moz://a

Pathways to a fairer digital world:

shaping rules to increase consumer protection and choice online

moz://a

Summary

In the evolving digital landscape, where every click, swipe, and interaction shapes people's daily lives, the need for robust consumer protection is more important than ever. The propagation of harmful design practices, aggressive personalisation, and proliferation of fake reviews have the potential to limit or distort choice online and harm people, particularly the most vulnerable, by leading them into taking actions that are not in their best interest, causing financial loss, loss of privacy, security, and well-being.

From the mildly persuasive techniques that nudge users in specific directions, to the more overtly deceptive practices, harmful design can be found both at the interface level, but also deeper in the system's architecture. The sheer diversity of harmful design can make it difficult to craft rules aiming to tackle such practices. Additionally, the widespread use of milder 'dark patterns' makes enforcement of the rules more difficult.

Take for example, the design of cookie banners and the use of high and low-contrasting colors. While this nudging technique is not explicitly illegal under existing EU rules, Data Protection Authorities, like the Danish DPA, have argued that the use of colors when choosing options can influence visitors to make certain choices. Looking into the system's architecture, harmful choice structures on operating systems include setting default choices that are not in consumers' best interests, changing the order or appearance of options to self-preference the platform, or making it difficult for consumers to make decisions by overloading choices. Research conducted by the European Commission showed that choice structure practices like defaults and false hierarchy are among the most prevalent manipulative design practices. There is strong evidence that these practices (in particular default settings) have a significant effect on consumer behavior and that they directly impact competition.

At the same time, aggressive personalisation practices are becoming the norm. There is nothing inherently wrong with personalizing content online and tailoring recommendations to users based on their individual preferences. However, an increasing number of platforms base their recommendations and personalized services on aggressive data collection practices, presenting users with false binaries, or collecting data without the consent or knowledge of users. Such practices can pose risks to online privacy and perpetuate biases and discrimination. Enforcing consumer choices in a meaningful manner (e.g. respecting universal opt-out signals), mandating platforms to allow users to influence the degree of personalisation and incentivising, through legislation, the use of privacy-enhancing technologies can prove effective in both safeguarding users' privacy and supporting innovation to offer a personalized online experience.

At Mozilla, we are committed to building a healthy Internet – an Internet that respects fundamental rights and constitutes a space where individuals can genuinely exercise their choices. Principles 4 and 5 of our Manifesto state that individuals must have the ability to shape the internet and their own experiences on it, while their security and privacy are fundamental and must not be treated as optional. In today's interconnected world, these are put at stake.

We believe that voluntary commitments by industry are not sufficient, and legislation can play a crucial role in regulating such practices. Recent years have seen the EU act as a pioneer when it comes to online platform regulation. Updating existing EU consumer protection rules and ensuring strong and coherent enforcement of existing legislation will build on this framework to further protect EU citizens in the digital age.

In this document, we outline our vision and key recommendations on how EU regulators can create a fairer digital world, particularly in the context of the fitness check the European Commission is conducting on consumer protection legislation.

Addressing harmful design practices to increase consumer protection & choice

In today's interconnected world, the design of digital interfaces significantly influences our daily interactions, decisions, and overall well-being. An observed troubling trend in the digital realm is the proliferation and pervasive use of harmful design practices. These practices, often termed 'dark patterns' or 'deceptive interfaces', subtly (or sometimes aggressively) coerce people into decisions they might not have otherwise made, compromising the fundamental principles of user autonomy and transparency.

These designs are more than mere annoyances; they represent a stealthy influence on people's behavior, exploiting a range of practices to undermine their autonomy to the benefit of online services. This phenomenon ranges from frustrating mazes and sneaky designs in user experiences to tricks like false scarcity claims in e-commerce. More insidiously, these designs often target the most vulnerable, exploiting personal characteristics such as disability, age, health, income, or digital literacy, as well as temporary states of vulnerability.[1]

The ethical implications of these practices are profound. They raise questions about the responsibility of designers and the impact of their creations on individual agency. As a result, there is a compelling need for a paradigm shift towards ethical digital design.

