# Playing fair in the Privacy Sandbox: competition, privacy, and interoperability standards

**Mark Nottingham**[*]

Abstract

Google's Privacy Sandbox proposals to change the Chrome browser in ways that are likely to further advantage them over other publishers and advertising platforms has attracted the attention of competition regulators, the online advertising industry, and critics of their platform power. At the same time, the Privacy Sandbox appears to answer a call from data protection regulators, privacy advocates and users for 'privacy by design,' moving in lockstep with its industry peers. How, then, should this behaviour be evaluated for abuse? I argue that there are several hurdles to considering the most controversial Privacy Sandbox proposal – blocking third-party cookies – as an abuse of market power. Furthermore, I propose that, because web browsers are an architecturally regulated market, competition regulators should distinguish unilateral behaviour by examining it in the context of other browsers' behaviours, along with signals regarding consensus from the relevant standards bodies.

## I Introduction

The UK Competition and Markets Authority (CMA) recently announced an investigation into Google's Privacy Sandbox proposals[1] because of their potential to 'undermine the ability of publishers to generate revenue and undermine competition in digital advertising, entrenching Google's market power.'[2] Geradin, Katsifis, and Karanikioti support this view, concluding that 'Chrome's policy change raises… antitrust concerns, in that it may distort

[*] Mark Nottingham is a student at Melbourne Law School, Chair of the IETF HTTP Working Group, and recently a member of the Internet Architecture Board. Previously, he was a member of the W3C Technical Architecture Group.

[1] 'The Privacy Sandbox', *The Chromium Projects* (Web Page) <https://www.chromium.org/Home/chromium-privacy/privacy-sandbox>.

[2] 'CMA to Investigate Google's "Privacy Sandbox" Browser Changes', *gov.uk* (Web Page) <https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes>.

competition among publishers and ad tech vendors, benefiting Google and leading to increased market concentration.'[3]

Unilateral changes in Chrome (the most popular web browser)[4] can indeed have *prima facie* anti-competitive effects when examined in isolation. However, we can also view these proposed changes as part of the legitimate architectural regulation of privacy on the web through the Standards Developing Organisations (SDOs) that specify browser's behaviours.

I contend that there are significant hurdles to considering the most controversial Privacy Sandbox measure – blocking third-party cookies – as anti-competitive when considered in this light. However, other changes in Chrome – even if made with the purpose of improving privacy – could still be unilateral and thus considered as anti-competitive. To distinguish them, I argue that competition regulators can (and should) use signals from SDOs and other browsers as a primary aid.

Part II of this paper contextualises the Privacy Sandbox proposal within the architectural regulation of privacy. Part III then examines the relevant aspects of the web browser market, since this is the means by which Google is said to be exerting. Part IV evaluates the Privacy Sandbox as a potential abuse of market dominance within that context, using the Commission's guidelines for enforcement priority regarding refusal to supply as a template. Part V then explores how a competition authority could distinguish unilateral activity by browser vendors in web related SDOs, and Part VI offers conclusions.

## II Architectural regulation of privacy

While the GDPR and ePrivacy Directive are the current basis of legal regulation of privacy in Europe, but they do not operate in a vacuum. Regulation also occurs through architecture – that is, constraints that are automatic once enabled, whether designed or absolute.[5] Most architectural constraints on the web are found in the behaviour and capabilities of websites and web browsers, and are often coordinated through technical standardisation.

[3] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'Google as a de Facto Privacy Regulator: Analyzing Chrome's Removal of Third-Party Cookies from an Antitrust Perspective' [2020] (November) *SSRN* <https://ssrn.com/abstract=3738107>.

[4] See below pt III(C).

[5] Lawrence Lessig, *Code* (Basic Books, 2006) 342.

There has been long-standing interest in and activity around architectural regulation of privacy on the web. The first formal technical specification for cookies (a web technology that can be used to track user activity) explicitly cautioned against 'unexpected cookie sharing' by user agents (the technical term for browsers):

> A user agent should make every attempt to prevent the sharing of session information between hosts that are in different domains. Embedded or inlined objects may cause particularly severe privacy problems if they can be used to share cookies between disparate hosts… User agent implementors are strongly encouraged to prevent this sort of exchange whenever possible.[6]

Browser vendors did not heed this advice, and so the 2000s saw sizeable increases in the use of cookie-based online tracking and profiling.[7] This increase was assisted by the development of other tracking methods; for example, browser fingerprinting has received broad attention since 2010.[8]

Responses that use architecture as a modality of regulation have varied. P3P[9] was an initial attempt to layer in a consent mechanism for tracking, followed later by DNT.[10] Both failed to achieve meaningful success, at least in part because they did not gain support from other regulatory modalities (namely, norms and/or law), and because they were resisted by the online advertising industry.

Third-party browser add-ons for blocking online tracking are another – albeit more fragmented – architectural response that have gained broad adoption.[11] Recently, browsers have taken proactive steps to implement these functions

[6] D. Kristol and L. Montulli, *HTTP State Management Mechanism* (IETF Historic RFC, February 1997), s 6.3 <https://tools.ietf.org/html/rfc2109>.

[7] See, eg, Balachander Krishnamurthy and Craig E Wills, 'Generating a Privacy Footprint on the Internet' [2006] *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement* 65 <http://portal.acm.org/citation.cfm?doid=1177080.1177088>.

[8] Peter Eckersley, 'How Unique Is Your Browser?' [2010] *International Symposium on Privacy Enhancing Technologies Symposium* 1.

[9] Ari Schwartz, 'Looking Back at P3P: Lessons for the Future', *Center for Democracy & Technology* (2009) <https://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf>.

[10] Glenn Fleishman, 'How the tragic death of Do Not Track ruined the web for everyone', *FastCompany (17 March 2019) < https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone>.*

[11] See, eg, Arunesh Mathur et al, 'Characterizing the Use of Browser-Based Blocking Extensions to Prevent Online Tracking' [2019] *Proceedings of the 14th Symposium on Usable Privacy and Security, SOUPS 2018* 103 <https://www.usenix.org/system/files/conference/soups2018/soups2018-mathur.pdf>.

natively, through limitations placed upon cookies and changes designed to frustrate fingerprinting.[12]

This is not unusual; browsers often migrate functions from extensions into the core when they become popular. For example, password managers, language translation and 'reader mode' were all features that were first browser extensions before they were implemented natively. These changes in browser behaviour are sometimes labelled as 'unilateral,'[13] but the consensus specification defining the operation of cookies explicitly gives browsers 'wide latitude to experiment with third-party cookie policies that balance the privacy and compatibility needs of their users.'[14] As such, it may be more accurate to view these changes as a correction of previously lax behaviour.

Such architectural regulation of privacy – sometimes knows as 'privacy by design' – has largely been seen as beneficial and complementary to legal regulation.[15] For example, the Data Protection Working Party opines that '[b]rowsers… which by default reject 3rd party cookies… may be able to deliver valid and effective consent.'[16] A subsequent statement by the Working Party is worth quoting in full, because it implies that architectural regulation can be more effective than legal regulation:

> Given the importance that browser settings play in ensuring that data subjects effectively give their consent to the storage of cookies and the processing of their information, it seems of paramount importance for browsers to be provided with default privacy-protective settings.[17]

As such, without robust architectural regulation, there would likely be a net loss in privacy. The CMA notes it is important 'to address legitimate privacy

[12] See, eg, John Wilander, 'Intelligent Tracking Prevention 2.3', *WebKit* (2019) <https://webkit.org/blog/9521/intelligent-tracking-prevention-2-3/>; 'Enhanced Tracking Protection in Firefox for Desktop', *Mozilla Support* <https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>.

