moz://a

CMA MOBILE BROWSERS AND CLOUD GAMING MARKET INVESTIGATION

Mozilla response to Statement of Issues

17 January 2023

1. Introduction

Mozilla is a unique public benefit organisation and open source community formed as a non-profit foundation. It is guided by a set of principles[1] recognising that, among other things, the internet is integral to modern life; the internet must remain open and accessible; security and privacy are fundamental; and that a balance between commercial profit and public benefit is critical.

As the developer of products including the Firefox browser and the Gecko browser engine, Mozilla has participated in the CMA's Mobile Ecosystems Market Study[2] and welcomes the opportunity to comment on the mobile browser issues set out in the Statement of Issues in the context of the mobile browsers and cloud gaming market investigation ("Market Investigation").

Mozilla supports the Market Investigation and broadly agrees that:

- The CMA has identified the relevant theories of harm to investigate. Further, it is Mozilla's experience that many of the issues identified at 27(a) to (f) are in fact adversely affecting competition with regard to mobile browsers and browser engines.
- The CMA should focus on those remedies identified at paragraphs 57 onwards.

While Mozilla acknowledges that the different theories of harm may be considered and addressed separately, we note that many of the issues being considered are deeply connected and interrelated. Accordingly, Mozilla believes that, to be most effective, the remedies set out in this response should be considered together and implemented in full.

[1] https://www.mozilla.org/en-GB/about/manifesto/details/
[2] https://assets.publishing.service.gov.uk/media/6229acf6e90e0747aa8eb698/Mozilla.pdf

2. The CMA can address indirect network effects and resulting web compatibility issues through encouraging the use of formal standards developments organisations

The CMA's Market Study rightly found that web compatibility is a barrier to competition between different browsers and browser engines and that the existence of open standards have not in practice remedied this issue. It noted that this is caused by certain browsers releasing features without going through formal standards development organisations (SDOs) and web developers developing for specific browsers rather than against standards.[3]

Indirect network effects reinforce both of these problems: the more users a browser engine has, the larger its ability to bypass formal standards and, in turn, the more likely developers are to ensure their websites are compatible with that browser engine. When adhered to by market participants, open standards are a powerful tool to encourage interoperability, reduce network effects, lower barriers to entry and ultimately enhance competition and choice.

Ensuring effective web compatibility on the open web is a shared responsibility between service providers and browser vendors, where both parties must implement standards in a manner that allows for services to work seamlessly (within reason) regardless of the engine or operating system. In the context of the Market Investigation, this relates to the role and responsibility of browser vendors in implementing these web standards and its corresponding impact on web compatibility.

Certain practices currently prevent the conditions required for interoperability (and ensuing web compatibility) with competitor products in the browser ecosystem. This includes when dominant players:

1. Design, test and release features primarily for their own affiliated platform products. This is the case, for example, when Google Widevine (which provides critical DRM services to Firefox) and YouTube are designed first for Chrome and feature gaps are later addressed for other browsers, if at all.
2. Design, test and release features without going through formal SDOs and processes. This is why Mozilla has advocated that Google's Chrome Privacy Sandbox proposals should be developed at SDOs.

[3] Final Report, page 163

3. Design, test and release features without adhering to existing SDO specifications or the commitments made. This is what happened with WebRTC, as detailed in previous submissions to the CMA.[4]

The first practice is a business decision to self-preference to the detriment of competitor and third-party companies. The second and third practices are business decisions not to formally engage in or implement the outcomes of voluntary multi-stakeholder public standards development.

Sometimes these decisions may have valid rational business reasons whereas others may be unintentional. Regardless of the reason, harmful network effects can occur when such actions are undertaken by dominant players, where features may not be available, may appear late, or may have inferior performance on rival operating systems and browsers. This has a direct consequence on rival browser functionality and consumer usage because when key web services and web pages do not work on a rival browser consumers will switch back to the browsers on which these services do work.

This in turn creates powerful lock-in effects for consumers and increases their switching costs to try and stick with rival browsers. In this regard, even motivated consumers will be deterred from switching to alternative solutions if effective interoperability is not guaranteed.

