

European Commission
Directorate-General for Competition
1049
Bruxelles/Brussel
Belgique/Belgie

Via designated online submission portal only

Our Ref: TC/ADM838
15th September 2023

Dear Sirs,

RE: Consultation on the template relating to the reporting on consumer profiling techniques

We write on behalf of Movement for an Open Web (“MOW”), a not-for-profit organization that is seeking to secure an open and decentralized web, in response to the Commission’s consultation request on its template for the description of consumer profiling techniques.¹ It is our view that an annual audit goes a long way to increasing transparency around data processing and encouraging a code of compliance amongst gatekeeper platforms.

As part of this process, we agree with the Commission's separation of business processing inputs from the outputs of the processing. We further agree with the distinctions noted between personal data actively declared by specific individuals, and business data observed or derived from network activity and online interaction with publisher content that is not linked to the identity of specific individuals.

To further strengthen the existing template, we would ask the Commission to ensure compliance reporting includes conduct by Internet Gatekeepers that restricts rival business-facing solution providers from using the same non-identity data that their own business-facing solutions use as inputs. For example, Apple’s privacy policy and choice architecture does not apply the same consumer settings to its own apps as it imposes on rival businesses (e.g., ATT prompt). This practice has been criticized by the CMA’s mobile ecosystem report and is being actively investigated by the Autorite de la Concurrence.

Contrary to privacy washing narratives, most modern, digital business processing relies on non-human readable scores and statistical coefficients to inform the automated matching of digital content to internet-connected devices. Taking Search automated results sets or Google’s automated answer engine, Bard, for instance; neither rely on any profiles to inform the digital content returned in response to a consumer-initiated request. The same is true for Google’s Maps and Shopping websites.

Display digital advertising, as the funding model for most ad-supported digital content, is distinguished from these as being initiated by a business stakeholder, rather than a consumer. To ensure that internet gatekeepers do not hide their anticompetitive conduct behind a false veneer of protecting “privacy”, we urge the Commission to ensure its reporting obligations capture in greater detail what data linked to

¹ See Consultation details at: https://digital-markets-act.ec.europa.eu/consultations/consultation-template-relating-reporting-consumer-profiling-techniques_en

individuals is used by Internet Gatekeepers and what conduct they restrict from safer rivals who rely on only deidentified match keys to support the high-quality, continuous, real-time unaggregated data interoperability required within digital markets.

This insertion is based on our understanding of platform strategy, which aims to restrict rivals' access to necessary input data required to compete against the platform's own business-facing solutions under the illusory guise of "improving privacy". Technically speaking, consumers have the option to choose Google's browser; they have far less choice over selecting which Operating System will run on their internet-connected devices. We believe Google's unilateral policies and proposed restrictions on rivals' ability to access open standards to support interoperable exchanges of business information, would violate their obligations under Articles 5 and 6 of the DMA. Google's ability to use its dominant position as an internet gatekeeper to steer business choices is further exacerbated by its use of dark patterns to steer user choices, facilitating its capture of all user data from all of its products.

As an internet gatekeeper, Google also uses dark patterns within its consumer-facing browser and OS software, to coerce consumers into disclosing their identity, at sign-in, for instance. If consumers wish to restrict Google's data collection and processing of their identity, they are required to go through a five-stage process of "manual personalisation". There is no standalone option by which users can declare a preference to restrict all personalisation, the default setting being "express personalisation" which allows Google to use specific individual's identity as a common match key with advertisers (e.g., Customer Match). This setting is then used to exempt any consumer decision that applies to rivals' use of data from impacting its own use, especially for such business-facing solutions (e.g., its Ad Systems).

Google thus encourages users to consent to extensive data processing by adding friction to alternatives but also through suggestive phrasing. Describing the default personalisation settings as "Express personalisation", rather than "high-level personalisation", for instance, simply confers that it is quick and easy. It is not immediately apparent that the user is giving Google extensive, fine-grained information on their online activity. Thus, by depriving consumers of a default option by which they can reject Google's use of targeted advertising whilst mislabelling the choice which allows Google to track and commercialise user identity-linked data, Google cleverly establishes a choice architecture which encourages users to check the first box and continue. This practice is common to several other gatekeeper platforms with large consumer interfaces.

To address the above competition concerns, we would ask the Commission to require reporting on how many users are presented choices with identical language to the choices for alternative business-facing solutions provided by the Internet Gatekeeper (e.g., Apple's SKAN attribution service or Google's attribution APIs within its Privacy Sandbox initiative, which without modification is likely distort competition within digital markets according to the UK CMA). Further, we note that the Commission requires that gatekeepers include statistics on how many consumers choose to undergo profiling if they are given a choice. This is an important provision, which will help regulators and researchers better understand and tackle the so-called 'privacy paradox', wherein consumers tend to give more data than they are comfortable with or would accept after due consideration. However, for this information to be useful to the Commission, we would suggest it be benchmarked against a poll of user preferences, which the Commission could require the gatekeeper to include in its annual audit.²

Please do be in touch with any questions regarding the above. We would also be very happy to arrange a call to address the points we have raised further.

² The UK's OFCOM survey associated with individual's perception of how organizations collect personal information online found that consumers were happy with companies use of identity-linked personal data (73% in 2021 and 72% in 2022 said they were "totally happy", whereas 21% in 2021 and 20% in 2022 were "unhappy"). See <https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes/interactive-tool-2021> and <https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes/interactive-tool>

Yours faithfully,

A handwritten signature in blue ink, appearing to read "Preiskel & Co", with a stylized flourish at the end.

Preiskel & Co LLP