Ethical design must empower users to make decisions aligned with their values, free from subtle coercion or manipulation. This involves prioritizing clear communication and ensuring users fully understand the implications of their choices. Moreover, digital interfaces must be inclusive, considering diverse perspectives and needs to create a positive and accessible online experience for all. Designers also have a responsibility to prioritize the security and privacy of user data, adhering to robust standards to protect user information. However, it is important to note that

[1] Such characteristics can make people more susceptible to harmful design techniques. Sunstein, C. R. (2020). Sludge Audits. Behavioural Public Policy, 1–20. https://doi.org/10.1017/bpp.2019.32

designers may be subject to (or overridden by) commercial or business incentives.[2] As a result, regulation can play a crucial role in addressing the challenges and mitigating the risks stemming from harmful design practices, particularly for the most vulnerable consumers. It can also help to align incentives within companies by providing clearer lines and consequences for harmful design techniques.

Research by Mozilla has found that operating systems use online choice architecture to push people away from selecting their own browser, which not only impedes choice but also has cascading effects related to privacy and cybersecurity, as well as competition. We've also conducted research on YouTube's user controls, which give people a false sense of agency when navigating YouTube's recommendation algorithm. This research has important implications for regulators since harmful design is a common circumvention technique whereby companies meet a surface level of compliance without committing to meaningful change in their architecture for end-users.

The EU at the center of regulating 'dark patterns'

Harmful design practices can mislead users, particularly vulnerable consumers, into making decisions that are not in their best interest, thereby impairing their autonomy, decision-making, and choice. It can also have negative financial and emotional consequences for people. The EU has to date made a significant effort in regulating 'dark patterns', adopting various pieces of legislation and guidance documents to that end.

The European Data Protection Board (EDPB) and the recently adopted Data Act have provided definitions and categorizations of dark patterns, emphasizing their manipulative nature and the resultant harmful outcomes for consumers. Although the General Data Protection Regulation (GDPR) and the ePrivacy Directive do not explicitly mention dark patterns, they form part of the legal framework regulating these practices. For instance, the collection of consent under the GDPR or the ePrivacy Directive could involve harmful design techniques. The EDPB's guidelines on dark patterns for social media platforms offer practical recommendations for assessing these practices, highlighting their potential to hinder users' ability to provide informed consent.

The Unfair Commercial Practices Directive (UCPD) is another crucial piece of legislation that covers harmful design, especially in the context of online advertising and commercial practices. The Directive prohibits unfair practices that could mislead consumers and affect their economic decisions. The Digital Services Act (DSA) and the Digital Markets Act (DMA) further expand the regulatory framework, specifically targeting deceptive techniques that distort user choice. Last but not least, the meteoric rise and expansion of AI, the widespread use of large language models as well as general purpose AI tools have the potential to intensify the deployment and sophistication of such unfair commercial practices, doing so even more opaquely and amplifying the harms of

[2] See, for example, the US Federal Trade Commission's 2022 complaint against Epic Games for illegal dark patterns tricking consumers into making purchases which found that designers within the company had raised concerns: https://www.ftc.gov/system/files/ftc_gov/pdf/1923203EpicGamesComplaint.pdf

harmful design interfaces. The recently agreed AI Act includes a number of provisions and prohibitions against practices that "exploit vulnerabilities of specific groups of persons" or "use subliminal techniques beyond a person's consciousness" to manipulate individuals into making decisions that they may not have otherwise made. It further includes a series of transparency obligations for certain AI systems to ensure that natural persons are informed that they are interacting with an AI system.

Amidst all this legislative activity, there is an ongoing debate around the extent and immediacy of further legislative action in this area. Some argue for a 'wait and see' approach, emphasizing the need to allow current regulations to be enforced fully and to identify gaps before introducing additional legislation. Additionally, there are arguments that such regulation might hinder innovation or undermine a seamless online consumer experience.

Given the prevalence of harmful design patterns (97% of the most popular websites and apps, according to one Commission study[3]), the burden on consumers is already high. At Mozilla, we believe that as technology evolves and new features are introduced on online platforms, the asymmetry of power and information between people and platforms becomes even greater, and consumers become more and more vulnerable. For that reason, the regulatory framework should also evolve and adjust to ensure that the causes and effects of such harmful practices are sufficiently addressed.

In addition, any legislative and regulatory action must consider how to address subtler techniques that might not (whether individually or cumulatively) meet the threshold for any bright line restrictions. For example, we know that milder harmful design patterns may not elicit the same backlash as more aggressive ones, and they disproportionately impact more vulnerable people[4]; therefore, subtlety and detectability are important factors to take into account. The nature of user experiences today means that consumers are not always well-equipped to either understand the subtleties or detect such mild dark patterns. Additionally, the focus should not only be on the visible harmful design techniques, but we need to move beyond those and think about the underlying systems, the structural design of the product, and the overall system architecture. Last but not least, any rethinking of EU consumer protection regulation should ensure that traders or platforms will not deploy design techniques to circumvent requirements stipulated within EU law.

