20 April 2022

Federal Trade Commission and Department of Justice

RESPONSE OF MOZILLA TO REQUEST FOR INFORMATION ON MERGER ENFORCEMENT

Mozilla welcomes the opportunity to respond to the Request for Information on Merger Enforcement from the Federal Trade Commission and the Antitrust Division of the U.S. Department of Justice (the "RFI").

One of the specific areas of inquiry is the way in which the guidelines should take into account the unique characteristics of digital markets. Given our area of expertise, Mozilla's filing focuses principally on challenges to competition in digital markets and the need for greater transparency into the ecosystem impact of our online data. We are encouraged to see that legislators and antitrust enforcers in many jurisdictions are exploring how to update consumer protection and competition policies to meet the challenges of today's internet, including in the context of merger enforcement. The FTC and DOJ have long played critical roles in this area and we look forward to having the opportunity to assist the agencies as they reassess their enforcement approach to digital markets.

Table of Contents

1. About Mozilla

Mozilla is a unique public benefit organization and open source community formed as a non-profit foundation in the United States. We have a strong reputation for our commitment to ensuring that privacy and security are fundamental to the internet. This is one of our guiding principles that recognises, among other things, that 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.[1] These principles, in addition to our Data Privacy Principles[2], provide the basis for the way we develop products, manage the consumer data we collect, how we select and interact with partners, and how we shape our public policy and advocacy work.

Our Public Mission & Incentives

Mozilla's story originated in 1997 with Netscape Navigator, the original consumer browser and a popular browser of the 1990s. In a historic move for competition, Netscape publicly released its new browser engine (called "Gecko") under an open source license to enable others to verify, improve, and reuse the source code in their own products. The company was later the subject of the failed acquisition strategy of a powerful digital gatekeeper, when AOL purchased it in 1999. Although Netscape did not last following its acquisition by AOL, its open source browser engine Gecko has continued to shape the internet.

The non-profit Mozilla Foundation was created in 2003 to continue work on open source browser technology and with a larger mission to preserve the open internet. Firefox v1.0 was released in 2004 using Gecko with volunteer open source code contributions from around the world, and it was one of the first major consumer facing products to be built in this way using open source methodology. Today localization developers continue to make Firefox available in local languages and with local customizations for their communities to access the internet. Other developers have forked the Firefox codebase and used the Gecko browser engine to create new browsers with different features. The most well known example is Tor, an anonymity browser frequently used by journalists and human rights activists. While it has officially been blocked in Russia,[3] reliance on Tor has increased recently as a means to gain access to the open internet.[4]

[1] Mozilla's 10 Principles, https://www.mozilla.org/about/manifesto/
[2] Mozilla's Data Privacy Principles, https://www.mozilla.org/en-US/privacy/principles/
[3] https://ooni.org/post/2021-russia-blocks-tor/
[4] https://www.wsj.com/articles/russia-rolls-down-internet-iron-curtain-but-gaps-remain-11647087321

In 2005, the Mozilla Foundation created a wholly-owned taxable subsidiary, the Mozilla Corporation, to serve its public mission through open source technology and product development of Firefox. In addition to remaining the sole shareholder of the Corporation, the Foundation advocates for better privacy, trustworthy AI, and digital rights and runs philanthropic programs in support of a more inclusive internet. These programs currently include fellowships and awards that invest in community leaders who are developing technology, policy, education and norms that will ultimately protect and empower people online.

Building the Internet through Open Source Development

Mozilla has spent years building the internet as an open and interoperable platform, especially through our work with Firefox and Gecko. Privacy and security have been fundamental to this work. Mozilla has influenced major companies to adopt better privacy practices such as browser anti-tracking measures and directly provided consumers with tools to improve their digital literacy and better understand third party data collection. We have also sponsored projects to break down barriers for developers. For example, Mozilla previously created an open source mobile operating system (Firefox OS) and app store premised on HTML5 "web-apps" interoperable with any device rather than the "native app" single device approach. Today Mozilla sponsors crowdsourcing projects for location and speech data for developers to access high quality and free data sets to make products for their local communities.

