



moz://a

**Mozilla's Vision for the
EU Mandate 2024-2029**

*Towards greater openness, privacy, fair
competition, and choice for all*

July 2024



Table of Contents

Our policy vision in a nutshell	3
Priority 1: Promoting Openness & Accountability in AI	5
Priority 2: Safeguarding Privacy & Restoring Trust Online	9
Priority 3: Increasing Fairness & Choice for Consumers	13
About Mozilla	17



Our policy vision in a nutshell

Mozilla envisions a future where the Internet is a truly global public resource that is open, accessible, and safe for all. Our commitment to this vision stems from our foundational belief that the Internet was built by people for people and that its future should not be dictated by a few powerful organizations.

When technology is developed solely for profit, it risks causing real harm to its users. True choice and control for individuals online can only be achieved through open, fair, and competitive markets that foster innovation and diversity of services and providers. However, today's internet is far from this ideal state.

Over the coming years, we must radically shift the direction of the web—and, by extension, the internet—towards greater openness, privacy, fair competition, and choice.

In recent years, the European Union has adopted milestone pieces of tech legislation that strive to achieve these goals and have set the tone for global regulatory trends. In order for laws like the Digital Services Act (DSA), the Digital Markets Act (DMA), the GDPR, and the AI Act to realise their full potential, closer collaboration is needed amongst regulators and enforcement authorities in Brussels and at member state level. For that reason, we strongly support reinforcing cooperation, shared resources, and alignment amongst data protection, competition, consumer protection, and market surveillance authorities. This need is further dictated by the ongoing complexity the latest market developments (e.g. AI) have created in enforcing tech rules.

In parallel, as the new European Commission mandate kicks in, new regulatory approaches still have a crucial role to play in realising these ambitions. Our policy vision for the next five years (2024-2029) is anchored in our [guiding principles](#) for a Healthy Internet. Having these principles in mind, we believe that the following

priorities should be the 'north star' for EU regulators and policymakers in realising the radical shift today's web needs:

Promoting Openness & Accountability in AI

- Update Europe's Open Source Strategy in order to leverage the value and benefits open approaches can bring in the AI space and to create the conditions that can fuel and foster Europe's economic growth.
- Involve civil society, researchers, academia, and smaller AI developers in the AI Act implementation to prevent big AI companies from dominating the process.
- Address cloud market concentration, ensure robust liability frameworks, and guarantee meaningful researcher access to scrutinize AI models for greater accountability and transparency.

Safeguarding Privacy & Restoring Trust Online

- Safeguard Europe's existing high privacy standards (e.g. GDPR)
- Address aggressive tracking techniques and ensure the technical expression of user choice through the use of browser-based signals is respected
- Incentivize privacy-enhancing technologies (PETs) and mandate greater transparency in the online advertising value chain to enhance accountability and data protection.

Increasing Fairness & Choice for Consumers

- Ensure robust enforcement of the DSA and DMA by empowering regulatory bodies and assessing compliance proposals for true contestability and fairness.
- Update EU consumer protection rules to address harmful design practices both at interface and system architecture levels,
- Introduce anti-circumvention clauses for effective compliance with rules, while also ensuring consumers are given meaningful choices and control over personalization features.

Priority 1: Promoting Openness & Accountability in AI

In its early days, the open architecture of the internet created conditions for broad access and participation. However, these values have eroded over time, with open-source software increasingly enveloped by proprietary systems. As the internet evolves to encompass new technologies— most notably AI—the principles of openness and the development and uptake of open standards must remain at the core to ensure it continues to serve the public good.

Openness is a spectrum, not a binary state. It addresses challenges stemming from walled gardens, gatekeeper behaviors, and closed systems that lack accountability.

