Digital Markets Act (DMA)

July 2021 position paper on the European Commission's legislative proposal for an EU Digital Markets Act

Raegan MacDonald
Owen Bennett
Udbhav Tiwari

At Mozilla, we're a global community of technologists, thinkers, and builders working together to keep the Internet alive and accessible, so people worldwide can be informed contributors and creators of the Web. We believe this act of human collaboration across an open platform is essential to individual growth and our collective future.

Our mission is to ensure the internet is a global public resource, open and accessible to all. An Internet that truly puts people first, where individuals can shape their own experience and are empowered, safe and independent.

About Mozilla

Mozilla has long promoted a decentralised, open, and interoperable internet.

Our story started 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 freely reuse its source code in their own products. Although Netscape did not last after its acquisition by AOL, the stewards of Gecko created the nonprofit Mozilla Foundation with a mission to preserve the open internet and to continue working on open source browser technology. A wholly-owned taxable subsidiary, the Mozilla Corporation, was later created to serve the Foundation's public mission through open source technology and product development, including Firefox.

Today hundreds of millions of people worldwide choose Firefox for a more private, secure and customisable online experience. Localisation developers continue to make Firefox available in local languages and with local customisations for their communities to access the internet. Others have forked the Firefox codebase and used the Gecko browser engine

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

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.

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, called the Manifesto, in addition to our Data Privacy Principles[2], provide the basis for the way we develop products, manage the user data we collect, how we select and interact with partners, and how we shape our public policy and advocacy work.

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. We have made online commerce and navigation safer through protocols and initiatives like TLS 1.3 and Let's Encrypt.[3] We have created foundational compilers and programming 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 small size—less than 1,000 employees worldwide—a fraction of the workforces of the giant technology companies competing in these spaces.

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.

[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] 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.

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

The incentive for our work has always been to level the playing field so that competition can thrive and people can shape their own online experiences.[4] Although today's dominant platforms have contributed to many successful innovations to improve 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 it is necessary for effective competition regulation.

The DMA Offers Promising Legislation

Mozilla welcomes the European Commission's legislative proposal for the Digital Markets Act. A vibrant and open internet depends on fair conditions, open standards, and opportunities for a diversity of market participants. We believe that with targeted improvements and effective enforcement the DMA could help restore the internet to be the universal platform where any company can advertise itself and offer its services, any developer can write code and collaborate with others to create new technologies on a fair playing field, and any consumer can navigate information, use critical online services, connect with others, find entertainment, and improve their livelihood.

We are conscious that there are several aspects of the draft DMA that ought to be clarified, and there are a number of important market dynamics that, while warranting intervention, are overlooked by the draft law. This position paper provides recommendations on how the draft law can be improved, recommendations that channel our vision for a competitive and diverse internet ecosystem. That vision can be summed up in four key objectives:

- Protect & expand the standards-based open web;
- Empower consumers to use software they want;
- Create the right incentives today for digital competition;
- Enable the horizon of independent innovation.

[4] See Mozilla Principle 5.

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

Recommended Improvements to the DMA

1. Consumer Control

The DMA should prohibit Gatekeepers from engaging in design practices that inhibit consumer control over their software preferences. This includes prohibiting 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 prioritising business objectives over true consumer control.[5] The wide variety of techniques and practices that fall within the category of Dark Patterns generally share some common features. They are:

- Asymmetric (meaning that "they impose unequal weights or burdens on the available choices presented to the user in the interface");
- Concealed;
- Deceptive (in that they "induce false beliefs either through affirmative misstatements, misleading statements, or merely omissions");
- They hide information from users; and,
- Restrict their set of choices.[6]

These practices were first identified a decade ago by Harry Brignull, a UK-based user experience designer with a PhD in cognitive science. Since then, multiple academics,[7]

[5] For more information, see: https://www.darkpatterns.org/
[6] This taxonomy of dark pattern characteristics is drawn from Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, by Arunesh Mathur (Princeton University) and Others, available at https://webtransparency.cs.princeton.edu/dark-patterns/
[7] For example, see work by researchers at Princeton available at https://webtransparency.cs.princeton.edu/dark-patterns/ , and Purdue, available at: https://darkpatterns.uxp2.com/

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

journalists,[8] consumer rights groups,[9] and regulators[10] (including the European Commission) have acknowledged the harms of these design practices to consumers, most of whom are unable to detect them. The Impact Assessment accompanying the DMA even elaborated on Gatekeepers' use of these design practices to engage in self-preferencing:

