may be refused.

Proposed Conduct Requirement App Review (CR GR-4): Minimum transition periods
Google's "reasonable notice" and "grace periods" must be converted into minimum, enforceable transition periods (30/60-day minima depending on impact), with emergency exceptions narrowly defined and subject to retrospective independent review.

Proposed Conduct Requirement App Review (CR GR-5): Disaggregated reporting
In addition to aggregated UK reporting, Google must provide the CMA and Independent Monitor with disaggregated metrics (by category, enforcement reason, competitor adjacency, and comparable treatment of Google first-party apps) sufficient to detect discrimination, with quarterly cadence and developer-standing analytics access.

B. Ranking / Discovery

Proposed Conduct Requirement Ranking (CR RK-1): Objective definitions and proxy discrimination ban
Google must define "user relevance," "app quality," and "user experience" in objectively testable terms, and must expressly prohibit direct or proxy ranking signals that systematically advantage apps based on adoption of Google's B2B services (payments, ads, attribution, analytics), consistent with the discrimination theory already set out in this submission.

Proposed Conduct Requirement Ranking (CR RK-2): Independent algorithm audit
Google must engage a CMA-approved independent auditor to conduct periodic audits of Play ranking outputs (including query testing and statistical analysis for preferencing), with confidential access as necessary, and publish non-confidential summaries.

Proposed Conduct Requirement Ranking (CR RK-3): Paid/organic separation
Google must ensure that paid promotion, ad spend, and monetisation-linked signals do not influence organic ranking, directly or indirectly, and must maintain auditable separation of feature pipelines used for ads/promotion versus organic discovery.

Proposed Conduct Requirement Ranking (CR RK-4): Pre-implementation notification
Google must notify the CMA and Independent Monitor in advance of any material change to ranking inputs, weighting, presentation, or policies that could affect discovery outcomes, with a minimum notice period and a CMA right for review.

C. Use of Data

Proposed Conduct Requirement Data Use (CR DU-G1): "Non-public Play data" Scope must include derived intelligence
The prohibition must apply to all non-public developer and market data obtained through Play operations, including derived insights, behavioural engagement intelligence, and model training data used for competitive decisions.

Proposed Conduct Requirement Data Use (CR DU-G2): Independent Data Auditor + access logs
Google must appoint a CMA-approved Independent Data Auditor with ongoing read access to relevant access logs and authority to report suspected breaches to the CMA (and notify affected developers) within defined deadlines.

Proposed Conduct Requirement Data Use (CR DU-G3): Self-reporting and remediation protocol
Google must self-report any discovered breach to the CMA within a fixed time period and provide remediation steps (developer notification, corrective action, and audit findings).

D. Interoperability and open standards are omitted from Google's proposal

Proposed Conduct Requirement Interoperability (CR I-G1): Interoperability request channel + published criteria
Google must implement a formal interoperability request channel for Android/GMS-dependent functionalities where Google's platform terms and integrations constrain rivals, with published criteria, enforceable timelines, and independent appeal. This is necessary to avoid asymmetric treatment where only Apple provides an interoperability request process.

E. Monitoring and Enforcement

Proposed Conduct Requirement Monitoring (CR MON-G1): Independent technical monitor and continuous output metrics
The CMA must appoint an Independent Technical Monitor empowered to audit outputs (review outcomes, ranking distributions, and data access controls) on a continuous basis, rather than relying on retrospective attestations and non-binding mediation

Part 10: Legal Consistency with UK and EU Competition Law

We appreciate that the DMCCA is different from competition law as it exists in the Competition Act 1998 ("**CA 1998**") and EU competition law but also would observe that the CMA's duties mean the CMA cannot use one to contradict outcomes in the other. Any remedies implemented by the CMA under the DMCCA will be taken into account by the courts under CA98 too, so the impact on private recovery needs to be considered by the CMA.

The DMCCA operates alongside, and does not replace, the CA98 and Article 102 TFEU as retained in UK law. The CMA's proposed commitments must not, by normalising Apple's and Google's restrictions, inadvertently create inconsistencies with established competition law principles that continue to apply in parallel.

- **Apple IAP and anti-steering:** The EC has found Apple non-compliant under the DMA in relation to anti-steering rules preventing developers from directing users to alternative purchase methods. The US District Court in *Epic v. Apple* (April 2025) required Apple to permit external purchase links in the US. The CMA's framework must deliver equivalent UK outcomes without requiring UK developers to litigate each restriction separately.
- **Apple NFC and digital wallets:** The EC reached a commitments decision with Apple on NFC access in 2024 following a finding that Apple's restriction constituted an abuse of dominance. The CMA's roadmap identified NFC access as a priority intervention. The proposed commitments do not deliver it. Formal Conduct Requirements are required on the timeline indicated in the roadmap.
- **Google AdTech:** The US DOJ AdTech case (verdict April 2025) found Google liable under Section 2 of the Sherman Act in relation to its ad server and ad exchange conduct. Remedies are ongoing. The CMA's monitoring of Google's mobile platform must cover the interaction between Android platform control, GMS terms, and Google's advertising services to ensure that US and EU adtech remedies are not circumvented through platform-level Android controls.
- **Revenue-sharing agreement remedies:** The US DOJ Search remedies proceedings are addressing the legality of Google's revenue-sharing agreement with Apple as a mechanism for foreclosing rival search engines from default status. Any remedy the CMA imposes on the Apple-Google ISA must be consistent with — and should be coordinated with — the US remedies outcome. MOW recommends that the total payments from any search engine to any browser be capped as a percentage of revenue to match what browser vendors receive from rival search providers, preventing Google from circumventing a cap on Apple-only payments by distributing equivalent payments across multiple browser vendors.

