moz://a

Mozilla's Vision for the United States: 2025 - 2026

Promoting openness in AI, protecting Americans' privacy online, and expanding choice and competition.

March 26, 2025

moz://a

In Brief: Mozilla's Policy Vision

Mozilla envisions a future where the internet is a truly global public resource that is open, accessible, and safe for all. An internet that benefits people using online services, prioritizes the right to privacy, and enables economic dynamism. Our commitment to this vision stems from Mozilla's 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 can only be achieved through a competitive ecosystem with a range of services and providers that foster innovation. However, today's internet is far from this ideal state, and is only set to become increasingly consolidated in the age of AI.

Over the coming years, we must radically shift the direction of the internet and Artificial Intelligence out of the hands of a few large private players and towards greater openness and choice, enhanced privacy, and fair competition.

Mozilla remains committed to working alongside policymakers to advance a free and open internet in the coming years, both through our products and through our engagement with regulators and legislators across the aisle. Collaboration with civil society and the broader policy community is essential to ensure everyone reaps the benefits of technological progress and innovation.

Our policy vision is anchored in our guiding principles for a healthy internet. We believe that the following priorities should be the 'north star' for U.S. policymakers and regulators.

moz://a

Priority 1: Promoting Openness, Competition, & Accountability in AI

AI is set to be one of the most critical innovations of recent memory, and its benefits must be shared widely while mitigating potential harms.

The modern web was founded on the ideal of openness and built on an architecture that enabled broad access and participation. However, the open architecture that defined the outset of the web has been eroded, with the internet increasingly dominated by a few big platforms and proprietary systems and technologies. At the dawn of the AI age, these same dominant tech companies are positioned to hegemonize the next phase of the internet by controlling major AI systems. In order to have a dynamic internet economy and AI ecosystem that offers real accountability and choice, the principles of the modern web – focused on openness, access, and participation – must be protected. The AI era cannot be dominated by big tech companies, which could both threaten the pace of innovation and run roughshod over individual rights, like privacy.

Well-designed regulation is needed to make AI more trustworthy and to mitigate risk. AI policy should center on openness, competition, and accountability as the backbone of responsible regulation. American leadership in AI requires investments in the tools and resources necessary to build Public AI infrastructure. Well managed government-led or facilitated investment into Public AI, including investment into fundamental research and AI infrastructure like the National AI Research Resource (NAIRR), can also help to facilitate a more level playing field, and create choice for consumers and small businesses.

Promoting open approaches in AI has the potential not just to create technology that benefits individuals, but also to make AI systems safer and more transparent. Open approaches and public investment can spur increased research and

development, create products that are more affordable and less vulnerable to cyberattacks, and help to catalyze investment and job creation.

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

To ensure everyone can reap the benefits that AI has to offer, policymakers should avoid heavy-handed levers like export controls on open-source AI models. Instead, the new administration should build on the recommendations of NTIA and the Bipartisan House Task Force Report on AI to support the open-source AI ecosystem while continuing to collect information for future data-driven assessments. The enactment of broad export controls on open-source AI models would stymie innovation and allow for AI created by malign global actors to proliferate and gain significant market share across the world, to the detriment of America's national and economic security.

Key Recommendations

Increase Government Use of, and Support for, Open-Source AI: The federal government procures billions of dollars of software every year. However, much of it is closed-source, proprietary, and expensive. If Congress and the administration ease the ability to procure and use open-source software, it could result in significant time and cost savings for government IT projects. As federal agencies increasingly procure AI-enabled technology, using open-source AI models and software will help to increase government efficiency while strengthening the open-source ecosystem. More broadly, the government should promote and leverage open-source AI when possible, helping to enable more rapid diffusion of key technologies across the economy and drive growth —

including at the state level. Such an approach facilitates the development of a more competitive AI ecosystem, unlocking AI for everyone.

Develop & Fund Public AI Infrastructure: Public AI infrastructure takes a range of forms, but one concrete proposal is the National AI Research Resource (NAIRR). By supporting the creation and funding of the NAIRR, Congress and the administration could kickstart the development of Public AI, giving researchers and smaller universities access to AI tools and compute resources, and enabling innovation and a more level playing field. In addition, supporting projects like the Department of Energy's proposed Frontiers in Artificial Intelligence for Science, Security and Technology (FASST) initiative will be critical in not only pushing the scientific frontier forward, but in creating Public AI infrastructure that benefits the American people.

Growing the AI Talent Ecosystem: America must invest in community colleges, rural and public universities, apprenticeship and retraining programs, and beyond to develop and grow the domestic AI talent ecosystem. This will not only help America compete with a workforce necessary to be a global AI leader, but provide pathways to good jobs for those who have been left behind.