The incentive for Mozilla's work has always been to level the playing field so that competition can thrive and people can shape their own online experiences.[5] Although today's large platforms have contributed to many successful innovations that have improved the internet, they should not be "gatekeepers" that reduce it into walled gardens. The internet should be the ultimate universal platform that can grow and thrive with new independent technologies developed by people and companies around the world. This is Mozilla's North Star and we believe effective competition regulation and enforcement is necessary to support this goal.

Beyond browsers, Mozilla is a home for talented engineers that make the internet more secure, fast, private, and functional in multiple ways. We continue to play a key role in browsers, standards, and open source community initiatives. For example, we have made online commerce and navigation safe through protocols and initiatives like TLS 1.3 and Let's Encrypt.[6] We have created foundational compilers and programming

[5] See Mozilla Principle 5.

[6] Mozilla co-founded the Let's Encrypt project to provide free digital certificates that enable site owners to adopt HTTPS encryption. This promotes security and privacy for all internet users. See https://en.wikipedia.org/wiki/Let%27s_Encrypt

languages like Rust and Web Assembly which are now coordinated by new open source communities for emerging industry applications. We have contributed significantly at global standards bodies to the future of the internet through voice and speech recognition, mixed reality experiences, and royalty free video and audio codecs that make streaming better and more affordable. Mozilla does this despite its relatively small size—fewer than 1,000 employees worldwide—a fraction of the giant technology companies competing in these spaces.

2. The Challenge of Centralization Online

The internet as a driver for innovation depends on market entry and growth. Increased centralization of data and networks challenges the role of the internet as a healthy marketplace that protects the principles of openness and decentralization, and empowers people to choose their own online experience.

Regulators and enforcers must tackle structural problems that tilt the balance against independent companies and consumer empowerment. The structural problems are the result of the walled gardens and vertically-integrated technology stacks that have come to define digital markets in recent years. Most of the harms that have led to greater governmental scrutiny in numerous jurisdictions can be traced back to a handful of very large companies establishing themselves as gatekeepers through mergers and acquisition strategies, among other things.

Continuing this trend, 2021 was a record breaking year for mergers and acquisitions, with the technology sector accounting for the highest number of mergers and acquisitions globally (measured both by volume and value) and software deals representing half of these technology transactions.[7] Such transactions are increasingly likely to be scrutinized by the FTC and DOJ in the context of merger control. The next section discusses non-horizontal dynamics in relation to technologies more generally. However, given the importance of browsers as a ubiquitous consumer-facing technology, we believe it is important to understand the role of browsers and the functioning of competition in both browsers and browser engines when updating the merger guidelines to reflect the current realities in digital markets and to ensure that competition and consumer choice flourish in these markets. We have therefore set out further detail on this topic in the Annex to this submission.

[7] https://www.refinitiv.com/perspectives/market-insights/dealmakers-ring-out-2021-as-the-year-of-ma/

Non-Horizontal Dynamics

Question 12g of the RFI relates to non-horizontal mergers. This is a particularly acute issue in digital markets; recent years have seen a large number of acquisitions by large platforms of firms in adjacent markets, building an ecosystem of products and services which are complementary to their core offering. For example, the FTC's 2021 study into acquisitions by Alphabet Inc., Amazon.com, Inc., Apple Inc., Facebook, Inc., and Microsoft Corp. between 2010 and 2019 looked at more than 600 transactions valued at over $1 million.[8] Only a small number of these transactions were reviewed by competition authorities, none were blocked and very few were subject to any conditions when cleared by the agencies. Regulators and enforcers in many jurisdictions have subsequently sought to reassess how such acquisitions should be analyzed in the context of wider digital market regulation. The analytical framework is an important element of this reassessment, particularly as vertical mergers can be part of a wider industry trend.[9] However, the dynamic nature of digital markets means that they often do not lend themselves to bright line rules or neat distinctions of horizontal and vertical assessments.

One of the key elements behind the success of the digital economy is the ability of new technologies to build on top of previous ones (this is sometimes known as a "stack"). However, competition issues can arise where software or services with substantial market presence are technically interconnected with other software or services operated by the same business. A vertically integrated company may engineer compatibility to optimize the benefits of integration. Where that firm exercises significant market power, this must not lead to the ability for it to engage in harmful self-preferencing and the exclusion of competitors.