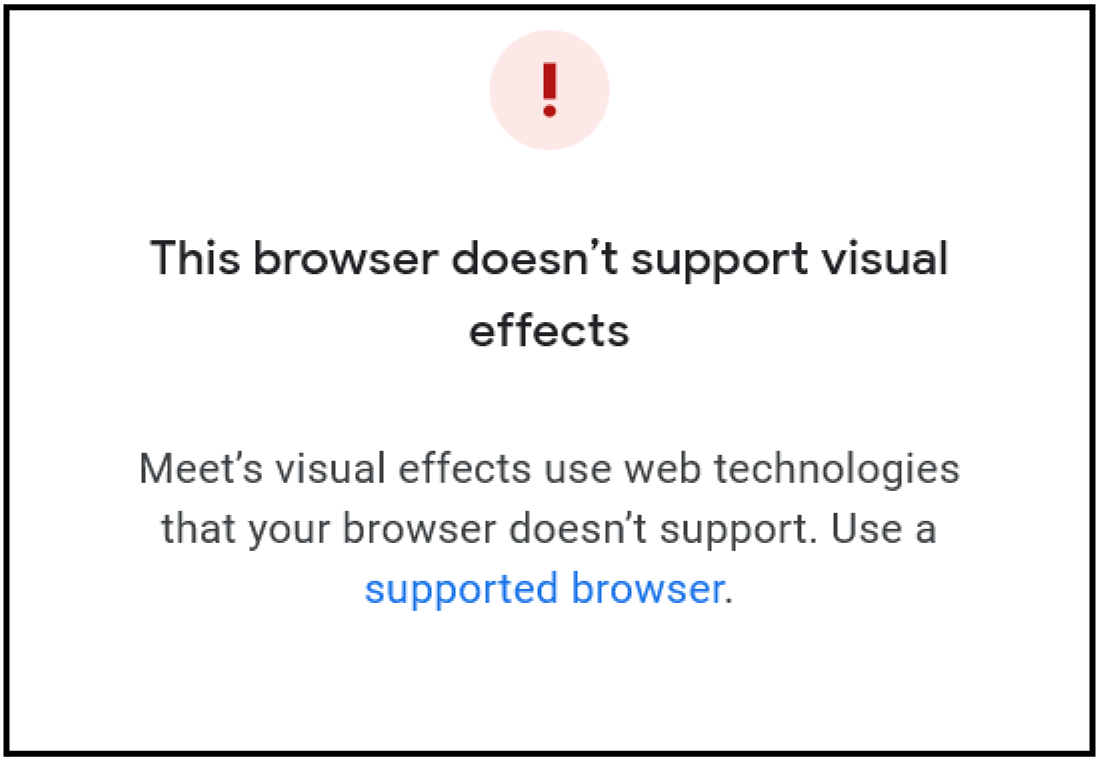
Web compatibility also creates a burden on companies like Mozilla that have to invest financial and human resources into evaluating and minimising, if even possible, the lack of interoperability and ensuing web compatibility breakage. Mozilla has an entire web compatibility team that is dedicated to identifying and attempting to resolve issues with developers. The team relies on community reports from dedicated Firefox consumers, such as through Mozilla's website webcompat.com.

Mozilla has also experimented with user agent changes to receive service parity (for example, with Google search on Android). However, this alone would not solve web compatibility issues which also stem from Mozilla’s use of Gecko and dominant companies deviating from standards and engaging in self-preferencing. The result is a more centralised and less interoperable internet with reduced competition, contestability and consumer control.

In many cases, services which suffer from interoperability failures are owned by Google and Apple and lead to suboptimal experiences for consumers who access these

[4] See, for example, Mozilla’s response to the CMA’s July 2021 Google Privacy Sandbox consultation, page 7 onwards https://blog.mozilla.org/netpolicy/files/2021/07/Mozillas-Response-to-the-CMA-Consultation-on-Googles-Chrome-Privacy-Sandbox-Commitments-Case-50972.pdf

services on other platforms or browser engines. To give just one example, when someone using Firefox accesses Google Meet and attempts to blur their background, they are shown the following message:



This browser doesn’t support visual effects

Meet’s visual effects use web technologies that your browser doesn’t support. Use a supported browser.