Conclusion and Summary of Necessary Action

MOW supports the CMA's decision to act swiftly following Apple's and Google's SMS designations. The two firms' proposed commitments highlight that instead of being a welcome step forward, they merely serve as a delaying tactic to effective remedies to competition in mobile platform markets. The proposed commitments only mention a subset of the documented harms and contain definitional vulnerabilities that both firms are highly likely to exploit to avoid providing true remedies to their ongoing abusive conduct.

MOW urges the CMA to supplement the commitments with formal Conduct Requirements in the following areas:

1. **App Review / PlayStore Listing and Discovery**: All app listing criteria and discovery mechanisms must be objectively justified, proportionate, and applied symmetrically to first-party and alternative apps. Prohibit platform discrimination through undefined concepts such as "quality" or "relevance"; prevent paid advertising, monetisation choices, or adoption of platform B2B services from influencing organic discovery. Moreover, independent

oversight, binding external appeals, advance notice of material changes, and output-based monitoring of review and ranking outcomes must be mandated.

2. **B2B service coercion:** Prohibit Apple and Google from mandating use of the B2B adjacent services or their own app stores as a condition of app distribution. Require equivalent access for alternative payment processors, alternative measurement providers, and alternative advertising networks on technically and commercially equivalent terms.
3. **Fair ranking and B2B service neutrality:** Extend non-discrimination obligations to cover any ranking signal systematically correlated with platform B2B service adoption, with Apple and Google bearing the justification burden. Apply this obligation to editorial and curated placements as well as algorithmic ranking.
4. **Browser engine interoperability and real-time communication open web standards support:** Require Apple to permit alternative browser engines on iOS/iPadOS, subject only to security requirements assessed by an independent technical expert. Platforms must have mandated timely, non-discriminatory implementation of real-time communication open web standards and must be prevented from implementing technical or policy restrictions that degrade web-based communications relative to native services. Moreover, platforms must be prohibited from relying on undefined privacy or security justifications without independent assessment, and ensure interoperability obligations are enforceable, monitored, and subject to independent oversight.
5. **Objective "privacy" and "security" definitions:** Incorporate objective definitions of privacy risk, Personal Data, deidentified data, and choice architecture standards into the CR. Require that any privacy or security justification offered by Apple or Google for a restriction on rivals be assessed against these definitions by an independent technical expert, with Apple and Google bearing the evidential burden.
6. **NFC and real-time communications:** Require Apple to provide equivalent NFC access to competing payment apps and to publish FRAND interoperability specifications for APNs or permit competing real-time communications infrastructure on equivalent terms.
7. **Broader generative AI distribution and choice**: AI-driven assistants and generative AI features must not entrench platform self-preferencing. Conduct requirements should require parity of access and outcomes for alternative AI services competing with platforms' assistants; prohibit default routing or integration advantages that foreclose rivals; ensure user-controlled choice of AI services; and subject AI distribution, intent routing, and default settings to independent oversight and monitoring
8. **Standards body conduct:** Require Apple and Google to publish a competition impact assessment for any proposal they submit to a technical standards body that would restrict rivals' access to functionality, reviewed by the CMA before implementation.
9. **Independent technical monitor:** Appoint an independent technical monitor with algorithmic audit powers, access to interoperability decision records, and authority to review privacy justifications and choice architecture.
10. **Continuous output monitoring:** Require daily or weekly CMA access to aggregate output data on app ranking distributions by B2B service adoption category; monthly interoperability request outcome data; quarterly attribution signal parity reporting; and an anonymous developer reporting channel.
11. **Pre-implementation notification:** Require 60 days advance notice to the CMA of material changes to payment policies, attribution APIs, advertising identifier frameworks,

interoperability criteria, or consumer-facing choice architecture, with a CMA right to pause implementation pending review.

12. **Revenue-sharing cap:** Cap total payments from any single search engine to any browser vendor as a percentage of revenue aligned with what browser vendors receive from rival search providers, consistent with the US DOJ Search remedies.

MOW reserves its position on the proportionality assessment of specific measures pending the CMA's response to this consultation. All rights are reserved. MOW welcomes the opportunity to meet with the CMA to discuss the specific drafting requirements set out in this submission.