While some fear that regulation could hinder open values, the reality is that smart regulation is essential for fostering online innovation that serves people's interests. For example, the General Data Protection Regulation (GDPR) has shown how privacy protections can further open values of access, empowerment, and opportunity. The Digital Markets Act (DMA) serves as an exemplary framework, illustrating how regulation can ensure fair competition in the digital age. The Digital Services Act (DSA) sets the framework for creating a safer, more responsible, and trustworthy online environment by imposing a set of obligations, increasing transparency on online providers, and tackling specific risks stemming from the largest online platforms. Similarly, fostering innovation in the AI space requires that core building blocks of technology remain broadly accessible.

Promoting open approaches in AI has the potential to truly create technology that benefits society broadly. Openness and transparency are key to ensuring AI safety and accountability. Competition driven by open approaches can spur research and development, create more affordable and safer products, and invigorate investment and job creation.

For people to truly benefit from the development of AI, we should treat AI as a public good to ensure that its advantages are widely shared. This will also function

as a counterweight (and not a replacement) to the development of corporate AI that predominantly serves private interests. To get there, we need open and public AI infrastructure — such as compute, data, tools, and talent — that everyone can use to build and test AI systems. It needs to run on a different economic engine from the one powering Big Tech so that it can be used for public interest projects without needing to rely on the same logic of commercial surveillance. And critical to creating a truly public AI is supporting regulations that protect people’s data and promote competition, as well as building it on collaborative platforms in an open manner, where governments, nonprofits, startups, and individuals can share data, models, and best practices.

Additionally, to build trustworthy AI, we need clear and enforceable rules. Letting big tech companies self-regulate has consistently failed. These companies often prioritise profit over public benefit, leading to harms like discrimination, scams, electoral manipulation, and privacy violations. Introducing regulations and guardrails, such as those included in the AI Act, can steer progress in the right direction. Now, it is high time to robustly operationalise and enforce those rules — and to make sure voices from civil society and the open source community are heard in the process.

Learning from the past, we must ensure that a handful of big players do not dominate the AI market, creating a playing field that primarily benefits themselves. Critical resources for competitive AI products and research should not be concentrated in the hands of a few. Computing resources, essential for developing cutting-edge AI models, are currently controlled by big cloud providers. To distribute AI innovation benefits evenly, we must ensure that AI research and development is not confined to these companies.

Key Recommendations

Effective AI Act implementation: EU policymakers should ensure that civil society, researchers, academia, and smaller AI developers will be involved in a structured manner during the implementation phase of the AI Act to ensure that enforcement will not be dictated and driven by big AI's profit-making mindset but rather benefit humanity and society overall. The implementation of the Act must not turn into an exercise where big AI players tailor codes of conduct, standards, and guidelines to their own capabilities.

Avoid Walled Gardens: Regulators must address concentration in the cloud market and help build shared compute capacity to support smaller players and independent researchers. At the same time, given the value data plays in training AI models, data protection and competition authorities should work closer together to alleviate privacy and competition concerns from the concentration of such data in the hands of a few companies.

Robust liability framework for AI: The inclusion of AI under the scope of the recently revised Product Liability Directive (PLD) has paused discussions around the proposed - but not yet finalized - AI Liability Directive (AILD). We ask policymakers to advance the AILD discussions in this new mandate and ensure that it effectively complements the AI Act and the PLD. Whereas the AI Act aims at ensuring that AI products and services in the EU are trustworthy and that harms are prevented and mitigated, the AILD, together with the PLD, have the potential to enable compensation where such harms (both material and non-material, such as violation of fundamental rights) still manifest.

Ensure Meaningful Researcher Access: Effective and meaningful access for researchers to scrutinize AI models will be beneficial in holding AI companies accountable. While the global trend across many tech companies is to roll back transparency, we believe it is particularly important for civil society researchers and journalists to access transparency tools to bridge the information asymmetry between these companies and society

Update Europe's Open Source Strategy: The EU has long been a supporter and promoter of leveraging the transformative, innovative, and collaborative power of open source. The most recent Open Source Software Strategy expired in 2023, and we believe it is high time for an updated Strategy that will also reflect the transformative impact open source approaches can have in AI development. Creating incentives to promote the adoption of open source, fostering interoperability and standards, and supporting open source communities, research, and development has the potential to give Europe a competitive advantage, foster economic growth, and shape a digital landscape that prioritizes innovation, security, and transparency. By embracing open source, the EU can pave the way for a more inclusive, competitive, and resilient digital future also in the AI space.