[13] *Online Platforms and Digital Advertising Final Report, Appendix G: The Role of Tracking in Digital Advertising* (2020) 119.

[14] Adam Barth, *HTTP State Management Mechanism* (IETF Proposed Standard, April 2011), s 7.1 <https://httpwg.org/specs/rfc6265.html>.

[15] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 199/1, Article 25.

[16] *Opinion 2/2010 on Online Behavioural Advertising* (Advisory Opinion) (Article 29 Data Protection Working Party, WP171, 22 June 2010) 14.

[17] Ibid 15.

concerns without distorting competition.'[18] The converse proposition – that it is important to address legitimate competition concerns without distorting privacy – may not be achieved if browsers are prevented from fulfilling their architectural regulatory role.

### A *The Privacy Sandbox as architectural regulation*

Within this context, we can view the Privacy Sandbox as a set of proposals (currently twenty-four) from Google for the architectural regulation of privacy on the web platform.

Some of these proposals are newly and exclusively made by Google. For example, the Privacy Budget[19] is a proposal by a Google employee to limit the information made available for fingerprinting; it has no formal standing in any standards process.

Other Privacy Sandbox proposals are co-opted from existing efforts that are in the process of standardisation, or that are already considered standard (either *de facto* or *de jure*). For example, the Privacy Sandbox proposal listed as 'SNI' refers to the Encrypted Client Hello specification,[20] an effort to prevent observation of the sites that a user is visiting, effectively 'plugging a hole' in the security of the web. This specification has already been adopted by the IETF TLS Working Group as a work item that enjoys broad industry participation and implementation.[21]

Likewise, 'Partitioning HTTP cache' refers to ongoing efforts in both the IETF HTTP Working Group caching specification[22] and in the WHATWG's Fetch specification[23] to prevent web caches (which are used to improve performance by storing copies of often-used responses locally) from being used

[18] 'CMA to Investigate Google's "Privacy Sandbox" Browser Changes' (n 2).

[19] Brad Lassey, 'Combatting Fingerprinting with a Privacy Budget' (Web Page) <https://github.com/bslassey/privacy-budget>.

[20] Eric Rescorla et al, *TLS Encrypted Client Hello* (IETF Internet-Draft, 16 December 2020) <https://tlswg.org/draft-ietf-tls-esni/draft-ietf-tls-esni.html>.

[21] See, eg, 'Encrypted Client Hello: the future of ESNI in Firefox', *Mozilla Security Blog* (Blog Entry, 7 January 2021) <https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/>.

[22] Roy Fielding, Mark Nottingham and Julian Reschke, *HTTP Caching* (IETF Internet-Draft, 29 January 2021), s 7.2 <https://httpwg.org/http-core/draft-ietf-httpbis-cache-latest.html>.

[23] Anne van Kesteren, 'Fetch Standard' (Living Standard, WHATWG), s 2.7 <https://fetch.spec.whatwg.org/>.

to track user activity – again, enjoying active participation and implementation from other browser vendors, as well as other parties.[24]

The Privacy Sandbox also co-exists with competing proposals. Take, for example, the User-Agent HTTP header, which traditionally identifies the 'make and model' of the browser to the web server, but also can be used to help fingerprint the user, and thereby track them. Whereas Google's stated preference is to require the server to ask for it using the Client Hints mechanism,[25] Mozilla believes that privacy is better served by stopping changes to the header's value, effectively freezing it and thereby removing its utility as a vector for fingerprinting. However, this is a disagreement about the route, not the goal: Mozilla labels Chrome's preferred approach as 'non-harmful.'[26]

As is often the case for web standards, it may be some years before the fate of all the Privacy Sandbox proposals becomes clear. When that occurs, the outcomes might vary in two relevant ways. The first is the disposition of a given proposal's *specification* – whether it explicitly gains consensus in a relevant SDO, or remains a private document, or is not formally documented at all. The second is the proposal's *implementation*: whether it is present in Chrome, Chrome and some other browsers, or Chrome and all other browsers.

These factors can be used as indicators of unliteral action by Google or any other browser vendor. Thus, some Privacy Sandbox proposals might represent unilateral action by Google in the browser market, with a non-consensus specification and no other implementation. Alternatively, they might gain SDO consensus and see broad implementation. These are the two most common outcomes, but others are possible; for example, some commonly implemented features are not yet well-specified, and some consensus specifications only see limited implementation.[27]

[24] See, eg, 'Firefox 85 Cracks Down on Supercookies', *Mozilla Security Blog* (Blog Entry, 26 January 2021) <https://blog.mozilla.org/security/2021/01/26/supercookie-protections/>.

[25] Mike Taylor and Yoav Weiss, *User-Agent Client Hints*, (W3C Draft Community Group Report, 29 January 2021) <https://wicg.github.io/ua-client-hints/>.

[26] 'User Agent Client Hints', *Mozilla Standards Positions* (Web Page) <https://github.com/mozilla/standards-positions/issues/202>.

[27] See, eg, Lorrie Cranor et al, *The Platform for Privacy Preferences 1.0 (P3P1.0)* (W3C Recommendation, 2002) <https://www.w3.org/TR/P3P/>.

# III The browser markets

The mechanism that Google is alleged to be using for leverage – the Chrome web browser – also bears examination. The CMA report pegs its market share at 50% in the UK as of October 2019, [28]and Geradin, Katsifis, and Karanikioti characterise it as having a 'dominant position in the market for browsers'[29] because it had a 66% worldwide market share according to StatCounter.[30]

However, these industry-sourced estimates of market share do not define the multiple markets that browsers take part in for the purposes of competition law, and do not consider their unique features. This is critical, as '[a] pure market share focus risks failing to take proper account of the degree to which competitors can constrain the behaviour of the allegedly dominant company.'[31]

## A *Browsers and browser engines*

We can view Chrome as being involved in two distinct browser-related markets. First, browsers compete against each other in a *web browser market* to attract users, thereby gaining market share. This is the market in which Google is said to be exercising power, because it has sole control of Chrome.

Second, Chrome is based upon Blink,[32] which competes in the *browser engine market*. Because of browsers' inherent complexity, few parties have the resources to write the millions of lines of code to create one. Instead, they can more easily create one by starting with a browser engine, of which there are currently three: Google's Blink (also the basis of Microsoft Edge, Brave, Yandex browser, QQ browser, and others), Mozilla's Gecko (the basis of Firefox), and Apple's Webkit (the basis of Safari, Blackberry Browser, Playstation browser, Kindle browser, and others). All three are Open Source: Gecko because of its origins in a non-profit foundation, Blink because it was

[28] *Online Platforms and Digital Advertising* (2020) 62 <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.

[29] Geradin, Katsifis and Karanikioti (n 3) 33.

[30] Ibid 62.

[31] Neelie Kroes, 'Preliminary Thoughts on Policy Review of Article 82' (Speech, Fordham Corporate Law Institute, 23 September 2005) 3 <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_05_537/SPEECH_05_537_EN.pdf>.