Against this background, the current patchwork approach to regulating harmful design practices will not be sufficient. Reforming consumer protection legislation is crucial to address the challenges posed by harmful designs in a comprehensive and future-proof manner.

[3] Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, Final Report 2022

[4] Luguri, Jamie and Strahilevitz, Lior, Shining a Light on Dark Patterns (March 29, 2021). 13 Journal of Legal Analysis 43

moz://a

Policy Recommendations

- **Revise EU's consumer protection rules:** This should involve *updating the list of prohibited unfair commercial practices*[5] to also include milder 'dark patterns', as well as an *anti-circumvention clause* to ensure that no bypassing of legal requirements by design techniques will be possible. At the same time, principles that can guide the design of fair digital interfaces should be established. To increase legal clarity across member states, the EU should *turn the Unfair Commercial Practices Directive (UCPD) into a maximum harmonization directive* and publish clear guidelines on the interaction between the UCPD and the explicit prohibition of dark patterns in Article 25 of the DSA.
- **Strong Enforcement of Existing Rules:** Ensure robust enforcement of existing regulations, including the GDPR, DSA, and DMA. This includes empowering regulatory bodies with the necessary resources and authority to monitor and penalize violations effectively, as well as provide clarity through the form of guidance and guidelines on how these different proposals interact in practice.
- **Create Meaningful Transparency & Disclosure:** Mandating transparent communication of design choices can help users be informed about their interactions and the potential impacts of user behavior. Transparency, however, should not turn into a tick-the-box exercise for platforms. To create meaningful transparency requirements, they should be standardized across the EU and evaluated on a regular basis to ensure their effectiveness. Additionally, platforms should be equally transparent with enforcement bodies and regulators regarding their measures, practices, and policies.
- **Assist UX designers:** The EC has a crucial role to play in supporting those working within online platforms who aspire to act ethically in their design and operational choices. By assisting designers and platforms in crafting their user interfaces (UIs) and underlying systems to avoid harmful design, the EC can play a pivotal role in creating a more ethical digital landscape. This assistance can take various forms, including the provision of resources, guidelines, and best practices that help designers prioritize user rights and data protection in their work.
- **Support for Research:** There is already a good body of research around manipulative designs and dark patterns and extensive taxonomies illustrating harmful design practices compiled by academics, designers, and regulators. Further investment in research should be supported to provide evidence of the efficiency of adopted policies. This research can inform future legislative efforts and help regulators enforce rules more effectively. It will also allow for the regular update of taxonomies relating to harmful designs and what constitutes an unfair commercial practice, as well as its severity and if it should be added to the list of prohibited practices.

[5] Annex I, Directive 2005/29/EC

moz://a

Personalization Practices: Balancing Innovation with Consumer Protection

In the evolving digital landscape, personalization has become a cornerstone of the online experience, offering enhanced user interaction and innovative customization. The advent of personalization in digital services has ushered in a new era of user experience. By tailoring recommendations and interfaces to individual preferences, personalization fosters a more engaging and innovative online environment.

Nevertheless, these advancements bring forth significant challenges. The extensive collection and use of personal data in personalization pose risks to user privacy, potentially leading to the exposure of sensitive information. Moreover, personalization algorithms may perpetuate biases and discrimination, reinforcing societal inequalities. A notable concern is the lack of transparency in these algorithms, often described as 'black boxes,' which can erode user trust and impede informed decision-making.

Significant steps have been taken recently with the adoption of the Digital Services Act in addressing the above-mentioned challenges. As we have previously outlined, the DSA includes a number of provisions that explicitly address the role of recommender systems. The novel approach of the DSA requires VLOPs/VLOSEs to assess and mitigate their "systemic risks" (Articles 34 and 35), also accounting for "the design of their recommender systems and any other relevant algorithmic system" (Article 34 (2)). Article 27 (which applies to all online platforms) is even more direct, providing for a baseline of user-facing transparency around recommender systems. On top of this, Article 38 mandates that VLOPs/VLOSEs must offer at least one version of their recommender system that does not rely on "profiling" under the General Data Protection Regulation (GDPR). Thus, the DSA serves as a robust foundation that legislators can build on when revising consumer protection legislation.