> "Gatekeepers use various techniques (e.g. design of choices, misdirection, social pressure, sneaking items into the user's shopping basket, and inciting a sense of urgency or scarcity) that 'nudge' users into certain decisions. A recent search on 11,000 shopping websites identified 818 patterns of practices used to incite users doing things they have not intended to do."[11]

The Commission relied on a 2020 publication by the European Commission's own Joint Research Center, examining the impact of technology on political information and decision making. The report notes the pervasiveness of dark patterns and two persuasive design techniques called *framing* and *commercial nudging*—used to nudge users towards a choice by presenting the alternative as risky. The JRC notes "[t]he attention economy is characterised by a profound asymmetry between the power of platforms and the limited power of users" and recommends that European data and consumer protection regimes "can be used to supplement and complement each other." A recent study by the European Parliament also indicates that "[e]xamples of dark patterns abound in privacy and security", such as the "persistent [...] asking for users to confirm personal information that they will eventually relent to prevent further nagging, and not because they want to share this information".[12]

---

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

[9] BEUC DMA Paper, available at: https://www.beuc.eu/publications/beuc-x-2021-030_digital_markets_act_proposal.pdf; the Federation of German Consumer Organisations ("VZBV") DMA paper, available at https://www.vzbv.de/publikationen/wahlfreiheit-fuer-nutzer-digitalen-maerkten-sicherstellen; Norwegian Consumer Council, available at: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[10] See California Privacy Rights Act of 2020, section 1798.140. Available at https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/#S140. See also: UK Competition and Markets Authority, 'Final Report - Online Platforms and Digital Advertising', section 4.198. Available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

[11] European Commission, Digital Markets Act Impact assessment Part 1, §80.

[12] Study of the European Parliament *Online Platforms: Economic and Societal effects*, published on 10 March 2021, page 54.

Frictions created by Gatekeepers through these practices inhibit switching and suppress contestable digital markets. This is why the DMA should ban such existing practices and not leave them solely to privacy or consumer protection law - the competition implications go well beyond the mandate of exclusively privacy or consumer protection agencies. At the same time, the DMA should remain as broad as possible to anticipate any further developments that would have the same economic effects and impact on consumers' choices. Recent antitrust investigations both at the EU[13] and national levels[14] have shed light on the implications of privacy and data protection breaches on fair competition in the digital sector. A comprehensive and forward-looking outlook on the regulation of competition and data protection is hence necessary to ensure fair and contestable digital markets.

In relation to the intersections between data protection and market contestability more broadly, the DMA should also set more ambitious requirements with regard to portability (Article 6. 1 (h)), with a view to ensuring that consumers can easily switch from one service provider to another. In fact, at this stage Article 6.1 (h) appears to focus only on the access by third party business users to data generated by users on the Gatekeeper's platform. The underlying rationale of that provision appears to be that Gatekeepers shall provide third party business users with effective data porting possibilities for data generated on their core platform services, subject to Regulation (EU) 2016/679 ("GDPR") consent requirements as applicable. However, the DMA must also prohibit barriers to portability in the context of consumers-to-Gatekeeper relationships – and in particular ensure that portability barriers do not discourage consumers from switching from one service provider to another. This would be aligned with and strengthen the right to switch set out in Article 6.1 (e). Moreover, it would also further complement the right to portability established in Article 20 of the GDPR.

Ultimately, the prohibition on Dark Patterns and other forms of Manipulative Design Techniques should not be limited to the ex-ante obligations in Article 6 of the DMA. While more robust prohibitions on, inter alia, self-preferencing and interoperability are necessary (see below), the DMA should also be amended in order to target the use of those

[13] In particular, the recently opened investigation by the Commission into possible anticompetitive conduct of Facebook, which was launched in parallel to that of the UK CMA. (See press release of 4 June 2021 on the Commission's website, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2848

[14] For instance, the decision of 6 February 2019 of the German Federal Cartel Office concerning Facebook abuse of dominance, a summary of which is available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html . The Court of Justice of the EU is expected to provide its guidance on this decision in the pending preliminary ruling proceedings in case C-252/21, Facebook and Others.

misleading design techniques as part of the anti-circumvention prohibition set out in Article 11. This Article should include an overall provision prohibiting any form of behavioural techniques and interface design that would undermine the effectiveness of Articles 5 and 6.