Vertical mergers that involve large user bases at one part of a stack of technologies pose a particular risk to innovation and the competitive process. The dependence on a key technology in that stack (often but not necessarily a "platform") can impede development and innovation in other layers of the stack. For example, new and superior services from smaller rival companies could be squashed by services offered by large vertically integrated companies which offer special technical treatment to one or more of their own business lines. Despite their superiority, these services from smaller rivals are

---

[8] https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-staff-presents-report-nearly-decade-unreporte-acquisitions-biggest-technology-companies. Similarly, a 2019 study commissioned by the UK government found that between 2008 and 2018 these companies had between them made over 400 acquisitions, with 250 of them made in the last five years. Furman Review (2019), Unlocking Digital Competition, paragraphs 1.107-1.111

[9] *Ex-post Evaluation of Vertical Mergers, Report for the Competition and Markets Authority* by E.CA Economics, 31 March 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069164/E.CA_Report_on_Ex-post_Evaluation_of_Vertical_Mergers_.pdf

not able to compete fairly with the self-preferenced business lines or technologies, thereby restricting competition and consumer choice.

This special treatment may confer advantages upon preferred products or services through their superior integration and such advantages can become quasi-permanent given the difficulty of or prohibition on reverse-engineering interoperability into established technology stacks. The recent House Judiciary Subcommittee report on Competition in Digital Markets referenced a number of examples where such positions had been built up through technology acquisitions.[10] Apple's treatment of Safari on iOS and Microsoft's treatment of Edge on Windows are also illustrative here, because each of these vertically-integrated browsers benefit from private application programming interfaces ("APIs" - software which allows two services to connect) and integration with their affiliated operating systems from which rival third party browsers (such as Firefox) are precluded.[11]

These issues are exacerbated when related technologies interoperate (or don't) on rival products. To continue with Apple as an example, many iOS consumers find Apple Pay a convenient form of quick payment. Unfortunately, Apple Pay is only available on Safari and cannot be used on alternative browsers like Firefox. In the same vein, iOS consumers who enjoy using voice assistants like Apple's Siri are limited to using Apple Pay, and cannot initiate payments using alternative providers like Stripe or PayPal. Further, similar to Safari's uneven relationship with other browsers, Siri has competitive advantages over all third party voice assistants on iOS because it has operating system level access that all third party voice assistants lack.

Connected to this is the issue of potential competition in section 6 of the RFI. The nature of digital technologies and markets means that presumptions based on current competitors are insufficient and instead a more flexible approach to dynamic competition must be adopted. As noted in another response to the present consultation,[12] the UK Competition and Markets Authority's (the "CMA") *Merger Assessment Guidelines*[13] may be instructive in this regard, particularly alongside a

---

[10] Majority Staff Report of the House Judiciary Antitrust Subcommittee on Antitrust, Commercial and Administrative Law, *the Investigation of Competition in Digital Markets,* pages 406 onwards list merger activity by certain platforms. https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519

[11] See, for example, the *Interim Report* of the UK CMA's Mobile Ecosystems Market Study, para 6.27 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1048746/MobileEcosystems_InterimReport.pdf

[12] Rose and Shapiro, What Next for the Horizontal Merger Guidelines?*, Antitrust Magazine,* Spring 2022 (forthcoming), available at SSRN: https://ssrn.com/abstract=4034923, page 10

[13]See Merger Assessment Guidelines, Chapter 5, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051823/MAGs_for_publication_2021_--_.pdf

recent review into the CMA's decisions on vertical mergers.[14] In addition, the merger guidelines should take into consideration the incentive for powerful platforms to acquire potential competitors as a preferable alternative to competing with them.[15] This is a practice which is relevant to digital markets in recent years and one which should be assessed in part through greater scrutiny of the rationale for a merger, having regard to the totality of the evidence.[16]

In light of the above, the merger guidelines should go further than looking more critically at the purported benefits of vertical mergers through the elimination of double marginalization. They must also take into account the significance of vertical integration in markets relating to digital technology, including in relation to the use of data.

The Role of Data

Another unique feature of the internet economy is the role played by data, including data collected from users and data generated about them. It is therefore encouraging that the RFI specifically addresses the role of data aggregation as a motive and/or effect of a merger.