[32] 'Blink (Rendering Engine)', *The Chromium Projects* (Web Page) <https://www.chromium.org/blink>.

forked from WebKit (and thus needed to conform to its license), and likewise WebKit because it was forked from the Open Source KHTML project.[33]

As such, browser engines can be considered a vertical market, supplying browsers.

### B *Market governance: the web platform*

The web is a two-sided market that brings together end users (who want to access web content) and content providers, including advertisers (who want to make their content available to end users), with both direct and indirect positive network effects on both sides. In industry, this is known as the *web platform*.[34]

The web platform is architecturally governed by horizontal agreements between browser and browser engine vendors. While these agreements can occasionally be characterised as concerted practices, they are often more formally documented in technical specifications. These specifications ensure interoperability between browsers and websites, and also seek to ensure the longer-term viability of the web as a platform, incorporating goals such as security, privacy and accessibility.[35] Many of these specifications are developed by consensus in one of the SDOs that is relevant to the web, including the World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), and CA/Browser Forum (CAB Forum).

Google's freedom of action within these fora has been widely discussed. For example, the CMA notes that 'Google has an outsized impact on the standards for how technology develops.'[36] However, while browser vendors – and particularly Google – take part in these fora and make significant contributions, they do not completely control them, either individually or collectively. Each venue has its own process for making decisions (typically, some form of consensus), its own rules for participation and contribution, and its own principles that constrain the resulting design.

[33] Dirk Mueller, 'Greetings from the Safari team at Apple computer' (Email, 7 January 2003) <https://marc.info/?m=104197092318639>

[34] See, eg, 'webplatform.org' (Web Page) <https://webplatform.org/>.

[35] See, eg, Daniel Appelquist and Hadley Beeman, *Ethical Web Principles* (W3C Draft TAG Finding, 6 October 2020) <https://w3ctag.github.io/ethical-web-principles/>.

[36] *Online Platforms and Digital Advertising Final Report, Appendix G: The Role of Tracking in Digital Advertising* (n 13) 105.

For example, the W3C's Process document dictates that every member has a vote, but that decisions should strive for consensus.[37] Because the membership of the W3C includes not only browser vendors and other tech companies but also universities, government departments, and civil society,[38] that consensus is required to be broadly representative of those groups (provided they choose to show up).

That consensus is also informed by wider discussion because web-related SDOs allow anyone who wishes to take part and contribute (e.g., by submitting draft documents for consideration and filing issues against proposals or existing specifications).

As a result, it would be incorrect to characterise these SDOs as mere venues for agreements between competitors. Their unconditional openness 'may even justify a claim to represent the global public, because everyone has a direct or indirect stake on the Internet, and everyone can participate.'[39]

### C *Market share*

Historically, web browsers have seen significant fluctuations in their market share over time.

In the early years, Netscape Navigator (Firefox's predecessor) held a market share of over 80%, most likely due to it being the first well-supported browser in the market.[40] IE became a dominant force in the market through the 2000s, reaching greater than 95% market share by some accounts.[41] Microsoft obtained this market share at least partially by bundling of the browser their operating system, a practice which stopped in 2009 after agreeing to allow browser choice.

[37] Elika J Etemad and Florian Rivoal, *W3C Process Document* (World Wide Web Consortium, 15 September 2020) s 3.3 <https://www.w3.org/Consortium/Process/>.

[38] 'Current Members', *World Wide Web Consortium* (Web Page) <https://www.w3.org/Consortium/Member/List>.

[39] Biel Company, 'A Public Law Approach to Internet Standards Setting' (2016) 7(1) *Goettingen Journal of International Law* 49, 93 <https://ssrn.com/abstract=2840126>.

[40] Ed Kubaitis, 'Browser Statistics for April 1996' (Web Page, 1996) <https://web.archive.org/web/20010507151202/http://www.ews.uiuc.edu/bstats/months/9604-month.html>.

[41] 'Browser Stats' (Web Page, 2004) <https://web.archive.org/web/20050206164945/https://www.thecounter.com/stats/2004/February/browser.php>.

Chrome, which currently enjoys an approximately 70% share of the web browser market, eventually displaced IE.[42] Its market share has been attributed to factors ranging from technical superiority[43] to imposition of agreements upon Android phone manufacturers that require its installation as the default browser.[44]

Beyond these situational influences, however, browser market shares are likely to fluctuate because of two factors: the relative ease of entry into the browser market, and customers' capacity to react by switching browsers.

### D *Entry into the browser market*

Entry into the browser market relatively easy, thanks to the availability of multiple browser engines with generous licensing terms. For example, Brave was able to launch their browser with seed funding of USD7 million.[45] Vivaldi's founder estimated his investment for the first release of their browser at USD6.07 million, and as requiring five million users to support on an ongoing basis.[46] Both browsers started with an existing browser engine, adding extra features to customise its operation.

The browser engine market, however, has significant barriers to entry. There are substantial costs involved in building and maintaining one, due to the inherent complexity of the web and the burden of assuring compatibility with the considerable variety of content already there. Furthermore, the three major browser engines are all free to use and modify – thereby creating a corresponding downward price pressure on any new browser engine.

This situation has been lamented in the web community, as diversity of browser engines is seen as critical for the long-term health of the web (until recently, there were four major browser engines).[47] Nevertheless, it is unlikely that this market could be characterised as uncompetitive: because of their open

[42] Tim Schiesser, 'Chrome overtakes Internet Explorer in market share', *Neowin* (Web page, 21 May 2012) <https://www.neowin.net/news/chrome-overtakes-internet-explorer-in-market-share>.

[43] Jonathan Tamary, Dror G. Feitelson, 'The rise of Chrome' *PeerJ Computer Science* (2015) 1(28).

[44] *United States of America v Google LLC* (Case 1:20-cv-03010), Complaint [2020] [76].

[45] 'Brave', *Crunchbase* (Web Page) <https://www.crunchbase.com/organization/brave-software/company_financials>.

[46] Joachim Dagenborg, 'Browser startup Vivaldi says needs 5 million users to turn profit', *Reuters* (Web Page, 15 April 2016) <https://www.reuters.com/article/us-internet-vivaldi-idUSKCN0XC1J6>

[47] See, eg, Brian Kardell, 'Web Engine Diversity and Ecosystem Health' (Blog Entry, 26 May 2020) <https://bkardell.com/blog/EcosystemHealth.html>.

licensing terms, another party with sufficient resources could create another browser engine by 'forking' one of the existing ones, as Google did to WebKit to create Blink.[48]

### E *Motivations to enter the browser markets*

Because browsers are typically free, it is reasonable to ask why an undertaking would enter the browser or browser engine market. Creating a browser (and browser engine, in some cases) has a variety of potential benefits, including bolstering an associated operating system platform (in the case of Apple and Microsoft), offering alternative advertising platforms (with Brave), and the public good (in the case of Firefox).

Significantly, both Apple and Mozilla also attract sizeable payments to set Google Search as the default search engine in their browsers – estimated to be between US$400-450 million annually for Mozilla,[49] and a substantial portion of the GBP1.2 billion that Google pays to Apple annually for such defaults in the UK alone.[50]

For large web-based platforms like Google, there are also significant benefits to controlling a browser. When launching Chrome in 2008, Google claimed they were doing so to 'add value for users and… help drive innovation on the web.'[51] However, in 2011 Google's CFO nominated another motivation – that

> everybody that uses Chrome is a guaranteed locked-in user for us in terms of having access to Google… [this] impacts many of our other products that work as part of Chrome. So the lifetime value of a Chrome user is phenomenal.[52]

In this light, Google's continued investment into Chrome and the Blink browser engine and its default payments to its competitors is not surprising.