The DMA should enhance consumer control in the following ways:

- A new corresponding recital should be added to the DMA, that outlines a non-exhaustive set of examples of these user-experience frictions that are likely to be incompatible with the rules.
- The scope of article 6.1 (e) should be expanded such that it applies to operational, commercial restrictions and frictions as well as technical barriers, or of "any other nature". Lawmakers could also consider adding a new corresponding general recital that clarifies what these practices typically manifest, as e.g. 'dark patterns' and what the general features of those misleading design techniques are (i.e., asymmetric, covert, deceptive, and hide information from and restrict the choice of users).
- Article 6.1 (h) should be expanded in such a way as to also prohibit barriers to portability in the context of consumers-to-Gatekeeper relationships – in particular, to ensure that portability barriers do not discourage consumers from switching from one service provider to another.
- In order to ensure effective compliance with Articles 5 and 6, the anti-circumvention provision (Article 11) should require Gatekeepers not to implement any Dark Patterns and other forms of Manipulative Design Techniques that would ultimately undermine the effectiveness of the obligations set out in Articles 5 and 6.

2. Interoperability & Core Platform Services

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. In this context, the DMA must strike a fair balance between, on the one hand, the rights of Gatekeepers, and, on the other hand,

the rights of end-users to freely choose and combine their preferred core platform services. The users' freedom of choice is protected by Articles 38 of the Charter of Fundamental rights of the EU and 169 of the Treaty on Functioning of the EU ("TFEU"). The fundamental rights of users, as well as the overall pluralism of the digital environment, are strictly dependent on the interoperability between core platform services.[15]

Unfortunately, certain practices currently prevent the conditions required for interoperability with competitor products. This includes when Gatekeepers:

- 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. Sometimes 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 performed by a Gatekeeper of core platform services; 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, one must underline 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 minimising, if even possible, the lack of interoperability. The result is a more centralised and less interoperable internet with reduced competition, contestability, and consumer control.

Article 6.1 (f) of the Commission's DMA proposal imposes an obligation on Gatekeepers to "allow . . . effective use of third party software applications" and "allow . . . access to and

[15] See Amnesty International's DMA Paper, p. 17, available at: https://www.amnesty.eu/wp-content/uploads/2021/04/Amnesty-International-Position-Paper-Digital-Services-Act-Package_March2021_Updated.pdf. See also, Access Now Europe's DMA paper, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers/F2256643_en.

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

interoperability with [Gatekeeper applications]." However, mere access is insufficient. To be effective, these obligations should be expanded to impose an affirmative duty on Gatekeepers to create the conditions necessary for effective third-party interoperability.

This includes:

- Designing, testing and releasing core platform services on a nondiscriminatory basis and intentionally to achieve interoperability;
- Addressing and testing relevant interoperability concerns on a timely basis;
- Committing to SDOs and complying with formal specifications; and
- Offering timely and relevant public critical interfaces, APIs, and documentation for product interoperability.

Moreover, the duty to ensure access to interoperability should not be limited to ancillary services provided by business users and providers. These obligations must apply also in the core platform services market, in order to ensure that consumers are granted effective freedom of choice. The requirements of Article 6(1)(f) must therefore be extended to cover not only ancillary services but also cover core services. [16]

As stated in Mozilla's Manifesto: "The effectiveness of the internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralized participation worldwide." We believe that competition legislation should encourage Gatekeeping platforms to share the responsibility of maintaining the open internet.

The DMA should ensure effective interoperability in the following ways:

- Article 6.1 (f) should be expanded to empower regulators to investigate and restrain Gatekeepers from behaviour that explicitly goes against the spirit of interoperability. The interoperability obligation in Article 6.1 (f) should be extended to cover not only ancillary services but the relationship between core services.

[16] This view is also supported by OpenForum Europe's DMA Paper, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers/F2256885_en

- Any binding mandates under this provision should have to meet a very high bar of impact and necessity, with special consideration that they do not inhibit privacy or security objectives both in standards development and adoption or in products themselves.

3. Innovation not Discrimination

We welcome the underlying purpose of the DMA, which is to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. However, in order for this framework to have a meaningful impact on the market of today (and tomorrow), it must more robustly address the harms associated with affiliated preferencing, particularly at the operating system level. Our core recommendation in this section is to broaden the prohibition on self-preferencing in ranking systems to a general prohibition.

As noted above, self-preferencing may in fact occur in the form of preferred rankings, which is mentioned in Article 6.1 (d), or in interoperability barriers – of commercial, technical or whatever other nature – that should be addressed by expanding the scope of the prohibition set out in Article 6. 1 (e). At the same time, however, self-preferencing can entail a much broader variety of practices that are intended to favor affiliated undertakings.