Data can improve the quality of a service and the revenue that it can generate in ways that may be impossible to replicate without achieving a comparable data set. Compared to the number of users as a measure of the size of a product or service, data is potentially far more robust. When users leave the network, their data and the power that comes with it may stay behind, particularly as a component of aggregated data powering improved machine learning.

At Mozilla, we have a strong reputation for our commitment to ensuring that privacy and security are fundamental to the internet. As noted above, our Data Privacy Principles provide the basis for the way we operate in all aspects of our organization. However, this approach to data is not more widely adopted. The harms that accrue to both consumers and other competitors from vertically-integrated data sharing within group companies have become increasingly clear over the past few years.[17] Regulators and

[14] *Ex-post Evaluation of Vertical Mergers, Report for the Competition and Markets Authority* by E.CA Economics, 31 March 2022
[15] See C Caffarra, G Crawford, T Valletti, *'How tech rolls' Potential competition and 'reverse' killer acquisitions*, 11 May 2020.
[16] *Ex-post Evaluation of Vertical Mergers, Report for the Competition and Markets Authority* by E.CA Economics, 31 March 2022, section 3.2.1.1
[17] See, for example, the 2019 decision (under appeal) from the German Competition Authority finding Facebook's collection, merging and use of account data an abuse of market power and prohibiting Facebook from combining data from different accounts across services: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

enforcers must be empowered to evaluate and block mergers in the interest of consumer experience, innovation, privacy and competition.

Privacy and data protection concerns can be incorporated into the analytical framework in a number of ways. First, as referenced in question 2a of the RFI, there are non-price effects on competition which should be assessed in the context of merger review. Privacy protection can be one such non-price parameter of competition in mergers. For example, it could be considered as an element of product quality, or it could be considered as a feature of consumer choice and/or as a non-monetary price (i.e. considering personal data as a non-monetary price paid by consumers when they use free online products and services).[18] One such example is the Facebook/WhatApp merger, which was assessed by the European Commission in 2014. In that case, it was noted that a high number of German users switched from WhatsApp to Threema within 24 hours of the announcement of Facebook's acquisition, seemingly prompted by privacy concerns.[19] In addition, in non-horizontal mergers, acquisitions of data can also be assessed as part of a foreclosure theory of harm.

Secondly, it should be noted that there may be harm to data privacy which arises from the acquisition by a large or powerful firm in an unrelated market but one which gives it access to a valuable dataset. The combination of two valuable datasets could lead to a decrease in privacy protection through alignment of privacy policies or increased ability to profile customers. More critically here, such data, when shared across business units, can also be used to bolster a platform's position in the market. The effects of such actions must be taken into consideration as part of any relevant merger assessment.

To give an example in relation to browsers, it is worth asking why Google's Chrome and Microsoft's Edge continue to receive Android and Windows pre-installation respectively and why digital platforms like Apple, Facebook, and Amazon choose to build and preinstall their own browsers (no easy task), rather than distribute high quality browsers developed by others. Alongside customer convenience, the answer is data. Web browsers are powerful tools that have access to information about much of a person's activity online. Google, Microsoft, Amazon and Facebook all have advertising businesses that benefit financially from consumer data collected through the provision of a browser.

[18] E. Deutscher, '*How to measure privacy-related consumer harm in merger analysis? : a critical reassessment of the EU Commission's merger control in data-driven markets*' (2018). EUI Law Working Paper 2018/13. http://cadmus.eui.eu//handle/1814/58064
[19] Case COMP/M.7217 Facebook/Whatsapp, paragraph 174

Greater Transparency to inform Regulator Interventions

Data should also be considered from the point of view of transparency. Many of the harms we see on the internet today are in part a result of pervasive data collection and underlying privacy risk. Targeting and personalization systems generate real value for consumers. But, as we have learned from recent whistleblower disclosures, these systems also can be abused, resulting in real world harm to individuals and communities. To address this, we need solutions that would provide greater levels of transparency into the ecosystem impact of our online data. Mozilla - alongside academics, civil society, and government leaders - has called on major platforms to release data so researchers can analyze online discrimination and harms that today are hidden from the public and from regulators.[20]

We have also called for establishing a safe harbor allowing researchers, journalists, and others to access relevant datasets, free from threats of legal action. Such a safe harbor should protect research in the public interest as long as researchers handle data responsibly and adhere to professional and ethical standards. We know there is enormous value this can provide to the public. Mozilla has one of the earliest Bug Bounty[21] programs in software. We make clear that we will not threaten or bring any legal action against anyone who makes a good faith effort to comply with our vulnerability notification policy because this encourages security researchers to investigate and disclose security issues. Their research helps make the internet a safer place.