[48] Steven J. Vaughan-Nichols, 'Blink! Google forks WebKit', *ZDNet* (Web Page, 4 April 2013) <https://www.zdnet.com/article/blink-google-forks-webkit/>.

[49] Catalin Cimpanu, 'Sources: Mozilla extends its Google search deal', *ZDNet* (Web Page, 12 August 2020) <https://www.zdnet.com/article/sources-mozilla-extends-its-google-search-deal/>.

[50] *Online Platforms and Digital Advertising* (n 29) 33.

[51] 'A fresh take on the browser', *Google Official Blog* (Blog Entry, 1 September 2008) <https://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html>.

[52] Larry Dignan, 'Why is Chrome so important to Google? It's a "locked-in user"', *ZDNet* (Web Page, 14 April 2011) <https://www.zdnet.com/article/why-is-chrome-so-important-to-google-its-a-locked-in-user/>

### F *Customers' capacity to react*

From the end consumer side of the web platform, browsers are easily substitutable, even though individual consumers might have personal preferences that make them loyal to a particular product. This creates significant pressure on browsers to be compatible with existing web content, so that they do not lose market share; users are quick to abandon a browser that they perceive as 'breaking the web.'

To foster interoperability, browsers not only take part in SDOs that define new features for the web, they also have created a separate SDO, the Web Hypertext Application Technology Working Group (WHATWG). There, they painstakingly document the exact algorithms that browsers use, to encourage uniform behaviour amongst them.[53] That creates a positive feedback loop whereby increased demand substitutability creates pressure for improved interoperability, thereby encouraging a diverse and highly competitive browser market. Users can multi-home by installing more than one browser if they so wish, although anecdotal evidence suggests that most people have a strong affinity for a particular browser.

### G *Is Chrome dominant in the browser markets?*

Over the history of the web, there have been several dramatic changes in browser and browser engine market shares. While the currently popular browser can be perceived as dominant, that dominance is often based upon the fickle preferences of consumers, rather than durable power. As established above, entry into the browser and browser engine markets is not difficult. Consumers also have a high capacity to react, because they can substitute browsers with relative ease – even when accessing Google's portfolio of sites.

As a result, while Chrome has enjoyed a substantial portion of the browser market in the last few years, an effort to characterise the Privacy Sandbox as anti-competitive will need to show that power as durable, genuinely resistant to new market entrants, with little possibility for consumer substitution.

[53] 'WHATWG – FAQ' (Web Page) <https://whatwg.org/faq>.

# IV The Privacy Sandbox as an abuse of market dominance

The CMA has expressed two distinct competitive concerns. The first is that disallowing third-party cookies (and mitigating workarounds like browser fingerprinting) creates an unfair advantage for Google, because sites that operate their own advertising infrastructure (as Google does) retain the rich targeting and profiling information that third-party advertising services will lose. In this view, Google is 'acting in a quasi-regulatory capacity… setting the rules around data sharing... for other market participants'[54] which can be seen as cross-market exclusionary conduct, with Google leveraging browser-based power for advantage in two other markets that it takes part in (and arguably dominates) – online display advertising and online publishing.

The second concern is that Google's proposals for replacing cookies give them 'the ability to use [Chrome] to favour Google's own adtech intermediation services' thereby making it likely that 'Google's position in the adtech ecosystem will remain central.'[55]

Considering these concerns with the context above in mind, we can now turn to the question of how the Privacy Sandbox intersects with European competition law.

Doing so with certainty is difficult. Nazinni points out that '[c]onsiderable uncertainty and a significant degree of controversy surround the tests that determine whether conduct is abusive under Article 102'[56] with the further complication that the relevant 'case law… has developed in a haphazard fashion, [without focus on] the need to set out clear rules and principles applicable in future cases.'[57]

Furthermore, with its many genuinely unique aspects, determining the exact nature of this allegedly abusive conduct is not clear-cut. It may be that a novel

[54] *Online Platforms and Digital Advertising* (Final Report, 2020) 47 <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.

[55] *Online Platforms and Digital Advertising Final Report, Appendix G: The Role of Tracking in Digital Advertising* (n 13) 108–9.

[56] Renato Nazinni, *The Foundations of European Union Competition Law* (Oxford University Press, 2011) 155.

[57] Ibid 156.

form of abuse is found (as in *Google Shopping*),[58] because the examples in Article 102 are not exhaustive.[59] That said, relating it to an existing form of abuse allows us to examine it in the light of existing case law and Commission guidelines.

Therefore, I consider the Privacy Sandbox by analogy to a vertical foreclosure of a downstream market, reasoning that by removing support for third-party cookies and other tracking mechanisms in its offerings in the web browser market, Google's actions can be seen to have a negative impact on competition in the display advertising market. This approach would invoke Article 102(b)'s prohibition on 'limiting production, markets or technical development to the prejudice of consumers.'[60]

This is not a perfect analogy. For example, although Google's conduct is in the browser market, the party selecting and using that product is a third party (the browser's user), not a participant in the affected display advertising market. As such, it does not represent a directly connected vertical market. However, considering it in this manner does allow us to touch upon many relevant aspects of the law.

This Part will examine the Privacy Sandbox as a refusal to supply, by first establishing Google's dominance in Section A, then evaluating it under the Commission's Guidelines in Section B. Section C highlights a resulting paradox, and Section D examines whether the Privacy Sandbox can be said to represent Google's conduct.

## A *Establishing Google's dominance*

An undertaking must be considered dominant in a relevant market before their conduct can be evaluated for abuse. Furthermore, there needs to be some 'link between the dominant position and the alleged abusive conduct.'[61] For the Privacy Sandbox the browser markets, the display advertising market

[58] *Google Search (Shopping)* (Case AT.39740), Commission Decision [2017].

[59] See, eg, *Europemballage Corporation v Continental Can Company v Commission* (C-6/72) [1973] ECR 217, 245 [26].

[60] *Consolidated Version of the Treaty on the Functioning of the European Union*, 26 October 2012, OJ L 326/47, Article 102(b).

[61] *Tetra Pak v Commission* (C-333/94 P) [1996] ECR I-5987, I-6008 [27]; see also Thomas Eilmansberger, 'How to Distinguish Good from Bad Competition under Article 82 EC' (2005) 42 *Common Market Law Review* 129, 140–6.

(including its component submarkets),[62] and the online publishing market are both relevant.

As discussed above, Google's *prima facie* dominance of the browser markets due to market share is qualified: in particular, it is subject to constraints due to the relative ease of entry into the market, its customers' capacity to react, and the standards and practices that define what a web browser is. While Google's considerable (and perhaps durable) market power could be used to establish its dominance, its ability to harm competition with power in browser markets has limits.

If Google is nonetheless found dominant in one or more of the browser markets, we can assume that its conduct 'played a decisive role in the practice bringing about the relevant effect,'[63] thereby linking dominance to conduct. If, however, Google is judged to not be dominant in any browser market, its dominance of the display advertising and online publishing markets (globally, including the EU) can be relied upon, having been established convincingly by many sources.[64]

Establishing a link in that case is less straightforward. The indirect relationship of Google's dominance in display advertising to its allegedly abusive conduct as a browser vendor implies a need to judge the conduct's effects, rather than considering it *per se* abusive. This makes analysing Google's conduct as a refusal to supply problematic, because 'the desired leveraging effect can only be achieved if the firm dominates the input market'[65] – in this case, browsers.