That extension of the scope of Article 6(1)(d) to a general prohibition would be consistent with Recital 49 of the DMA, which provides that "[t]*o ensure that this obligation* [i.e., the prohibition on self-preferencing] *is effective and cannot be circumvented it should also apply to any measure that may have an equivalent effect to the differentiated or preferential treatment in ranking*". In fact, the underlying *rationale* of the prohibition set out in Article 6. 1 (d) is to limit "[g]*atekeepers' power stemming from ability and incentive to engage in self-preferencing due to the vertical integration*", in order to avoid that competition on merits in adjacent markets is limited, and ensure "*better informed and more impartial choice for consumers*".[17] As noted below, there are several ways in which Gatekeepers can effectively put forward measures that have an equivalent restrictive effect on the contestability of the relevant market to the differentiated or preferential treatment in ranking – which is currently addressed by Article 6(1)(d).

[17] Section 2 of Annex 3 to the Impact assessment (part 2, p. 54, "*Table of impacts per considered obligation*").

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

In particular, 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 optimised 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 Gatekeeper status in the market. In those situations, the Gatekeeper 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 as such also prohibited.

Often, problematic affiliated preferencing manifests through marketing tactics that mislead consumers and undermine individual control of their software preferences. For 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 Gatekeeper's proprietary 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.[18] 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.[19]

The DMA should foster innovation by more broadly targeting discrimination in the following ways:

- Article 6.1 (d) prohibition on self-preferencing in ranking systems should be expanded to a more general prohibition, so as to address any problematic affiliated preferencing by Gatekeepers that make it more difficult for end-users to make effective use of third-party software.

[18] 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

[19] For instance, BEUC notes in its DMA position paper 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.

- Article 6.1 (c) should be amended such that it ensures that any prohibitions on third-party applications' access to a Gatekeeper's operating system are based on the fair and consistent implementation of the operating system's terms and conditions. This amendment should clarify that operating system's terms and conditions for applications must be:
    - Objective, and apply equally to the Gatekeeper's proprietary applications;
    - Not include technical specifications that privilege the Gatekeepers' applications over third-party ones.

- A new recital should be crafted outlining that the 'effective' use of third-party software applications in article 6.1 (c) requires that third-party applications be entitled to access the same components and APIs that the Gatekeeper grants to its own applications.

4. Meaningful Privacy

It is unsurprising and indeed welcomed that the DMA seeks to address market-distorting use of data by Gatekeepers. By placing a clear prohibition on the sharing of data by a Gatekeeper between its product verticals, the DMA reduces the incentive for excessive data collection and helps ensure that smaller companies active in a given market can compete on the merits of the service they provide, and not on the basis of how much personal data they have collected or have access too.

Despite the obvious promise of the policy approach, many stakeholders believe this provision contains a fatal flaw, in that it allows the combination of personal data between Gatekeeper verticals if data subject consent is secured in accordance with the GDPR, something which can be easily done through the Dark Patterns and Manipulative Design Techniques referred to earlier in this paper. That this provision is considered a flaw and a loophole speaks volumes regarding the state of GDPR implementation and enforcement today. At Mozilla, we believe individuals should always control how their personal data is used and by whom, and for that reason we do not object to the proviso that data subjects can consent to have their personal data combined between vertical services. However, we

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

urge the European Commission to redouble its efforts to ensure this proviso serves its intended purpose, and does not function as an unfortunate 'loophole'.

The DMA can advance meaningful privacy in the following ways:

- Maintain the prohibition on data sharing between Gatekeeper verticals in article 5 (a).
- Ensure appropriate implementation and enforcement of the GDPR, such that data subject consent for data sharing between verticals is meaningful and in compliance with the law.

5. Effective Oversight & Enforcement

As with any law, the DMA's provisions will be ineffective without meaningful oversight and enforcement by regulatory agencies. Moreover, the stated intention of the DMA is to provide a nimble set of market guardrails that, by being *ex ante* in nature and free of the procedural complexities of antitrust law, can limit the risks of market tipping. In that context, we recommend specific measures to boost these two features of the DMA.

First, the European Commission's legislative proposal seeks to centralise oversight and enforcement duties within the EU executive through the creation of a new function within DG CNECT. While EU-level centralisation has its merits, we believe that, as in the draft DSA, oversight should take a more polycentric character, specifically by harnessing the capacities of existing national-level regulatory authorities. In particular, the DMA should provide for the establishment of a network of national authorities and the Commission similar to the European Competition Network.