We believe that such transparency is important for effective security and competition on the internet. It is complementary to the issues being considered by the FTC and DOJ to modernize the enforcement of antitrust laws regarding mergers and relevant to the questions considered under section two of the RFI (Types and Sources of Evidence). Transparency tools can provide regulators and enforcers with an insight into how data is being used by gatekeeper platforms and/or how it is shared across verticals; this is important both for consumer protection and to ensure effective competition. For example, safe harbor access to data sets for researchers and others will lead to a better body of research and therefore better informed decisions by regulators and enforcers.

[20] https://blog.mozilla.org/en/mozilla/news/why-facebooks-claims-about-the-ad-observer-are-wrong/

[21] Bug bounty programs are deals offered by websites, organizations or software developers providing individuals recognition and/or compensation for reporting bugs, particularly those relating to security vulnerabilities.

3. Enabling Effective interoperability as a Remedy While Preserving User Control

Alongside traditional remedies, interoperability should feature as an essential tool in the competition enforcer's toolkit.[22] We believe this is an important factor that the FTC and DOJ should take into account in decision-making when allocating their resources and reaching enforcement decisions, including in the context of merger control. As Mozilla's principles state: "*The effectiveness of the internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralized participation worldwide*."

In particular, interoperability may prove to be a useful instrument to address harms arising from vertical mergers that involve one or more significant digital platforms, and should also be considered in the review of individual platform conduct where specific business actions or practices impede effective interoperability. However, enforcers should employ such tools in a way which enables effective interoperability while preserving user control. Agencies will also be seeking to balance limited resources when undertaking enforcement activities and monitoring compliance with remedies. As such, it will be necessary to learn from previous cases where remedies have failed, while also harnessing technologies which are available or may become available in the future, such as artificial intelligence and automated monitoring.[23]

Interoperability is fundamental to maintaining a balanced internet ecosystem in which consumers can fully exercise their fundamental rights and use a variety of core platform services from any operating system and any browser. Such web compatibility practices can be useful tools to address harms arising from a vertically integrated silo of technologies. Applying these principles specifically to our domain of the web and browsers, we believe that without properly targeted regulatory and enforcement intervention, there will be no change to the status quo, harming competition in browser engines and browsers, and harming innovation online (see section 4 and the Annex below for more detail on competition in browser engines and web compatibility).

---

[22] Its importance has been recognised in numerous recent reports by competition authorities and experts relating to digital markets. See, for example, the George J. Stigler Center for the Study of the Economy and the State, Market Structure and Antitrust Subcommittee Report, (Chicago: The University of Chicago Press, 2019), https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-Structure---report-as-of-15-may-2019.pdf and Digital Competition Expert Panel, *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, (London: Open Government License, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

[23] Himes et al, 2021, "Antitrust Enforcement and Big Tech: After the Remedy Is Ordered", *Stanford Computational Antitrust,* vol. 6, p.64 https://law.stanford.edu/wp-content/uploads/2021/06/himes-nieh-schnell-computational-antitrust.pdf?utm_source=pocket_mylist

Government action must strike a fair balance between, on the one hand, the rights of large platforms and powerful gatekeepers, and on the other hand, rights of end-users to choose freely and combine their preferred platforms and services. The fundamental rights of users, as well as the overall pluralism of the digital environment, are strictly dependent on the interoperability between digital products and services. Unfortunately, certain practices currently prevent the conditions required for interoperability with competitor products. This includes when such platforms:

- design, test and release features primarily for their own ancillary platform products;
- design, test and release features without going through formal standards development organizations ("SDOs") and processes; or
- design, test and release features without adhering to existing SDO specifications.

The first is a business decision to prefer its own business affiliates to competitor and third-party companies. The second and third practices are business decisions not to formally engage in voluntary multi-stakeholder public standards development.