As an important clarification, and as we stated in our submission to the CMA during the consultation on Google’s voluntary commitments in the Chrome Privacy Sandbox investigation[5]:

> “SDOs are the natural place for voluntary and collaborative technology development amongst multiple stakeholders. However, neither SDOs nor anyone else should require an influential stakeholder to adopt the resulting agreed-upon final standard or deploy it and/or deprecate old technology on specific timelines. In other words, regulatory oversight is not needed in the technology development space, but enforceable voluntary measures…would be helpful in ensuring that influential market stakeholders do not distort competition by making deployment decisions

[5] https://blog.mozilla.org/netpolicy/files/2021/07/Mozillas-Response-to-the-CMA-Consultation-on-Googles-Chrome-Privacy-Sandbox-Commitments-Case-50972.pdf

> that contravene final standards and timelines agreed upon in an SDO setting"

Overall, web compatibility is an area which should be investigated in more detail by the CMA and can be targeted through the Market Investigation. The CMA Board is correct when stating in its Advisory Steer that the market investigation tool is not appropriate to influence global standards bodies on an on-going basis. However, this does not preclude all action on web compatibility and nor should it; the CMA can have an effective role in influencing the actions of Apple and Google, for example, by requiring them to account for not adopting standards based technologies and by encouraging them to engage with SDOs in the development of their browsers. This would help to prevent parties bypassing standards processes and creating de facto standards by serving as a disincentive without being binding or mandatory.

3. The effectiveness of choice screens may be limited but broader choice architecture remains critical to consumer choice and competition

Mozilla supports the CMA's proposal to address the current use of choice architecture by Apple and Google to reinforce the positions of their browsers and raise barriers to expansion for competing browsers such as Firefox. Given that the success of historic choice screen remedies has been limited, it is necessary to consider and address broader choice architecture in order to successfully remedy the issues caused by defaults and pre-installation.

The CMA's Market Study considered the impact of browser pre-installation and default operating system settings on competition. In particular, it concluded that these factors "*have a significant impact on consumer behaviour*"[6] due to behavioural mechanisms in users such as status quo bias, inertia, implicit endorsement and reference point/loss aversion.[7] This is consistent with multi-country user research conducted by Mozilla in 2022 which found that in practice many people never install an alternative browser or change their default and their likelihood in doing so can be affected by comfort levels and age.[8]

Specifically in relation to UK residents, Mozilla's research showed that they were *most confident* in their ability to find things on the internet but, by contrast, they were among the *least confident* that they had a wide choice of browsers available to them. There

[6] Mobile Ecosystems market study, final report, 10 June 2022 ("Final Report"), paragraph 5.93

[7] Appendix G, paragraphs 44 and 45

[8] Mozilla Report, *Five Walled Gardens: Why Browsers are Essential to the Internet and How Operating Systems are Holding Them Back,* September 2022 ("Five Walled Gardens Report") https://research.mozilla.org/files/2022/10/Mozilla-Five-Walled-Gardens.pdf

was also a large gap between the proportion reporting that they knew how to install a browser and actually doing so.[9]

In fact, UK respondents were the least likely to download browsers on their desktops/laptops and the second least likely to do so on mobile. They were also the least likely to know how to change default browsers and the least likely to follow this through and change their default browsers.[10]

This points to the importance of operating system providers allowing pre-installation of alternative browsers and giving consumers easy routes to exercise their choice to:
(a) download alternative browsers; and (b) to set them as defaults. However, as noted by the CMA, six step (iOS) and seven step (Android) processes to change default browsers create barriers for users: "*[t]he user journey for changing default browser on both iOS and Android devices involves a number of potentially complex steps. Additionally, the relevant option in device settings for switching defaults may not always have intuitive text labels, making it harder for users to search for them.*"[11]

Building on the work of the CMA's Behavioural Unit on deceptive patterns, Mozilla has analysed the importance of choice architecture to competition, including highlighting in our recent report the design techniques used by operating system providers to obstruct consumer choice and control.[12]

Against this background, Mozilla welcomes the consideration of potential remedies to make it more straightforward for consumers to change default browsers in device settings. Well-designed choice architecture has the potential to address some of the adverse impact on competition caused by such user interfaces which discourage switching and entrench pre-installed options. Mozilla would encourage the CMA to work with a wide range of stakeholders when considering any such remedies, not only rival browser developers but also others including academics, consumer advocates, researchers and ethical design theorists.