We furthermore encourage EU lawmakers to explore ways in which NRAs can play both a "passive" and "active" role in their role as enforcement and oversight bodies, which could include the following:

- **NRAs should serve as a contact point for harmed businesses and end-users.** The DMA does not provide any mechanisms for reporting violations, and does not clarify which authorities would be competent to receive/review complaints. In that context, we believe that NRAs would be best-placed to act as a first contact point

for harmed users. This holds particularly true for small business-users and consumers, who could consider the barriers to contact the Commission and report a violation (e.g. language, costs, geographical distance, etc.) as a deterrent.

- **NRAs should be empowered to "actively" monitor their national markets**, as they may be better placed than the Commission to spot unfair and harmful practices that manifest at the national level. As noted by BEREC, the DMA could for instance provide a similar mechanism to that envisaged by the EU telecom rules,[20] which require NRAs to (systematically and periodically) collect information from market players, undertake monitoring activities, and report to the Commission.

Second, unlike in the antitrust domain, regulators overseeing and enforcing the DMA do not need to undertake complex market definition exercises or engage in rigorous economic analyses to identify whether and to what extent abuses of dominance have taken place. This is one of the DMA's key strengths and must be maintained. For that reason, we urge lawmakers to place considerations of speed and balance at the fore when considering new provisions and requests for additional procedural steps/Gatekeeper protections during the mark-up stage.

Finally, as has been noted by groups such as BEUC, the draft DMA already includes considerable procedural protections for Gatekeepers that may conflict with the spirit of the regulation, that is, to ensure speedy and effective action to prevent market tipping. Moreover, despite the web of procedural safeguards that exist in the DMA today, we note that there is little space for challenger companies or consumers to raise complaints or contribute to investigations and remedial actions. In remedying the aforementioned harms associated with affiliate preferencing and choice frictions, affected stakeholders - not just Gatekeepers - need to have a seat at the table. Ultimately then, rather than introducing new procedural safeguards for Gatekeepers, we encourage lawmakers to consider measures to promote the voice of challenger companies and consumers in oversight and enforcement.

The DMA's oversight and enforcement should be enhanced in the following ways:

[20] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36-214); the Open Internet Regulation (previously referred to); and Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union (OJ L 172, 30.6.2012, p. 10-35).

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

- NRAs should be empowered to receive complaints, and to "actively" monitor their national markets for DMA breaches, in particular:
    - The DMA could provide that NRAs are tasked with receiving and *prima facie* screening complaints. Upon request from the Commission, they should transfer to the Commission complaints that are likely to have an EU interest. Upon specific request of the Commission, the NRA may then be empowered to carry out specific investigative and enforcement actions, which should have EU-wide effects *vis-à-vis* other NRAs.
    - The Preamble to the DMA should include wording analogous to Recital 15 of Regulation 1/2003,[21] as a complement to the reference to cooperation currently set out in Article 1(7) of the DMA. This wording should strongly emphasise the need to ensure a polycentric and multi-level enforcement of the DMA, with an "active" involvement of the NRAs and the competent national jurisdictions at all levels of the investigation and enforcement of the DMA.

- Lawmakers should be mindful of the impact of Gatekeeper-directed procedural steps on the DMA's speed and utility. Should additional procedural measures be incorporated, they should address the underrepresentation in oversight and enforcement of challenger companies and consumers.

Conclusion

These comments outline Mozilla's perspectives and recommendations on various elements of the DMA. They are not intended to be exhaustive and we will continue to elaborate our perspectives as the EU discussions on the legislative proposal evolves.

Ultimately, we believe the DMA proposal lays the groundwork for an ambitious new standard that could enhance consumer choice and the ability of many companies to thrive,

[21] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003, p. 1-25). Recital 15 provides that "the Commission and the competition authorities of the Member States should form together a network of public authorities applying the Community competition rules in close cooperation. For that purpose it is necessary to set up arrangements for information and consultation. Further modalities for the cooperation within the network will be laid down and revised by the Commission, in close cooperation with the Member States".

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com

not just those under the umbrella of dominant platforms. The above recommendations can ensure the final legislative text realises this potential.

We look forward to working with EU lawmakers and the broader community of policy stakeholders to help ensure a final legislative text that promotes a healthy internet that puts competition and consumer choice first.

Mozilla EU Policy, Rue du Trône 51, Brussels 1050, Belgium | brussels@mozilla.com