In some cases these decisions may have valid or invalid rational business reasons whereas in others they may be unintentional. Regardless of the reason, harmful network effects can occur when undertaken by a powerful platform; features may not be available, may appear late, or may have inferior performance on rival operating systems and browsers. This creates powerful lock-in effects for consumers and increases their switching costs. In this regard, it should be underlined that even motivated consumers will be deterred from switching to alternative solutions if effective interoperability is not guaranteed. It also creates a burden on downstream companies that have to invest financial and human resources into evaluating and minimizing, if even possible, the lack of interoperability. The result is a more centralized and less interoperable internet with reduced competition, contestability, and consumer control.

In circumstances where interoperability is being considered as a potential remedy, the question arises as to what data and/or functionality must be included in order to reach a standard of effective interoperability. The answers to this question are very context-specific based on the products of the interoperating parties. The consequences of erring on either side of the balance can be significant - restricting competition and innovation in one direction, or potentially putting privacy and security at risk in the other. The case-by-case nature of competition and merger enforcement allows the specifics of each particular ecosystem to be assessed. Nevertheless, the same basic principle

should guide action in each case: enable effective interoperability while preserving user control.

4. Critical Role of Open Standards in Web Compatibility

Having considered the importance of interoperability for competition, it is necessary to discuss the role of open standards. Open internet standards are the linchpin to interoperability online and merit consideration in the context of competition regulation and enforcement, including digital market mergers and potential remedies. At a simple level, the adherence to open standards helps to overcome network effects by requiring different services to interact with each other using open, standardized formats. This allows users to switch, port their data between systems and interact with users of other systems. They also facilitate market entry and innovation. The effective functioning of open standards is crucial to many technologies consumers take for granted today, such as the web and email. As explained in the House Antitrust Subcommittee Report:

> "*Browsers abide by standards to ensure that anyone can properly use features within a website on any browser. For example, standards such as CSS and XML help ensure that a website functions the same in every browser. Web browser standards organizations include the World Wide Web Consortium (W3C), Web Hypertext Application Technology Working Group (WHATWG), and Internet Engineering Task Force (IETF). Through these organizations, stakeholders work in partnership to ensure that browser engines and web pages are interoperable*."[24]

However, as noted in section 3 above, platforms with market power can circumvent or sidestep SDOs and entrench network effects. Consumers experience website breakage, service unavailability or inconsistent implementation across browsers when key products or features are deployed in dominant browsers without following open standards and deployment commitments that would ensure interoperability. This forces users to choose between a sub-par experience or moving to the dominant browser, which is harmful to fair competition. Consequently, the role of SDOs and standards processes play a vital role in promoting interoperability and must be taken into account when exercising merger control powers in digital markets.

[24] Majority Staff Report of the House Judiciary Antitrust Subcommittee on Antitrust, Commercial and Administrative Law, *the Investigation of Competition in Digital Markets,* page 126 onwards

5. Harmful Design Practices Impede Consumer Choice

A particular area of practice we wish to draw to the attention of the FTC and DOJ is the use of harmful design practices (also known as "dark patterns"). Although consumer engagement with products and services has historically been reviewed under consumer protection laws rather than antitrust laws, this is relevant both to antitrust enforcement and also the enforcement of merger regulation, particularly in the context of question 1b of the RFI; mergers which create the ability or incentive for a firm to engage in harmful design practices should also be scrutinized through this lens. Academics,[25] journalists,[26] consumer rights groups,[27] companies,[28] and regulators[29] (including the FTC, the European Commission and the CMA) have acknowledged the harms of these design practices to consumer decision-making and control over which products to use and how to allow or limit use of personal data.

Specific forms of self-preferencing can occur when customers of one product or service are targeted with promotion of a related product by the same vendor, or when one product's user experience is optimized for compatibility with another product of the same vendor. These are common and accepted commercial practices. However, affiliated preferencing is not always benign, particularly in situations where the entity engaging in the practice enjoys a powerful or gatekeeper position in the market. In those situations, the firm can leverage its significant power and infrastructural role in the ecosystem to push consumers towards their own products in adjacent markets, in effect transforming the traditional affiliated preferencing practice into something akin to self-preferencing in the competition law context. The negative effects of such practices are essentially equivalent to preferential or discriminatory rankings – and should be prohibited.