Priority 2: Safeguarding Privacy & Restoring Trust Online

In today's internet landscape, running a successful business should not come at the cost of user privacy, data protection, or fundamental rights. At Mozilla, we firmly believe that individuals' security and privacy on the internet are fundamental rights that must not be treated as optional.

Legislation can incentivize companies to adopt or transition towards ethical and responsible business practices, ultimately benefiting users and consumers.

Europe has been a trailblazer in personal data protection with the implementation of GDPR, setting a global standard that has sparked similar discussions worldwide. However, privacy issues persist, with aggressive profiling and tracking practices resulting in users feeling powerless and losing trust in online services. In the meantime, only a handful of players, in an arbitrary manner, get to decide how our personal data are processed and managed online.

People risk losing control over their personal data and core GDPR concepts and norms such as data minimization, privacy, consent, and transparency in the handling of personal data are put at risk.

Take, for example, the AI space: the rush to secure data for training AI models should not lead to a race to the bottom in terms of privacy standards. Companies harvesting the most data from people gain an edge in AI development, risking a scenario where respecting privacy becomes a competitive disadvantage. Similarly, the current online advertising ecosystem, driven by pervasive surveillance and intrusive practices, is fundamentally broken, often harming individuals and society. We envision a future where online advertising is privacy-preserving, transparent, and user-centric. Advertising should no longer be powered by ubiquitous surveillance but should instead respect users' privacy and provide them with greater control.



As a browser maker and a values-driven organisation with a clear mission, Mozilla is dedicated to representing users' interests and realizing a web defined by privacy, security, and individual autonomy. To that end, we have already taken significant steps through our products and initiatives. For example, we deploy Enhanced Tracking Protection (ETP)¹ and Total Cookie Protection (TCP)² in Firefox, which in essence, are anti-tracking measures that aim to give a basic level of technical privacy protection. We also experiment with new tools³ that can help tackle the so-called 'cookie fatigue.' At the same time, we are committed to reshaping the digital landscape for advertisers, platforms, and consumers by investing and contributing to the creation of technologies that ensure user privacy while delivering effective advertising solutions.

We believe that all browsers should protect users from cross-site tracking, and we urge the industry to move expeditiously toward this goal. Additionally, our efforts extend beyond our products. Through the Mozilla Foundation, we support projects and drive research to advance privacy standards (e.g. *Privacy Not Included). We also actively participate in industry standards bodies like W3C to promote user privacy and ensure that the shift towards more privacy-preserving advertising is happening in an open manner.

For that reason, we see a significant opportunity to improve the privacy landscape through regulatory and market-based initiatives. In the short term, we advocate for stronger enforcement of existing privacy laws like the GDPR, increased transparency in the online advertising value chain, and restrictions on targeting sensitive data points to prevent social harms. Legislative initiatives like the Digital Services Act (DSA), in conjunction with GDPR and future regulations, can mitigate

¹ Launched in 2019, ETP blocks trackers that follow users around the web without breaking site functionality, including social media trackers, cross-site tracking cookies, and fingerprints

² An advancement to ETP, TCP ensures that cookies are limited to the site users are on, preventing third-party tracking across sites. This feature effectively blocks cookies from platforms like Facebook from tracking user activity beyond their site.

³ To combat 'cookie fatigue,' we have introduced a banner blocker, in private browsing mode, that either sets an opt-out cookie or chooses the decline option on cookie prompts, reducing the annoyance of constant consent requests.



harms from pervasive tracking and introduce systemic reforms in the online advertising landscape.

In the long term, we support the transition to less intrusive forms of advertising, which pose fewer risks to privacy while still delivering value to advertisers and hosts. By working collaboratively with industry leaders on privacy-preserving advertising technologies, we aim to create a safer, more respectful digital environment. At the same time, we call on policymakers to ensure that in the new mandate, a new legislative proposal focuses on reforming the online advertising space, safeguarding existing rules on personal data protection, and offering solutions to issues like consent management, cookie fatigue, and intrusive tracking practices.