As such, a successful argument that Google's dominance in the display advertising and/or online publishing markets is linked to its allegedly abusive behaviour would need to break new ground. The most obvious link – the dependence of the display advertising market upon browser behaviour – does not fit the pattern of other links found in case law.[66]

[62] See, eg, Damien Geradin and Dimitrios Katsifis, 'An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age' (2019) 15(1) *European Competition Journal* 55, 66–9 <https://doi.org/10.1080/17441056.2019.1574440>.

[63] Eilmansberger (n 59) 143.

[64] See, eg, Dina Srinivasan, 'Why Google Dominates Advertising Markets: Competition Policy Should Lean on the Principles of Financial Market Regulation' (2020) 24(1) *Stanford Technology Law Review* 56 <https://ssrn.com/abstract=3500919>; Geradin and Katsifis (n 60) 69–72.

[65] Eilmansberger (n 59) 144.

[66] Ibid 140–6.

## B *Evaluation of abuse*

If the hurdle of establishing Google's dominance and linking it to the conduct in question can be overcome, we would next turn to determining whether the Privacy Sandbox qualifies as abusive conduct.

The Commission's 2009 Guidance on Article 102[67] only attempts to document what they will prioritise for enforcement: as per Nazinni,

> [i]t is not guidance on the substantive tests for abuse [and] applies only as a matter of administrative discretion… is, at most, weakly persuasive… [and] is not always consistent with the case law.[68]

Nevertheless, it is a useful tool for structuring an evaluation of whether Google's conduct is abusive, if considered in the light of applicable case law. In deciding whether to prioritise enforcement actions for refusal to supply (in this case, a constructive[69] disruption[70] of supply), the Commission considers three factors.[71]

### 1 Objective necessity

The first factor is whether the refused input is 'objectively necessary to be able to compete effectively on a downstream market.'[72] In particular, if adtech vendors could duplicate the input in question in order 'to exert a competitive constraint on the dominant undertaking,'[73] enforcement for refusal of supply is unlikely to attract priority.

Members of the display advertising industry have discussed several potential substitutions for third-party cookies and fingerprinting as a source of targeting.

[67] 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (24 February 2009) ('Guidance on Abusive Conduct').

[68] Nazinni (n 54) 155.

[69] 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (n 65) [79].

[70] Ibid [84].

[71] Ibid [81].

[72] Ibid [82].

[73] Ibid [83].

Some market participants are using first-party information to target advertising in a process known as *identity resolution*.[74] A site can use the information it holds about its users (typically, because they are logged in, or they have substantial interactions with the site) to create segments of users and sell them directly to advertisers or make them available through an intermediary. The New York Times has done so since July 2020 and is phasing out third-party cookies in 2021.[75]

This is the advantage that Google is alleged to be reserving for itself: because of its considerable scope, scale, and access to data as an online publisher, it has an allegedly unfair advantage it has over smaller publishers (and the dependent display advertising industry).

However, smaller publishers can pool their first-party data without creating a profile for each user using techniques like differential privacy,[76] thereby creating a counterbalance to Google's advantages in data. Several companies offer products with the ability to target display advertising in this fashion,[77] often touting them as an improvement over third-party cookies:

> When Fitbit ran an A/B test using LiveRamp's identifier vs. third-party cookies, it doubled its [return on advertising spend], decreased cost-per-page-view by 34%, and increased average order value by 13%.[78]

Of course, Fitbit is now being acquired by Google, a move that has raised several competition regulators' eyebrows, but the point stands.

Identity resolution is not suitable for all sites – in particular, those who do not have such rich information about their users, because the users do not engage

[74] See, eg, Robin Kurzer, 'What is identity resolution?', *Martech* (Web page, 17 January 2019) <https://martechtoday.com/what-is-identity-resolution-229737>.

[75] Sara Fischer, 'Exclusive: New York Times phasing out all 3rd-party advertising data', *Axios* (Web page, 19 May 2020) <https://www.axios.com/new-york-times-advertising-792b3cd6-4bdb-47c3-9817-36601211a79d.html>.

[76] See, eg, 'Differential Privacy', *Harvard University Privacy Tools Project* (Web Page), <https://privacytools.seas.harvard.edu/differential-privacy>.

[77] See, eg, 'Identity Graph: Connecting Data for Better Customer Relationships', *Liveramp* (Web Page) <https://liveramp.com/our-platform/identity-graph/>; 'How we'll help you succeed in a world without third-party cookies', *Epsilon* (Web Page) <https://us.epsilon.com/epsilon-peoplecloud-overview/digital-media-solutions/cookieless-solution>.

[78] Travis Clinger, 'Chrome Announces End of Third-Party Cookies: One Year Later' *LiveRamp* (Blog Entry, 15 January 2021) <https://liveramp.com/blog/chrome-announces-end-third-party-cookies-one-year-later/>.

as closely with them. For these sites, remaining competitive requires another targeting mechanism.

One option is contextual advertising: serving ads based upon the content that someone is looking at, rather than behaviourally targeting them at a user profile. Again, multiple adtech vendors already offer this service,[79] including Google.[80] One test in 2013 found that consumers were 82% more likely to recall contextual ads, because they were more relevant to what the user was interested in that that time.[81]

Yet another option is panel-based advertising: that is, having a subset of consumers explicitly opt into being tracked (for example, with a special browser plugin) and being compensated for doing so. Effectively, this samples the audience, giving marketers the data that they desire. Once again, multiple adtech vendors offer this service.[82]

Finally, some Privacy Sandbox proposals themselves have the intent of replacing functions that advertising currently uses third-party cookies for. For example, the Federated Learning of Cohorts (FLoC) proposal allows advertisers to access a person's general interests for targeting purposes in a way that is intended to preserve privacy.[83] Google's tests indicate it is 95% as

[79] See, eg, 'Contextual ads' *Media.net* (Web Page) <https://www.media.net/contextualads/>; 'Contextual targeting that puts your brand in the best light' GumGum (Web Page) <https://gumgum.com/advertisers>.

[80] 'Contextual Targeting' *Google Ads Help* (Web Page) <https://support.google.com/google-ads/answer/1726458?hl=en>.

[81] 'Beating Banner Blindness', *Infolinks* (Report, July 2013) <http://resources.infolinks.com/static/eyetracking-whitepaper.pdf>.

[82] See, eg, Allison Schiff, 'Comscore is Evolving its Audience Targeting Tool away from Cookies', *AdExchanger* (Web Page, 11 January 2021) <https://www.adexchanger.com/data-exchanges/comscore-is-evolving-its-audience-targeting-tool-away-from-cookies/>; 'Pathmatics Launches First Panel-Based Paid Social Ad Intelligence', *MarTechSeries* (Web Page, 8 December 2017) <https://martechseries.com/sales-marketing/programmatic-buying/pathmatics-launches-first-panel-based-paid-social-ad-intelligence/>; Karlene Lukovitz, 'Nielsen Launches Metric Combining Panel and ACR Data', *MediaPos*t (Web Page, 13 December 2019) <https://www.mediapost.com/publications/article/344572/nielsen-launches-metric-combining-panel-and-acr-da.html>.