Mozilla supports this balanced and layered approach that protects user rights and autonomy while fostering innovation. Legislators have a crucial role in safeguarding individual privacy in the digital space. While critics might argue that users voluntarily provide personal information and that stringent privacy regulations could hinder the development of personalized services, we believe privacy protection is paramount. Personalization practices often involve extensive data collection, and without proper safeguards, this can lead to significant privacy breaches.

Policy Recommendations

EU consumer laws contain various provisions that require businesses to disclose information to consumers in order to increase awareness and understanding of how online services function, the so-called transparency requirements. However, transparency should not be seen as a panacea. More transparency will not necessarily solve the challenges brought upon by today's information asymmetry and power imbalance between consumers and businesses. In light of these

considerations, we believe that any upcoming review of consumer protection legislation in Europe should follow the below approach to ensure high levels of consumer protection in the realm of personalization:

- **Enforcing consumer choices:** Implement robust mechanisms, through legislation, for users to opt out of personalization features with clear, understandable consent processes. At the same time, leverage legislation to ensure that all actors involved (i.e., websites, online platforms, etc.) will respect and effectively apply the consumer preferences and privacy choices made through these consent processes. For example, universal opt-out signals such as Global Privacy Control (GPC) can only be effective and respected by websites if there is the necessary regulatory backing and actors are not allowed to ignore such signals.
- **Incentivising 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. Through the deployment of PETs, companies might be able to use information that would inform personalization choices, but those uses would be limited because they would be denied access to the underlying information. Consumer protection legislation should also encourage and incentivize the adoption of PETs, particularly in sensitive areas. Additionally, we believe the Consumer Rights Directive should be amended to mandate the use of PETs when digital content and digital services are provided free of charge but in exchange for personal data.
- **Transparent Algorithms & Personalisation Opt-outs:** Ensure transparency in algorithmic processes, enabling 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, users should be allowed to opt out of personalized recommendations or to influence the degree of personalization at any point in their product experience.
- **Establish Independent Audits:** We propose that any update in the consumer protection regulatory framework will require regular, independent audits of online platforms to assess and ensure compliance with anti-manipulative design standards. This can be modeled on the DSA's independent audits as stipulated in Article 37 of Regulation 2022/2065. Regularly auditing and evaluating personalization algorithms to identify and rectify biases can also foster inclusivity and diversity in recommendations.

Tackling Fake Reviews: establishing a Trusted Review Ecosystem

In the digital age, where online shopping has become a staple of consumer behavior, the integrity and trustworthiness of product reviews have become paramount. At Mozilla, we have observed with growing concern the pervasive issue of fake reviews across online platforms. These dishonest practices distort the true value of products and undermine consumer trust.

Fake reviews, both positive and negative, have become increasingly common on major e-commerce platforms. Research conducted by Fakespot[6] in 2020 indicated that nearly one-fifth of Shopify stores engaged in unreliable or deceptive behavior. At the same time, the rapid development and deployment of general-purpose AI is only adding fuel to this trend. These false reviews distort the e-commerce market, misleading consumers and impacting their purchasing decisions. The problem is exacerbated by incentivized reviews, such as those seen in programs like Amazon Vine or Influenster, which often do not reflect an actual purchaser's experience.

Mozilla supports legislative, policy, and regulatory efforts to fight against this scourge of dishonesty. We believe that the lack of serious action by platforms that host fake reviews necessitates a robust response from regulatory authorities.

Legislative Landscape in Europe

In Europe, there is growing recognition of the issue of fake online product reviews and their impact on consumer trust and market integrity. The pandemic has led to a surge in online shopping, with many consumers relying heavily on online reviews, comparable to personal recommendations. The prevalence of fake reviews has prompted regulatory action across Europe.

The European Commission and national consumer protection authorities conducted, in 2022, a comprehensive EU-wide examination of online consumer reviews across 223 major websites in 26 Member States, Iceland, and Norway. This extensive investigation raised significant concerns regarding the trustworthiness of online reviews. Key outcomes from this study revealed questionable review authenticity[7], transparency issues[8], failure to address fake reviews[9] and inadequate handling of incentivised reviews[10].