Key Recommendations

Maintain high privacy standards: Safeguarding the world's most comprehensive privacy regulation, the GDPR, is essential, particularly to develop AI responsibly while protecting people's right to privacy. Any upcoming evaluation and assessment of the GDPR should focus on improving its enforcement while maintaining the existing high standards of personal data protection.

Respect & Enforce User Choices: Leverage legislation to ensure that users' choices and preferences are respected by all actors involved (i.e., websites, online platforms, etc.). For example, currently, there is no legal obligation for online platforms or websites to respect browser-based signals that can be deployed to explicitly declare users' intention not to be tracked or have their data shared with third parties. For that reason, we call on policymakers to implement robust mechanisms through existing or new legislation to ensure that users' choices and preferences are effectively respected.

Incentivise Privacy-Enhancing Technologies (PETs): PETs have the potential to ensure data protection by design and by default and, at the same time, ensure minimal data collection. We call on policymakers to incentivise, through legislation, the uptake of such privacy-preserving technologies, particularly in

sensitive areas and in cases when digital content and digital services are provided 'free of charge' but in exchange for personal data.

Build on Platform Accountability and Transparency rules: The EU has made important steps towards a healthier advertising ecosystem, through advertising-related transparency provisions. For example, the inclusion of these provisions in the DSA is a crucial step forward towards a healthier advertising ecosystem. To complement these rules, we ask policymakers to mandate greater transparency in the online advertising value chain, including the logic of ad placements and the Real-Time Bidding mechanism

Priority 3: Increasing Fairness & Choice for Consumers

In today's rapidly evolving digital landscape, every click, swipe, and interaction significantly shapes individuals' daily lives. Harmful and deceptive design practices and aggressive personalisation increasingly limit or distort choices online. Such practices often harm users and consumers, particularly the most vulnerable, by misleading them into actions that are not in their best interest, causing financial loss, privacy breaches, security issues, and overall well-being detriments.

Mozilla is dedicated to building a healthy internet that respects fundamental rights and provides a space where individuals can genuinely exercise their choices. Principles 4 and 5 of the Mozilla Manifesto emphasize that individuals must have the ability to shape the internet and their own experiences and that their security and privacy must not be treated as optional. In today's interconnected world, these principles are increasingly at risk.

Harmful design practices not only manifest at the interface level but also lie deep within the system's architecture (e.g. OS-level), particularly in cases of vertical integration of services and features. Deploying manipulative, coercive, and deceptive tactics such as aggressive and misleading prompts, messages, and pop-ups risk overriding user choice entirely.

Along the same lines, while personalisation in digital services can enhance user interaction, it poses significant privacy risks and potential biases, leading to the exposure of sensitive information and societal inequalities.

To address these issues, we believe it is high-time for the EU to update its consumer protection rules in a holistic manner to create a fairer digital world, especially as technology continues to evolve.

The Digital Services Package has set the EU up for success in reining in big tech and creating a more trustworthy and accountable online environment. The DSA marks a significant step toward a better internet. Amongst many positive



provisions, it mandates big tech companies to provide access and share publicly accessible data with researchers and oversight bodies to understand “systemic risks”, while placing significant responsibilities on these companies to identify and mitigate hidden harms online, particularly in online advertising. Transparency is essential to uncovering and addressing these harms. Moreover, while the DSA doesn't solve every issue, it incentivizes companies to assess and address the risks their products may pose, encouraging those with the biggest problems to make the most significant efforts. The early messages from the Commission regarding DSA implementation are very encouraging and will set the blueprint for its long-term success.

At the same time, the DMA has the potential to significantly improve contestability and choice for EU consumers and businesses. Through obligations and restrictions on gatekeepers, the DMA aims to ensure fair competition in the digital sector, promoting innovation, consumer choice, and transparency by facilitating data access, promoting interoperability, addressing self-preferencing practices, and maintaining easy default settings and choice screens to foster consumer choice.