[83] 'Federated Learning of Cohorts (FLoC)', *Web Incubator Community Group* (Web Page) <https://github.com/WICG/floc>.

effective as cookie-based tracking,[84] but advertising industry representatives have questioned the methodology used.[85]

Judging the substitutability of these alternatives for cookie-based behavioural tracking information is controversial and subjective. Some industry sources claim that removing cookies leads to publishers' ad revenues dropping by 98%,[86] but a Google study indicates a 52% decrease,[87] while Marotta, Abhiskeh and Acquisti show that retaining cookies increases publishers' revenue by only 4%.[88] The market has also been found to have significant inefficacies,[89] with one analysis finding 55% of advertisers' funds going to tech vendors rather than publishers.[90]

Despite these uncertainties, many industry participants have already accepted 'the death of third-party cookies' and are now focusing their attention upon these substitutions, viewing it as an opportunity to transform the industry. [91]

[84] Sara Fischer, 'Google says it may have found a privacy-friendly substitute to cookies', *Axios* (Web Page, 25 January 2021) <https://www.axios.com/google-privacy-friendly-substitute-cookies-test-05c2c28e-77f1-4921-9a99-1ef0c009b064.html>.

[85] Karen Myers, 'Meeting minutes', *Improving Web Advertising BG* (Web Page, 26 January 2021) <https://www.w3.org/2021/01/26-web-adv-minutes.html#t03>.

[86] Laura Bassett, 'Digital Media is Suffocating – and it's Facebook and Google's Fault', The American Prospect (Web Page, 6 May 2019) <https://prospect.org/culture/digital-media-suffocating-and-facebook-google-s-fault/>.

[87] Deepak Ravichandran and Nitish Korula, 'Effect of disabling third-party cookies on publisher revenue' (Web Page, 27 August 2019) <https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf>.

[88] Veronica Marotta, Vibhanshu Abhishek and Alessandro Acquisti, 'Online Tracking and Publishers' Revenues : An Empirical Analysis' [2019] *Workshop on the Economics of Information Security* 1.

[89] 'ISBA Programmatic Supply Chain Transparency Study' (Report, May 2020) <https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf>.

[90] Ross Benes, 'Why Tech Firms Obtain Most of the Money in Programmatic Ad Buys', *Insider Intelligence* (Web Page, 16 April 2018) < https://www.emarketer.com/content/why-tech-firms-obtain-most-of-the-money-in-programmatic-purchases>.

[91] See, eg, Allison Schiff, 'Vox Media is All In on the Open Web', *AdExchanger* (Web Page, 16 December 2020) <https://www.adexchanger.com/the-sell-sider/vox-media-is-all-in-on-the-open-web/>; Erik Requidan, 'Privacy Regs and Chrome Changes Will Force an Evolution for Mid- and Long-Tail Publishers, Not Extinction', *AdExchanger* (Web Page, 10 April 2020) <https://www.adexchanger.com/the-sell-sider/privacy-regs-and-chrome-changes-will-force-an-evolution-for-mid-and-long-tail-publishers-not-extinction/>; Jasmine Giuliani, 'The Cookie-pocalypse: Interview with Kat Warboys', *Marketing* (Web Page, 27 April 2020) <https://www.marketingmag.com.au/hubs-c/interview-94909-2/>; Richy Glassberg, 'The Digital Advertising Sector's Original Sin, and How We Must Atone', *AdExchanger* (Web Page, 1 December

Over time, it should become clear whether these potential substitutes can exert a competitive constraint on Google. While third-party cookies are undoubtedly essential for adtech businesses who are heavily invested in them, it is far less clear that they are essential for a competitive market in display advertising.

## 2 Elimination of competition

The second factor that the Commission looks for is that the refusal is 'generally liable to eliminate, immediately or over time, effective competition in the downstream market.'[92]

Applying the Commission's metrics,[93] Google's market share (in both display advertising and publishing), the relative lack of capacity constraints on them, the high substitutability in the advertising marketplace (thanks to standard advertising practices), the high proportion of competitors that will be affected all point to this outcome. The only factor that remains in question is the likelihood of demand being diverted.

However, that is the operative question. *Continental Can* found that effective competition was eliminated when 'the degree of dominance reached substantially fetters competition, i.e., that only undertakings remain in the market whose behaviour depends on the dominant one.'[94] As discussed, the multiple avenues for substitutability available suggest that limitations on third-party cookies do not necessarily lead to dependence upon Google.

Furthermore, *GlaxoSmithKline* found effective competition to be 'the degree of competition necessary to ensure the attainment of the objectives of the Treaty.'[95] That brings into question how the competition aims will be balanced with other objectives – in particular, consumer welfare and data protection.

2020) <https://www.adexchanger.com/data-driven-thinking/the-digital-advertising-sectors-original-sin-and-how-we-must-atone/>.

[92] 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (n 69) [85].

[93] Ibid.

[94] *Europemballage Corporation v Continental Can Company* (n 62) 245 [26].

[95] *GlaxoSmithKline Services Unlimited v Commission* (T-168/01) [2006] ECR II-2981, II-3012 [109].

### 3 Balancing harmful consequences

The final factor is whether 'the likely negative consequences of the refusal to supply… outweigh over time the negative consequences of imposing an obligation to supply' regarding consumer harm.[96]

The direct negative consequence of refusing to supply online tracking information is reduced competition in advertising services. This is likely to harm individual consumers as well as businesses through increases in costs of advertising, which will probably be passed through to them. It also harms adtech businesses, which are also a consumer of this data.

An obligation to supply in this case would mean a requirement to continue allowing behavioural tracking. While there is an obvious consumer harm involved – damage to privacy caused by the restriction of architectural regulation – it is not immediately clear that would be considered. There is limited guidance on theories of consumer harm for unilateral conduct,[97] with the only explicit examples consisting of economic harms such as the '[prevention] of bringing innovative goods or services to market.'[98]

However, that is based upon competition law alone. Article 12 requires consumer protection to be considered in implementing other policies.[99] As consumer protection includes the ultimate consumer and is widely held to include data protection,[100] it follows that the Commission needs to take it into account in competition enforcement,[101] just as the Bundeskartellamt did when ruling against Facebook.[102]

[96] 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (n 65) 86.

[97] Hans Zenger and Mike Walker, 'Theories of Harm in European Competition Law: A Progress Report' [2012] *SSRN eLibrary* 29 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2009296&rec=1&srcabs=2044722>.

[98] 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (n 69) [87].

[99] *The Treaty on the Functioning of the European Union* (n 58) Article 12.

[100] 'Privacy and Competitiveness in the Age of Big Data' (March 2014) *Preliminary Opinion of the European Data Protection Supervisor* 19 [36].

[101] Anca D. Chirita, 'Undistorted, (Un)fair Competition, Consumer Welfare and the Interpretation of Article 102 TFEU' (2010) 33(3) *World Competition: Law and Economics Review* 417; cf Suzanne Kingston, 'Integrating Environmental Protection and EU Competition Law: Why Competition Isn't Special' (2010) 16(6) *European Law Journal* 780.

[102] *Facebook v Verbraucherzentrale Bundesverband* (B6-22/16) 6th Decision Division [2019].

Again, how these concerns will be ultimately balanced is highly subjective and controversial. That said, the availability of potential privacy-preserving substitutes for cookies strongly suggests a path forward.

### C *The display advertising paradox*

When considered together, the essential nature of third-party cookies in the display advertising market and the accepted definition of that market present an additional hurdle in the form of a paradox.