The EU has taken concrete steps to address this issue. On one hand, the Digital Services Act (DSA) introduces a series of measures to ensure the authenticity and reliability of online reviews, such as the obligation for platforms to verify the identity of reviewers, prevent fake reviews, and establish a system to remove discriminatory, defamatory or offensive reviews On the other hand, the Better Enforcement and Modernisation Directive (Directive (EU) 2019/2161), which came into effect on May 28, 2022, explicitly prohibits the sale, purchase, and submission of fake consumer reviews. However, the Directive's implementation varies across EU member states, and provisions within the Digital Services Act might not go far enough in tackling the emergence of fake reviews at its core.

---

[6] In May 2023, Mozilla acquired Fakespot, a startup whose website and browser plug-in help users identify bogus product reviews on e-commerce site. More on Fakespot here.

[7] Out of the 223 websites examined, 144 displayed doubts about the authenticity of their consumer reviews

[8] A total 104 websites failed to adequately inform consumers about these processes. Only 84 websites clearly provided this information on their review pages

[9] A large number of websites, 118 to be exact, did not offer information on measures to prevent fake reviews

[10] The majority of the websites, 176 in total, either did not explicitly state that incentivised reviews are prohibited by their policies or failed to detail how they identify and manage such reviews.

Policy Recommendations

Additionally to existing rules and legislation that can address fake reviews, the European Commission's fitness check should focus on updating other pieces of legislation or guidance documents (e.g. see UCPD) to make sure that all aspects of EU's consumer acquis are fit to tackle the proliferation of fake reviews. For these reasons, the following concepts should be embedded in legislation to ensure their effective enforcement:

- **Disclosures and Verification:** Legislators should require explicit disclosure if a reviewer is part of an incentivized review program. Platforms must eliminate reviews from unverified purchases and clearly separate incentivized reviews from verified purchase reviews.
- **Transparency & Responsibility:** Online marketplaces should report their efforts to remove fake reviews, provide an effective and easy-to-use mechanism for consumers to report suspicious reviews, and be transparent about any modifications, edits, or removals of reviews. This further implies thorough enforcement of the relevant provisions within the DSA. Platforms must also be held accountable to eliminate review censorship, in which negative reviews are removed or suppressed, presenting serious consumer harm in areas such as product safety. Finally, regulators should ensure that platform moderation capabilities are equal across languages and remove fake review groups and brokers from social media platforms.
- **Enforcement Against Incentivized Review Programs:** Companies facilitating incentivized reviews must implement safeguards to verify actual product use and disclosure. Actions should be taken against participants who resell products without using them.
- **International Consistency:** Reviews posted on international versions of e-commerce sites should not be cross-posted onto other country-specific platforms, as product differences and customer experiences can vary significantly.

Redefining the concept of the 'average consumer'

In EU consumer law, the concept of the *'average consumer'* is a critical benchmark used to assess the fairness of commercial practices. Historically, this 'average consumer' has been defined as "reasonably well informed, observant, and circumspect." However, this definition has come under scrutiny, particularly with the advent of digital commerce, where consumer vulnerabilities are more easily exploited. Studies in behavioral and psychological science suggest that actual consumer decision-making often deviates from this rational model, highlighting the need for a redefinition.

Criticism of the current definition has been growing over the past decade. With digital commercial environments presenting new challenges, there is a growing consensus that the time is ripe for EU consumer law to align more closely with the real capabilities of consumers. Additionally, there has been a greater understanding of the impact harmful designs have on consumers. For example, we know that vulnerable or less savvy consumers can be more susceptible to dark patterns overall. In

parallel, the time consumers are confronted with a choice to make can play a significant role in their decision, affecting their state of vulnerability. If, for example, a consumer is prompted to make a choice in the middle of an unrelated workflow, this can result in frustration and annoyance, eventually leading them to make an uninformed decision simply so they can continue with their workflow. This, combined with the offering of a commercial choice that is designed in a harmful way, significantly raises the state of vulnerability of the consumer at that moment.

Moreover, there is a need to clarify the application of the average consumer concept in personalized commercial practices. The Netherlands Authority for Consumers and Markets (ACM) suggests that in cases of personalization, where commercial practices are tailored to individual consumers or specific groups, the notion of an average consumer is less relevant. Personalization is based on specific characteristics of the targeted consumer or group, and these should be considered by traders in their commercial practices. This approach would prevent the exploitation of specific vulnerabilities and inherently protect more vulnerable consumer groups in cases of personalization.