However, its full potential is at risk due to gatekeepers' tactics, which aim to minimize the DMA's impact on their business models and hamper genuine consumer choice. The critical challenge is ensuring gatekeepers do not protect their closed ecosystems at the expense of competition. The Commission's recent investigations demonstrate a commitment to serious compliance, and we fully support effective compliance from gatekeepers to ensure the DMA delivers on its goals.

It is crucial that the European Commission and the co-legislators capitalise on the momentum created by the adoption of the DSA and DMA in the next five years to promote a safer, responsible, and trustworthy online environment that respects consumers' choices and allows them to shape their online experiences.

Key Recommendations

Strong Enforcement of Existing Rules: Ensure robust enforcement of milestone tech regulations such as the DSA and the DMA. This includes empowering regulatory bodies with the necessary resources and authority to monitor and penalize violations effectively. In the DMA, compliance proposals by gatekeepers should also be assessed through the lens of how effectively they contribute to the spirit of the law and eventually achieve true contestability and fairness in the digital markets. In the context of the DSA, compliance by designated VLOPs and VLOSEs must meaningfully improve transparency in practice, not only in theory. As an example, formal guidance on Article 40(12) is strongly recommended to ensure meaningful public data access for public interest research

Revising EU's consumer protection rules: Update the *Unfair Commercial Practices Directive* and its list of prohibited practices to include a wide range of harmful design practices, particularly those beyond the interface level, that aim to coerce, manipulate, or deceive consumers. At the same time, *anti-circumvention measures* should be introduced to ensure that no bypassing of legal requirements by design techniques will be possible. Finally, the drafting of clear guidelines on the interaction between different rules that address harmful and deceptive design practices (e.g. AI Act, DSA, GDPR, UCPD, etc) should be prioritized. In parallel, the update of EU consumer rules should create the conditions for the European Commission to assume increased enforcement powers.

Giving meaningful choices to consumers: Ensure that the DSA provisions around transparency in algorithmic processes will genuinely enable users to understand and interpret how personalization decisions are made, including the logic behind content recommendations and ad targeting. At the same time, for such transparency to be meaningful, implement robust mechanisms through legislation for users to opt out of personalization features with clear,

understandable processes and provide them with the ability to influence the degree of personalization at any point in their product experience.

Fostering open access and true interoperability: Key components to the creation of fair and contestable markets are open standards, enabling open access for developers and creating the conditions for true interoperability. Powerful tech companies, particularly vertically integrated ones, have little incentive to ensure openness and interoperability as they largely benefit from the lock-in effects. This is particularly prevalent in restrictions imposed by large developers of operating systems. We call on policymakers to embrace the adoption of open standards, and to facilitate access and interoperability so developers and users can reap the full benefits of competitive digital markets - including the choice and innovation that brings.



About Mozilla

Mozilla is most recognized as the maker of the open-source Firefox web browser, but our mission extends far beyond this. We are dedicated to protecting an open and accessible internet by investing in advocacy, research, and movement-building. We are guided by the principles enshrined in the [Mozilla Manifesto](#), asserting that the Internet must remain a public resource and that security and privacy are fundamental rights that must not be compromised.

For the past 25 years, Mozilla has been at the forefront of developing open-source software, supporting the open-source community, and championing digital empowerment and trustworthiness. Our next 25 years will build on this legacy, focusing on creating responsible tech products and growing our community with new talent committed to improving the internet.

Founded in 1998, Mozilla currently consists of five organizations: the 501(c)3 Mozilla Foundation, which leads our movement-building work; and its wholly owned subsidiary, the Mozilla Corporation, which leads our consumer product-based work; Mozilla Ventures, a tech-for-good investment fund; Mozilla.ai, an AI R&D lab; and MZLA, which makes Thunderbird. These organizations work in close concert with each other and a global community of tens of thousands of volunteers under the single banner: Mozilla