Ensuring that the wider choice architecture of an operating system is designed to facilitate rather than thwart consumer choice may also improve the effectiveness of other choice remedies such as choice screens. Mozilla's experience of the Android Browser Choice Screen implemented in the EU during the Spring of 2019 was that it did not change the status quo. One cause of this is likely to have been that it was

[9] Five Walled Gardens Report, tables 2 and 4

[10] Five Walled Gardens Report, tables 4 and 5

[11] Appendix G, paragraph 50

[12] Five Walled Gardens Report, part 2

considered in isolation, rather as part of the wider choice architecture of the operating system. As such, it is important that these remedies are adopted in coordination.

The design of choice screens is crucial. Browser ballots (i.e. the form of choice screens which have historically been implemented) are unlikely to overcome many of the behavioural biases mentioned above and in the CMA's Market Study. Moreover, operating system providers do not have an incentive to facilitate consumers switching away from their pre-installed, default browsers through, for example, innovation in choice screens.

As a result, for any choice screen remedy to be more effective than previous attempts there must be careful consideration given to factors such as: the design of the remedy; its timing for consumers; the level of regulatory oversight and scrutiny; participation of stakeholders; and the transparency of operating system A/B testing, research and data for stakeholders.

4. Operating system self-preferencing occurs in many forms and will be most effectively addressed through a holistic approach to remedies

There are a number of issues rightly identified by the CMA which relate to Apple and Google using their position as operating system providers to preference their own browser. We have commented on these issues and potential remedies below. Overall, we would note that while individual remedies will be capable of making a positive change, the most effective way to address the issues will be through applying various measures in conjunction with one another.

The WebKit requirement on iOS

As recognised in the Market Study, the requirement to use WebKit on iOS severely limits the ability of browser vendors to differentiate their products and offer alternative features to consumers which would otherwise be available.[13] Developers are also hampered by limited competition and choice in terms of features; they face reduced user-facing performance and capabilities, alongside less frequent bug fixes and updates.[14]

As consumers seek out privacy enhancing products (the CMA noted the ACCC's research which showed that privacy features were the most frequent reason for selecting Firefox on mobile[15]), the restriction on alternative browser engines impedes

[13] Final Report, paragraph 5.57; Appendix F: browser engines

[14] Final Report, paragraph 5.50

[15] Final Report, paragraph 5.40

the ability of independent browsers to compete across the full range of parameters, including in relation to privacy.

In considering measures to remove the restrictions on alternative browser engines on iOS, Mozilla would note that any intervention by the CMA will be most effective in remedying the adverse impacts on competition and choice for consumers when applied alongside the other measures in this response. This includes, in particular, supporting open standards and engaging in formal standards processes. Any such measures should also be accompanied by mandating access to equivalent functionality and APIs as are available to Safari and otherwise available on iOS, to ensure that consumers are able to benefit from the full range of innovation and features that other browsers offer.

Restrictions on browser APIs and functionality

The position of Apple and Google as both operating system providers and browser developers allows them to leverage market power in operating systems to the benefit of their browsers, Safari and Chrome respectively. This includes granting their browsers access to APIs and functionality which are not available to rival browsers.