Policy Recommendations

- Update and redefine the average consumer concept to better reflect real consumer behavior and enhance the overall protection level offered by current legislation, particularly in the digital age.
- Clarify that the average consumer standard should not apply in cases of personalized commercial practices.
- In some cases, such as deceptive design, where a substantial number of (but not all) users would be consistently harmed by a practice, the average consumer standard may not be as useful.
- Lower the existing high threshold in defining an 'average consumer' in order to raise the overall level of protection offered by the current legislation to better protect consumers in the digital age.

Conclusion

Mozilla stands resolutely committed to advocating for a digital environment that prioritizes fairness, transparency, and consumer protection.

We believe in a proactive, comprehensive approach to protecting consumers from harmful design practices. This includes updating EU consumer laws, enforcing existing rules, and supporting research. Additionally, we strongly believe there is a world where personalized services and practices can enhance user experience while safeguarding privacy and autonomy. Our aim is to achieve a balance where innovation in personalization is matched by rigorous consumer protection.

We also emphasize the importance of restoring trust in the online marketplace, particularly in the authenticity of online reviews. Lastly, we advocate for a redefinition of the 'average consumer' concept within EU consumer law, as well as lowering its threshold, to tackle the existing information asymmetry and power imbalance between consumers and businesses. Such an update is crucial to reflect the real behavior and capabilities of consumers in the digital age, where vulnerabilities can be more easily exploited.

In a nutshell, our policy recommendations focus on:

- **Addressing harmful design practices** - Harmful design practices in digital experiences - such as those that coerce, manipulate, or deceive consumers - are increasingly compromising user autonomy and reducing choice. We advocate for a shift towards ethical digital design through stronger regulation, particularly as technology evolves. This would include stronger enforcement of existing regulations addressing harmful design practices (e.g., GDPR, DSA, DMA). At the same time, the EU should update its consumer protection rules to address milder 'dark patterns' and introduce an anti-circumvention clause to ensure that no bypassing of legal requirements by design techniques will be possible.
- **Balancing personalization & privacy online** - Personalization in digital services enhances user interaction but poses significant privacy risks and potential biases, leading to the exposure of sensitive information and societal inequalities. To address these issues, our key recommendations include the adoption of rules that will ensure the enforcement of consumer choices given through consent processes and incentivizing privacy-enhancing technologies through legislation (e.g. Consumer Rights Directive) to strike the right balance between personalization practices and respect of privacy online.
- **Tackling fake reviews** - The growing problem of fake reviews on online platforms has the potential to mislead consumers and distort product value. We recommend stronger enforcement of existing rules, meaningful transparency measures, including explicit disclosure requirements for incentivized reviews, increased accountability for consumer-facing online platforms, and consistency across the EU and internationally in review-handling to ensure the integrity and trustworthiness of online reviews.
- **Rethinking the 'average consumer'** - The traditional definition of the 'average consumer' in EU consumer law is characterized as *"reasonably well informed, observant, and circumspect"*. The digital age directly challenges this definition as consumers are increasingly more vulnerable online. Due to the ever-growing information asymmetry between traders and consumers, the yardstick of an 'average consumer' does not necessarily reflect existing consumer behavior. For that reason, we ask for the reevaluation of this concept to reflect today's reality. Such an update will actively lower the existing threshold and thus increase the overall level of protection and prevent the exploitation of vulnerable groups, especially in personalized commercial practices.

We believe that these proposed policy recommendations, in the context of the EU's fitness check of consumer protection legislation, are essential steps towards ensuring consumer protection in an increasingly digital world.

moz://a

About Mozilla

Mozilla is the non-profit-backed technology company that champions privacy, human dignity, and an open internet. Our mission is to ensure the Internet is a global public resource, open and accessible to all. Founded as a community open-source project in 1998, Mozilla currently consists of the Mozilla Foundation, which leads our movement-building work; and its wholly-owned subsidiary, the Mozilla Corporation, which leads our consumer product-based work. Other entities include Mozilla Ventures, a tech-for-good investment fund; Mozilla.ai, an AI R&D lab; and MZLA, which makes Thunderbird. In May 2023, Mozilla acquired Fakespot, a small startup whose website and browser plug-in help users identify bogus product reviews on e-commerce sites.

For more information, please contact Tasos Stampelos (tstampelos@mozilla.com), Mozilla Corporation