Often, problematic affiliated preferencing manifests through marketing tactics that mislead consumers and undermine individual control of their software preferences. For

---

[25] For example, see work by researchers at Princeton available at https://webtransparency.cs.princeton.edu/dark-patterns/; Purdue, available at: https://darkpatterns.uxp2.com/; and a recent paper from the UK's CMA: https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers

[26] The Wall Street Journal, Vox, The New York Times, The Financial Times, The Verge, Gizmodo, The Atlantic, Fast Company, Ars Technica,

[27] BEUC DMA Paper, available at: https://www.beuc.eu/publications/beuc-x-2021-030_digital_markets_act_proposal.pdf; Norwegian Consumer Council, available at: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[28] ProtonMail Post on DMA, available at: https://protonmail.com/blog/dma-default-apps/; DuckDuckGo DMA Paper, available at: https://staticcdn.duckduckgo.com/press/DuckDuckGo-position-on-the-Digital-Markets-Act_March-2021.pdf

[29] For example, the CPRA defines a dark pattern explicitly and mandates that "agreement obtained through use of dark patterns does not constitute consent."), FCC, EU Commission's Impact Assessment that accompanied Commission's proposed legislation for competition reform, Digital Markets Act (DMA)

instance, device users, especially when they have downloaded a third-party application, are often bombarded with pop-ups and warning messages that urge them to switch to the firm's affiliated application on the basis of claims regarding quality, security, and privacy. Such complexity or other hassle factors are recognised to be effective barriers to prevent consumers from switching from one software to another.[30] By manufacturing concerns about the merits and risks of third-party competitors, this affiliated preferencing tactic can undermine fair competition and diminish consumers' ability to benefit from using the applications of their choice.[31]

The FTC and DOJ should also consider the possibility of firms engaging in such design practices that inhibit consumer control over their software preferences in the context of merger enforcement. This includes Dark Patterns and Manipulative Design Techniques—both concealed product design tactics used by companies to influence consumers into doing something they don't want to do or are unaware of—thereby prioritizing business objectives over true consumer control.[32]

We welcome recent efforts by the FTC to focus on how consumers' interactions with products influences competition.[33] Understanding and remedying dark patterns online that prevent users from making informed and effective choices, is a crucial aspect of a robust competition enforcement regime.

6. Conclusion

Mozilla is encouraged that the agencies have undertaken the process of reviewing the merger guidelines and are considering enhancing their enforcement in digital markets; the importance of these sectors of the economy to US consumers grows each day. The issues addressed in this paper reflect Mozilla's perspectives and recommendations on a number of key areas critical to competition and consumer choice in digital markets. They are not intended to be exhaustive and we would be happy to provide additional detail or further information if helpful. Nevertheless, we trust that this paper gives the

[30] See, UK Competition and Markets Authority, *Final Report - Online Platforms and Digital Advertising*, section 3.113, available at: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

[31] For instance, BEUC notes in its paper on the Digital Markets Act that "[e]ven where it is technically feasible for a consumer to switch a service, she/he may, for example, be bombarded with repeated and "intimidating" messages about the purported disadvantages or dangers of switching, or this may be made so time-consuming or complex that the consumer gives up. Such tactics can be just as effective as technical barriers". *Position paper of BEUC on DMA,* 1.4.2021, pp. 7-8.

[32] For more information, see: https://www.darkpatterns.org/

[33] FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap

FTC and DOJ a sense of Mozilla's role as a public benefit organization with the aim of stewarding a decentralized, open and interoperable internet that is accessible to everyone and benefits society in general.

ANNEX

The Importance of Browser Engines and Impact of Restrictive Product Policies

Browsers help a user visit sites and services they want to use and protect them while they are there, but they are more than a means to an end; instead, they represent the individual person using them. There are important differences between browser use on desktops and mobiles, not least the fact that 84% of the world is expected to access the internet via their smartphone by 2025.[34] However, the mobile device platform is often the opposite of the open web, with the operating system, app store, individual applications, and affiliated browser all controlled by the same company. Independent browsers must therefore work extremely hard to acquire and retain each customer who has to make an active choice to use this service over the pre-installed platform browser option; functionality, navigation efficiency, privacy, security and customization are all important.