Restrictions on APIs and functionality are particularly problematic in the case of iOS, where Apple withholds many of the critical WebKit APIs from rival browsers. Notable examples of these restricted APIs relate to privacy and security features, such as the Google Safe Browsing service[16] (only available to Safari on iOS) and process separation (a feature needed for stability, quality and security). Historically, Apple has also removed access to pre-existing functionality for data saving, cookie settings, multi-profiles, enterprise support and auto-detection encoding, many of which are necessary for privacy functionality.[17] Other features, such as browser extensions which allow for greater customisation, are also unavailable to browsers other than Safari. This feature is particularly valued by Firefox users and denied to them on iOS.[18]

Given that Apple has stated that browsers compete on privacy features and the Market Study also found privacy to be a dimension of quality on which browsers compete, the impact on competition of API and feature restrictions clearly serves to restrict competition between mobile browsers.[19] The CMA is therefore justified in focusing on this issue in the course of its Market Investigation.

[16] Google Safe Browsing is a service from Google that warns users when they attempt to navigate to a dangerous website or download dangerous files. Safe Browsing also notifies webmasters when their websites are compromised by malicious actors and helps them diagnose and resolve the problem.

[17] Final Report, page 172

[18] For example, around a third of Firefox users install add-ons: https://addons.mozilla.org/blog/firefoxs-most-popular-innovative-browser-extensions-of-2021/

[19] Apple's response to the Interim Report, paragraph 31; Final Report, paragraph 5.21

As acknowledged by the CMA, there may be legitimate security and privacy justifications that should be addressed in the design of any remedy. It will therefore be necessary for the CMA to continue to scrutinise carefully any security justifications put forward to object to equal access to APIs/functionality and requiring access to specific operating system functionality. It is certainly not the case that it is not possible to address certain API and functionality restrictions without compromising security or privacy. Moreover, requiring access only for those APIs/features implemented by the operating system browser would not fully encourage innovation as it would limit rival browsers to the development speed and direction of the operating system browser. By contrast, requiring access to operating system functionality which is available (even if not yet utilised by Safari or Chrome) could encourage differentiation and greater competition between browsers, benefiting consumers.

In-app browsers

The prevalence of in-app browsers was highlighted in the Market Study as a competition concern which could reinforce the position of WebKit and Blink and undermine the effectiveness of consumer browser choice.[20] On iOS, this is closely linked to the restriction of alternative browser engines since all in-app browsers must be built on WebKit. On Android, while alternative options for in-app browsers exist, the default is Android WebView, entrenching its position with web developers, ultimately leading to further web compatibility issues and undermining browser competition.

Mozilla supports the inclusion of in-app browsers in the Market Investigation and has separately highlighted this issue since the publication of the Final Report.[21] In-app browsers can be used to bypass consumer choice, such as where a consumer has specifically selected a browser other than the pre-installed operating system browser (for example, when clicking on hyperlinks). In this context issues concerning choice architecture are also relevant, underlining the interconnectedness of various remedies. In—app browsers can also be used by native apps to undermine user privacy, for example collecting data without the consumer's knowledge or consent.[22]

While the CMA's Advisory Board steer expressed support for investigating this issue further, it advised that interventions should be kept distinct from remedies relating to dedicated browser apps. Mozilla would note that there is interdependence between any

[20] Final Report, paragraphs 5.82 onwards
[21] Five Walled Gardens Report, pages 28-29
[22] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser
https://www.washingtonpost.com/technology/2022/09/13/facebook-instagram-data-privacy/

interventions for dedicated browsers and for in-app browsers, not least because a remedy to encourage choice and competition among in-app browsers will depend on there being effective choice for dedicated browsers apps.

Use of data

Apple and Google have access to a vast amount of data through their role as providers of operating systems, app store and a range of other apps, in addition to their position as browser developers. As noted in the Market Study: "*Through the operation of their app stores, Apple and Google have access to confidential information about rival apps that has the potential to give rise to competition concerns*."[23]

The CMA has already considered data separation remedies as "low cost" and previously found that Apple and Google should enforce data separation between app development and app review processes. The Market Investigation represents an opportunity to assess data advantages specifically in respect of browsers and, if appropriate, to propose remedies which allow independent browsers to compete on a level playing field (for example, keeping separate data collected as a browser developer from other products such as app stores).

***

[23] Final Report, paragraph 6.119