The CMA states that 'third-party cookies are a fundamental building block of open display advertising and make possible the flow of data about users… needed to target advertising and measure conversions.'[103] If this is indeed true, it will bolster the case for finding that their removal in Chrome is abusive.

However, third-party cookies enable the very attributes that distinguish the online display advertising market from the offline advertising market in case law, bringing the possibility of a larger redefinition of that market when they are removed. For example, *Google/Doubleclick* found that with online advertising

> [a]dvertisers can precisely target their audience by combining information regarding geographical location, time of day, areas of interest, previous purchasing record of the user and search preferences. This option is not available in the case of offline advertising, for which the amount of "wasted circulation" is undoubtedly higher.[104]

Furthermore, it is distinguished because

> while offline pricing is in general based on "impressions" viewed by a possible number of consumers (and estimated on the basis of general criteria), online advertising is paid on the basis of the number of internet viewers that effectively establish a contact with the ad.[105]

If these distinguishing factors are no longer present in online display advertising, or they are significantly changed by the removal of third-party cookies, a new (and likely larger) market definition will need to be found, and Google's conduct evaluated within that context. This could be seen to benefit

[103] *Online Platforms and Digital Advertising Final Report, Appendix G: The Role of Tracking in Digital Advertising* (n 13) 68.

[104] *Google/Doubleclick* (Case COMP.M.4731) Commission Decision [2008], 17-18 [45].

[105] Ibid 18 [46].

Google because of a *relative* reduction in its dominance of the display advertising market – which could be critical to maintain if dominance in the browser market cannot be relied upon.

That is not to say that one company's power to redefine a market unilaterally should not cause concern. However, this brings us to the next hurdle: whether the removal of third-party cookies represents Google's conduct or a broader change in the browser market's features.

### D *Does the Privacy Sandbox represent Google's conduct?*

The catalyst for any action against Google is 'the conduct, by commission or omission, which that undertaking decides on its own initiative to adopt.'[106] In determining whether such initiative exists, we can consider each proposals' specification and implementation status.

If Google (through Chrome) unilaterally specifies and implements a proposal, this is undoubtedly conduct representing its own initiative. However, if Chrome implements a proposal that was first proposed by another browser vendor, was developed in concert with other browser vendors, or perhaps even started by Google but then discussed, adopted, and implemented by other browser vendors, does this still represent Google's initiative?

Furthermore, if a broad, consensus-based interoperability standard encourages (or even requires) Google to implement changes which have the effect of diminishing competition in other markets it participates in, is this still Google's conduct? I argue that in following practices of other members of its market, especially when that conduct is sanctioned or required by interoperability standards, Google's initiative is extinguished, or at least diminished – at least to the degree where the lack of third-party cookies becomes a structural issue in the market, rather than merely conduct by one (albeit dominant) actor in it. While it may be that inoffensive conduct becomes abusive merely because it was carried out by a dominant undertaking, that arguably applies to independent conduct, not concerted action that is better characterised as part of the market's self-governance.

For example, blocking third-party cookies is the Privacy Sandbox proposal most relevant to competition concerns . Google has indicated that it will work towards that goal over a multi-year period, while developing technologies that

[106] *Konkurrensverket v Teliasonera Sveriege AB* (C-52/09) [2011] ECR I-564, I-582-3 [53].

replace some functions of cookies in a privacy-promoting fashion.[107] In doing so, Google is not alone; other browsers have taken different paths towards the same goal. For example, Safari has introduced Intelligent Tracking Prevention;[108] Firefox has Enhanced Tracking Protection.[109] Both approaches are broadly equivalent to Google's proposal and are already implemented.

Arguably, then, Google's removal of third-party cookies is not unilateral, because doing so has some amount of SDO consensus (due to the warnings and permissions already present in the Cookie specification), and enjoys broad implementation in other browsers, through functionally similar (if not identical) measures.

This argument can be supported by considering the *ex ante* counterfactual.[110] A world where Chrome does not implement the Privacy Sandbox would likely lead to a competitive disadvantage for Chrome on the web browser market, in that some consumers would be apt to switch to more privacy-preserving browsers – possibly, enough to represent a change in market power. This would not necessarily translate to more competition in the affected display advertising and publishing markets, and would also create potential consumer harm for those users who stay on Chrome and are unaware of the privacy implication of doing so.

An *ex post* counterfactual is worth considering as well, given the distinct nature of the web browser market and its governance by the web platform. If Google had never forked WebKit to create Blink and then Chrome, it is likely that the remaining browsers at the time – Firefox, Safari, and Internet Explorer (now Edge) – would still have significant market share, to varying degrees. All three have made significant efforts at regulating privacy though architecture, with Enhanced Tracking Prevention,[111] Intelligent Tracking Protection (ITP),[112] and

[107] 'Building a more private web: A path towards making third party cookies obsolete', *Chromium Blog* (Blog Entry, 14 January 2020) <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>.

[108] Wilander (n 12).

[109] 'Enhanced Tracking Protection in Firefox for Desktop' (n 12).

[110] As per 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (n 65) [21].

[111] 'Enhanced Tracking Protection in Firefox for Desktop' (n 12).

[112] Wilander (n 12).

Tracking Prevention,[113] respectively. While by nature *ex post* counterfactuals are unreliable, it is difficult to see how the display advertising market would not currently be facing architectural regulation in a world without Chrome.

In this view, the Privacy Sandbox projects concerning the prevention of cross-site tracking (specifically, those related to third-party cookies and prevention of fingerprinting) do not convey a special responsibility for Google to avoid impairing competition in the display advertising and publishing markets, because similar measures have already been implemented in other browsers, or are being actively contemplated by them. Adoption of these measures across the market is taken as an indicator that competition regulators should refrain from considering Google's behaviour as abusive, despite it being well-established that a dominant undertaking can be held to a higher standard.

On the other hand, the Privacy Sandbox projects that appear to be more unilateral – for example, FLoC and TURTLE-DOV – may very well attract such a responsibility. That might change if other browsers show interest, provide input, and eventually implement, and especially if they achieve consensus in a relevant SDO.

## V Identifying unilateral browser behaviour in SDOs

To date, competition authorities have largely considered SDOs largely as venues for sanctioned horizontal agreements, with a correspondingly narrow focus on Article 101(3). However, the CMA recognises that 'there is an opportunity to explore the role of internet governance forums such as the W3C, WHATWG and IETF in enhancing consumer protection online.'[114] If it is accepted that the blessing of one of these SDOs might lessen the risk of unilateral abusive conduct, it is reasonable to ask what the CMA, the Commission, or a Court should consider.

One relevant factor is the nature of the specific venue that a discussion is taking place in. While most web related SDOs are open to broad participation,

[113] 'Tracking Prevention in Microsoft Edge (Chromium)', *Microsoft* (Web Page, 27 October 2020) <https://docs.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention>.

[114] *Online Platforms and Digital Advertising Final Report, Appendix G: The Role of Tracking in Digital Advertising* (n 13) 27.

each has different ways of convening work and gathering specific communities, and those sub-fora have different properties.

For example, the W3C Improving Web Advertising Business Group[115] has been the focus of many discussions related to the Privacy Sandbox, but its status as a Business Group means that it cannot represent consensus of the entire organisation and does not receive cross-organisation review. Effectively, it is a self-organised group where the specific rules of discourse and decision-making are left to the conveners, with only broad guidelines to be 'fair.'[116] It does not necessarily represent an agreement amongst browser vendors, and its output cannot be considered as binding them.