A “browser engine” is the core software component of a web browser; it transforms the myriad content hosted on millions of web servers into a standard visual representation that people can interact with using their browser. While in 2011 there were five main browser engines[35], in 2022 there are only three (*Gecko* - developed by Mozilla, *Webkit* - developed by Apple using KHTML and *Blink/Chromium* - developed by Google).

This matters because browser engine diversity is qualitatively different from browser product variety. For instance, there is a limit to what browser products can substantively do beyond the underlying browser engines offered by Google and Apple. On Apple’s iOS operating system, all browsers are similar because Apple requires the use of WebKit. On all other platforms, the majority of browsers are similar because they all use Google's Blink/Chromium. This gives enormous power to Google and Apple to determine the capabilities of browsers and the web. Mozilla plays a key role to influence Apple and Google both through internet standards and browser features, made possible because Mozilla is independent and can innovate and implement changes into its Gecko browser without restriction.

However, maintaining a browser engine is a major cost and much resource is spent on dealing with issues that stem from lack of interoperability and self-preferencing of browsers. This resource could otherwise be spent on innovation. For example, Apple requires its browser engine to be used in any browser product listed in its app stores,

[34] GSMA: The Mobile Economy 2022, https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

[35] Trident - developed by Microsoft, Gecko - developed by Mozilla, Presto - developed by Opera, KHTML - developed by the KDE community and Webkit - developed by Apple using KHTML

entailing significant resources and preventing or delaying market entry. Until late 2021, Microsoft also imposed a similar restriction. Before this recent change, Mozilla had no listing in the Microsoft App Store on its Windows operating system because development on Microsoft's browser engine (which is currently Google's Blink/Chromium) is impractical when the value of Firefox is in its unique Gecko browser engine. This situation persisted for a number of years during which time the download and use of Firefox was impeded on Windows because it was not considered a "verified app" by Microsoft.[36]

Mozilla encountered this issue when the Apple App Store was opened to third parties in 2013, initially resulting in significant resources devoted to developing an additional version of Firefox for Apple's Webkit browser engine and delaying the availability of Firefox by a number of years. These restrictions impact the functionality of independent browsers - limiting the features, security and other developments. It has also hampered choice and innovation for consumers; iOS browser consumers only get what Apple offers, without the viewpoints and innovations of other providers. For example, although Mozilla was the first major browser developer to implement tracking protection, Firefox users on iOS could not receive this for many years. A non-privacy example is that Mozilla was unable to offer innovations in Web Real-Time Communication (which relate to video conferencing)[37] to Firefox users on iOS. Other applications such as email and productivity apps are also limited by iOS browser engine and API restrictions, and they may also be in "but for" situations where, but for Apple's restrictions,[38] consumers may have experienced more private, secure, or innovative experiences on iOS.

Accordingly, Mozilla has not committed resources to contribute to the WebKit project. Apple has not historically accepted contributions to WebKit around browser privacy and security and has not granted requests from multiple browser developers to open up closed APIs.[39]

Putting these factors into context, analysis from various competition authorities[40] examine the importance of browser engines in the web ecosystem and the indirect

---

[36] https://support.mozilla.org/en-US/kb/windows-10-warns-me-use-microsoft-verified-app

[37] Web Real-Time Communication is a technology that enables Web applications and sites to capture and optionally stream audio and/or video media, as well as to exchange arbitrary data between browsers without requiring an intermediary. The set of standards that comprise WebRTC makes it possible to share data and perform teleconferencing peer-to-peer, without requiring that the user install plug-ins or any other third-party software.

[38] These include Apple's policy against third party browser engines, running native code, running process separation, running in the background, accessing networking elements, etc.

[39] See the UK CMA's Mobile Ecosystems Market Study, paragraphs 5.123 onwards https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1048746/MobileEcosystems_InterimReport.pdf

[40] Such as the UK CMA's Mobile Ecosystems Market Study

network effects that incentivize developers to build their websites to ensure compatibility with engines that have the greatest number of users. This impacts the ability of smaller players (both browsers as well as service providers) to compete effectively in the market due to web compatibility concerns. These concerns are further exacerbated by operating system level restrictions on browser engines that create significant barriers for browser developers and prevent consumers from accessing and using a variety of browsers to fit their needs. Given the centrality of browsers to the web and many of the products and services offered in digital markets, these are important market dynamics in the context of merger regulation - as well as competition enforcement and regulation more widely.