Provide Access to AI-Related Resource Consumption Data: At its current growth trajectory, AI could end up consuming tremendous amounts of energy and natural resources. In order to more effectively understand the needs of the industry and work to bring more clean energy online to stabilize grids, and to help consumers retain access at reasonable prices, government should work with the AI industry (from semiconductor developers to cloud providers to model deployers) to provide open access to resource consumption data and increase industry transparency.

Clarify the Federal Position on Open-Source AI Export Controls*:* In their July 2024 report on the use of open models, NTIA concluded that based on the data available today, the government should take no current action to restrict open

foundation models. The bipartisan 2024 House AI Task Force report on AI similarly emphasized the benefits of openness in AI model development, while focusing on demonstrable harms and physical threats. In addition, the January 2025 AI Diffusion Framework created an exemption for models with publicly available model weights, serving to further highlight the importance of the diffusion of American open models. However, discussions linger over the use of export controls to limit the dissemination of open AI models. This creates uncertainty for the open-source community and the many startups that leverage such software to bring products to market cheaper and faster than large tech companies. By affirming a federal position on open-source AI export controls to reflect those of NTIA, and emphasizing the benefits of open models, the administration can spur further advancement in the field. This could in turn help advance American open-source powered AI exports around the world.

moz://a

Priority 2: Protecting Online Privacy & Ensuring Accountability

Today's internet economy is largely powered by hoovering up people's information and using it for monetization. While that data has enabled remarkable innovation and "free" online services, it has also resulted in real world harm to consumers. With the rise of generative AI, which requires massive amounts of data for model training, the issue of online privacy is more urgent than ever. The rush to secure data for training AI models may lead to a race to the bottom, with companies harvesting more and more data to gain an edge in AI development, making respect for privacy a competitive disadvantage.

At Mozilla, we firmly believe that individuals' security and privacy on the internet are fundamental and must not be treated as optional. Mozilla has taken significant steps through our products and wider efforts to create a more privacy-preserving web. For example, we deploy technical anti-tracking measures such as Enhanced Tracking Protection (ETP), and Total Cookie Protection (TCP), in Firefox. 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 improve privacy in the ecosystem while still delivering effective advertising solutions.

Our work extends beyond products. Through the Mozilla Foundation, we support projects and drive research to advance privacy practices and hold companies to account, including Meta over their deprecation of CrowdTangle, a public insights tool widely used by the research community. We also actively participate in standards bodies like W3C to promote user privacy and ensure that the shift towards more privacy-preserving advertising is happening in an open manner.

While organizations like Mozilla build privacy-protecting products to help consumers avoid the harms of the predatory data ecosystem, such solutions aren't enough – we need a change in incentives facilitated by government action.

moz://a

Legislation can incentivize companies to adopt more privacy-preserving business practices, ultimately benefiting users and supporting their right to privacy online.

Mozilla has long called on Congress to enact a strong, comprehensive federal privacy law – such as the American Data Protection and Privacy Act (ADPPA) – that protects all citizens from abuse and misuse of their data, and holds companies accountable for their privacy practices. While Congress has debated various proposals over the years, we are long overdue for action. In recent years, a number of states have stepped in to fill the gap in a federal standard; when crafted correctly, state laws provide vital privacy protections. We support the advancement of these strong state privacy laws. Ultimately though, all Americans deserve such protections.

Key Recommendations

Pass Strong Comprehensive Federal Privacy Legislation & Support State Efforts: Congress must enact a sufficiently strong and comprehensive federal privacy law, setting a high bar for meaningful protections. This is how Congress can create an environment where people can truly benefit from the technologies they rely on without paying the premium of having their personal data exploited. A comprehensive federal law should, among other things: address AI specific privacy protections; uphold data minimization; ensure the security protections that encryption provides people today; and cover both children and adults. In addition, we support vital efforts by states to fill the gap in federal action and enact strong state-level laws to protect their constituents.

Support the Development of Privacy Enhancing Technologies (PETs): Companies today are not incentivized to use PETs given current competitive dynamics that

lead to massive user data collection. Policymakers should support the development of Privacy Enhancing Technologies (PETs) by providing funding to NIST and the National Science Foundation to conduct research into fundamental and applied research while creating strong privacy protections that incentivize companies to adopt PETs. The global standards development and consensus process is essential for privacy preserving technologies to develop in a sustainable manner, in particular around areas like advertising.