Likewise, the W3C Web Platform Incubator Community Group (WICG)[117] is used extensively by Chrome for exposing its proposals to a wider audience.[118] Although its output is often mistaken for a W3C Recommendation (the designation of a specification which has achieved consensus), it has no such status, and other browser vendors might comment upon work there without committing to its output.

These groups serve an important purpose by offering a place for initial discussion and refinement of ideas and building a community of contributors. However, their work does not necessarily have properties that are important to competition regulators – in particular, broad review and input, representative participation and decision-making, and a robust oversight process.

In contrast, venues like W3C and IETF Working Groups are required to conform to more stringent requirements regarding intellectual property disclosures and licensing, participation, decision-making , cross-organisation review, and appeal. Their work is also more visible in the relevant communities, leading to more representative participation.

[115] 'Improving Web Advertising Business Group', *World Wide Web Consortium* (Web Page) <https://www.w3.org/community/web-adv/>.

[116] 'About W3C Community and Business Groups', *World Wide Web Consortium* (Web Page) <https://www.w3.org/community/about/#bg>.

[117] 'Web Platform Incubator Community Group', *World Wide Web Consortium* (Web Page) <https://www.w3.org/community/wicg/>.

[118] See, eg, Thomas Steiner et al, 'From Fugu with Love: New Capabilities for the Web' [2020] *The Web Conference 2020 - Companion of the World Wide Web Conference, WWW 2020* 135, s 1.3.

For example, the IETF HTTP Working Group[119] is currently revising the Cookie specification,[120] based upon input from not only browser vendors but also HTTP experts, civil society members, and other interested parties. It does so under the auspices of the Internet Standards Process,[121] just as other key technologies like HTTP, TCP, IP and DNS are.

It should be noted, however, that the decision processes of these bodies do not necessarily require perfect consensus between stakeholders; organisational goals such as interoperability, security, privacy and user benefit may cause the outcomes to disadvantage some parties, after due deliberation and consultation.[122] For the purposes of competition authorities, this is appropriate; there need not be agreement across all parties relevant to the web platform to prevent unilateral conduct in the web browser market.

Likewise, the creation of a formal body such as a Working Group does not always reflect consensus amongst browser vendors. For example, serious concerns were expressed about the formation of the IETF Web Packaging Working Group, which is working on technology related to Google AMP. In a workshop held to explore these concerns, 'several online publishers indicated that if it weren't for the privileged position in the Google Search carousel given to AMP content, they would not publish in that format.'[123] Notably, Mozilla classified Web Packaging as 'harmful' to the web.[124] As a result, browser implementation plans should be considered concurrently with standardisation status. Vendors often make this explicit as an aid to the standardisation process; for example, Mozilla has a public list of its positions on various proposals for standardisation.[125]

[119] 'HTTP Working Group' (Web Page) <https://httpwg.org/>.

[120] Mike West and John Wilander, *Cookies: HTTP State Mechanism* (IETF Internet-Draft, 29 January 2021) <https://httpwg.org/http-extensions/draft-ietf-httpbis-rfc6265bis.html>.

[121] Scott Bradner, *The Internet Standards Process -- Revision 3* (IETF Best Current Practice, October 1996) <https://tools.ietf.org/html/rfc2026>.

[122] See, eg, Mark Nottingham, *The Internet is for End Users* (IETF Informational RFC, August 2020) <https://tools.ietf.org/html/rfc8890>; Pete Resnick, *On Consensus and Humming in the IETF* (IETF Informational RFC, June 2014) <https://tools.ietf.org/html/rfc7282>.

[123] Martin Thomson and Mark Nottingham, Report from the *IAB Workshop on Exploring Synergy between Content Aggregation and the Publisher Ecosystem (ESCAPE)* (IAB Informational RFC, March 2020) <https://tools.ietf.org/html/rfc8752.html>.

[124] 'RFP: Web Packaging Format' *Mozilla Standards Positions* (Web Page) <https://github.com/mozilla/standards-positions/issues/29>.

[125] 'Mozilla Specification Positions' (Web Page) <https://mozilla.github.io/standards-positions/>.

Another relevant factor is the status of a technical specification in question. This is often confusing to those unused to working with SDOs, with a proposal that has no formal status being cited as a standard, lending it undeserved credibility. This can be avoided by understanding the venue in which the document resides within and their system of status indicators. For example, the Client Hints specification has a status of *Experimental*, reflecting a compromise where no browser vendor besides Chrome was willing to commit to implementing it, but there was not a strong objection to its adoption.[126]

## VI Conclusion

This paper has explored some of the hurdles that that the CMA (or the Commission) would face in establishing the Privacy Sandbox as a constructive disruption of supply. While a different or even novel form of abuse might be found, it would face many of the same issues, and perhaps others (e.g., the issue of Google's intent).[127]

While the loss of third-party cookies undoubtedly disrupts some businesses and may pose some challenges for funding smaller publishers, that alone is insufficient to invoke abuse of dominance. The emergence of responses that follow 'privacy by design' principles is a promising market development that makes *ex ante* enforcement undesirable, as they could have the effect of preventing changes that benefit consumers.

And, while Google's actions as a browser vendor as should be carefully monitored for potential abuse, characterising them as a gatekeeper being able 'to decide for everyone the "right" trade-off between privacy, competition, and efficiency, and impose their value judgment on all ecosystem participants'[128] is premature, given the state of the proposals in the greater context of architectural regulation of the web.

This is not to say that these hurdles are insurmountable, or that Google's scale, scope, and access to data as an online publisher and advertising platform

[126] Ilya Grigorik and Yoav Weiss, *HTTP Client Hints* (IETF Experimental RFC, 29 January 2021) <https://httpwg.org/http-extensions/draft-ietf-httpbis-client-hints.html>.

[127] Nazinni (n 54) 187.

[128] Geradin, Katsifis and Karanikioti (n 3) 35.

are not concerning. It may very well be that various remedies to their apparent abuse(s) of power will need to be imposed by competition authorities.

However, addressing Google's market power by hobbling privacy on the web platform is not good policy. Government intervention in information technology standards setting carries many risks due to the sophisticated nature of the material and the international implications of such an intervention.[129] In particular, doing so could hobble the ability of the internet to evolve.

Instead, the CMA (and other competition authorities) should only consider enforcement related to Chrome when a proposal reflects unilateral action within the web browser markets, relying at least partially on signals from SDOs and other browser and browser engine vendors to make that determination.

For example, a CMA injunction to prevent Google from changing its third-party cookie policy would be inappropriate in this view, because it is not truly unilateral behaviour. On the other hand, an injunction to prevent Google from shipping FLoC (for example) before it went through a consensus process and/or saw implementation by other browsers – if there were specific competitive concerns regarding it – could be quite reasonable.

Finally, both competition regulators and SDOs can and should facilitate this process through better communication. Competition regulators that understand the nuances of the standardisation process can make better determinations based upon the signals it gives; SDOs that understand the needs of competition regulators can better anticipate how to clearly signal the status of a given work item.

[129] Stacy Baird, 'The Government at the Standards Bazaar' in Laura DeNardis (ed), *Opening Standards: The Global Politics of Interoperability* (MIT Press, 2011) 13.