Provide Necessary Resources & Tools to Data Privacy Regulators: As some of the most aggressive collectors of Americans' data, big tech companies and data brokers have been repeatedly implicated in privacy-related abuses. Congress and the administration should enable and empower relevant federal regulators by providing additional resources and authorizations to facilitate privacy-related investigations and enforcement. Efforts should, in particular, target data brokers who traffic sensitive data, especially those who sell information to malign actors, while rigorously enforcing the Protecting Americans' Data from Foreign Adversaries Act of 2024. Congress should consider what additional legislative actions are necessary to tackle the data broker industry.

Support Critical Independent Research: Policymakers should work to ensure meaningful access to important data from major platforms for academia and civil society so that big tech's harms can be more effectively studied and the companies held to account. These transparency efforts would help send a strong signal to industry that privacy-related harms will no longer be tolerated. Mozilla supported the bipartisan Platform Accountability and Transparency Act (PATA), which would help advance social media and ad transparency while creating a safe harbor for public-interest research. Such legislation remains critical, especially if also applied to AI platforms and model providers.

Respecting Browser Opt-Out Signals: Today, the technology exists for internet users to set "signals" within their browsers that automatically tell websites they

visit that they don't wish to be tracked, or have their personal data sold. A prime example of this is Global Privacy Control (GPC), a feature built into Firefox. Despite this progress, many browsers and operating systems – including the largest ones – still do not offer native support for these mechanisms. Mozilla previously emphasized the importance of regulation requiring browsers and mobile operating systems to include an opt-out setting; we are pleased to see a similar bill (California's AB 566) introduced in 2025. We encourage lawmakers at the state and federal level to support this key privacy tool in law and meet the expectations that consumers rightly have about treatment of their personal information.

moz://a

Priority 3: Expanding Choice for Consumers

It's clear that a small number of large tech companies control how people experience the internet today. We see harmful self-preferencing practices that manifest not only 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. Operating systems are incentivized to unfairly advantage their own products and to raise barriers for competitors, rather than foster interoperability, innovation, and openness.

Deceptive design practices – also called dark patterns – can limit or distort choice online as well. Deploying manipulative, coercive, and deceptive tactics such as aggressive and misleading prompts, messages, and pop-ups risk overriding user choice entirely.

Principle 4 of our Manifesto emphasizes that individuals must have the ability to shape the internet and their own experiences. Mozilla believes that people should be able to choose which software they wish to use, including being free to choose something different from the operating system provider's own browser and software. We live this principle through our products, including the Firefox browser and Gecko browser engine– offering people genuine choice over how they experience the web.

At Mozilla, we see firsthand the importance of user choice and competition in the browser and browser engine ecosystem – yet it's often overlooked. These issues have a real cost to society. When big tech platforms use deceptive tactics to hinder competition, consumers and startups lose out on vital opportunities for innovation, product diversity, privacy, and security.

moz://a

No company should be punished for their success or building products that people prefer, but anti-competitive practices like harmful self-preferencing create an imbalanced market and must be addressed to prevent consumer harm & protect innovation.

Today, the technology sector is at an inflection point, as the largest companies position themselves as the main beneficiaries of the AI revolution. The tactics that created market concentration today must not work tomorrow. Updated competition laws – and an understanding of the importance of competition at every layer of the ecosystem – are essential for the internet to be private, secure, interoperable, open, transparent, and to balance commercial profit with public benefit. Mozilla is committed to this future.

Key Recommendations

Update Antitrust Legislation: No company should be punished for their success or building products that people prefer. However, policymakers must address anti-competitive business practices that stymie innovation and limit consumer choice. In order to effectively tackle the root causes of anti-competitive behavior in the tech industry, Congress must pass antitrust legislation which addresses harmful self-preferencing practices and provides necessary resources, expertise, and authorities to relevant regulatory agencies. Legislation like the bipartisan American Innovation and Choice Online Act (AICOA) serves as an example of the type of regulation necessary to create a level playing field.

Tackle Illegal and Harmful Online Practices such as Deceptive Design Practices: Harmful deceptive design practices not only manifest at the interface level, but also deeper at the operating system 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. Policymakers must hold bad actors accountable.

Foster Competition Across the Ecosystem: Independent browser and browser engine developers, like Mozilla, have a long history of innovating and offering privacy and security conscious users a meaningful alternative to big tech browser engines. They also have a long history of using their browsers to promote competition. It's important that policymakers take into account the importance of independent browsers and browser engines as a means to ensure a safe, open, and interoperable web that offers people meaningful choice.

moz://a

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 our time and resources in advocacy, research, startups, 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.

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 Builders, a startup accelerator program to support the open-source AI ecosystem; 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.