How Ethical is your Web Browser?

Summer / Autumn 2025

In an age dominated by "big tech" and artificial intelligence (AI), online privacy and data monopoly are more important than ever. Your choice of web browser plays a critical role in controlling how much personal data is gathered about you and your online activity.

Initially the guide explores: the crucial reasons why your browser choice matters - how to find the best browsers for privacy and security - the ethical considerations behind big tech companies like Google, Apple, and Microsoft - the environmental impact of data centers and AI - simple ways you can reduce your internet-related carbon footprint – then is followed by a comprehensive analysis of web browsers, data ethics and corporate responsibility

Contents:

Why Your Browser Choice is a Big Deal

The most popular browsers—Chrome (Google), Edge (Microsoft), and Safari (Apple)—are owned by big tech companies that profit from your online activity. These companies track your browsing history and personal data to create user profiles for targeted advertising and to sell to third parties. This is how they make most of their money.

Have you ever searched for a holiday destination and then seen endless ads for flights and hotels? That's targeted advertising in action. While some find this helpful, many see it as a significant invasion of privacy.

Beyond advertising, some browser-owning companies, such as Google and Microsoft, use your browsing data to train powerful AI tools. If you're uncomfortable with your data being monetized or used for other means, switching to a more privacy-focused browser is essential.

Browser Market Share: Who's in Charge?

Globally, Google Chrome is the undisputed leader, with around 65% of the market. Apple's Safari is a distant second, with nearly 20%. Other browsers have a minimal share in comparison, though market dominance varies by country and device.

Browser	Global Market Share
Chrome (Google)	65%
Safari (Apple)	18%
Edge (Microsoft)	5%
Firefox (Mozilla)	2.5%
Samsung Internet	2.2%
Opera	2.1%

Sources: StatCounter and Oberlo.

How to Block Online Ads and Trackers

Annoying pop-ups and auto-playing video ads can be more than just a nuisance; they can redirect you to malicious sites containing malware or viruses. Blocking them improves your browsing experience, making it faster and safer.

You can install an ad blocker as a browser extension or choose a browser with one built-in. Popular extensions include Ad Blocker, Ghostery, and uBlock Origin.

Some browsers with built-in ad blockers include:

- Brave
- LibreWolf
- Opera
- Tor

However, it's worth noting that Google is actively working to limit ad blocker extensions on its Chromium-based browsers (including Chrome, Edge, and Opera), as these extensions interfere with their primary revenue source.

The Best Browsers for Privacy and Security

Your personal data is a valuable commodity, and browser privacy settings are your first line of defence. The default settings vary widely, but some browsers are built with privacy as a priority.

Cookie Control

Cookies are small text files that websites place on your device. While some are harmless (first-party cookies that remember your login or language preferences), others are used by advertisers to track your activity across different sites (third-party cookies). This tracking allows them to target you with specific ads.

Private Browsing and VPNs

Most browsers offer a private browsing or incognito mode, which prevents your activity from being recorded in your browser history or storing cookies. However, your Internet Service Provider (ISP) can still see your activity. For true privacy, a Virtual Private Network (VPN) is the best solution. A VPN encrypts your internet traffic, hiding your IP address and identity from your ISP and the websites you visit.

Browsers with Strong Default Privacy

If you want to avoid a deep dive into your browser's settings, these browsers offer a higher level of privacy by default:

- Brave: Blocks ads and trackers automatically and even allows users to earn rewards by opting into privacy-respecting ads.
- Firefox: Created by a non-profit organization, Mozilla, which is committed to internet privacy and safety.
- DuckDuckGo: Known for its privacy-focused search engine, it also has a browser with built-in tracker blocking and a privacy-grade feature for websites.
- Tor: The most well-known browser for anonymity. It routes your traffic through multiple servers to conceal your IP address, making it impossible to trace your activity.

The Best Security Features

To protect against phishing and malware, always use the latest version of your browser. Some browsers, like Brave, also automatically block malicious sites or default to HTTPS connections, which encrypt your communication with websites.

Ethical Issues with Big Tech

Choosing an ethical browser is just one step. Many of the companies that dominate the browser market are also connected to broader ethical concerns.

Tax Avoidance

Companies like Amazon, Google, and Microsoft have been criticized for complex financial structures that allow them to pay a fraction of the taxes they should on profits earned in countries like the UK. This avoided tax revenue could otherwise fund vital public services.

Military and Human Rights

Both Google and Microsoft have been implicated in supporting the Israeli military and government through lucrative contracts. This has led to protests and calls for greater accountability from these tech giants.

Energy Consumption and AI

Powering the internet is incredibly energy intensive. Every search, data storage action, and AI-powered task uses a huge amount of electricity. Data centers—massive warehouses full of computer equipment—are responsible for this consumption. In the UK, data centers are projected to account for 10% of the national electricity demand by 2050.

The rapid expansion of AI, in particular, is driving this demand. For example, a single ChatGPT search uses about ten times more electricity than a standard internet search.

How to Reduce Your Internet Carbon Footprint

While your personal internet use may not be a huge part of your carbon footprint, every little bit helps.

- Use Bookmarks: Instead of searching for the same websites repeatedly, use bookmarks. This can cut your browsing-related carbon emissions by up to 35%.
- Avoid AI-Generated Searches: If you don't want AI-generated answers, use search engines that don't currently use them, like Ecosia, or find a way to turn them off.
- Choose Efficient Browsers: Browsers that block ads and pop-ups tend to load pages faster, which slightly reduces energy usage.

Who Owns Which Browser?

The browser world is split between "big tech" giants and independent, often non-profit, organisations.

- Big Tech:
    - Chrome (Google)
    - Edge (Microsoft)
    - Safari (Apple)
- Independent/Non-Profit:
    - Brave: Open source.
    - DuckDuckGo: Open-source.
    - Ecosia: An independent B Corp that uses its profits to plant trees.
    - Firefox: A non-profit developed by the Mozilla Foundation.

- Tor: Open-source and non-profit, developed by the Tor Project.

Making an ethical switch is one of the easiest, most painless, and free changes you can make to your online life. By choosing a browser that prioritizes privacy, security, and ethics, you can take control of your digital footprint and support a more open and fair internet.

A Comprehensive Analysis of Web Browsers, Data Ethics, and Corporate Responsibility

Summer / Autumn 2025

Executive Summary

This report provides a comprehensive analysis of the web browser, moving beyond its function as a simple tool to explore its role as a critical piece of digital infrastructure with significant ethical, environmental, and geopolitical implications. The findings presented here challenge the notion that a browser is a neutral gateway to the internet, revealing instead a complex ecosystem shaped by corporate business models, data collection practices, and global supply chains.

The analysis indicates that the web browser market is not a diverse landscape but a highly concentrated duopoly dominated by Google Chrome and Apple's Safari. This market control is not merely a reflection of user preference but a structural advantage tied to the parent companies'

ownership of the most prevalent mobile operating systems. The core business model of these dominant players is a data-for-service exchange, where the "free" browser serves as a conduit for extensive, often opaque, data collection, which is then used to fuel targeted advertising and a larger ecosystem of services.

Furthermore, the report uncovers the significant environmental costs hidden behind a seemingly weightless digital experience. The exponential growth of artificial intelligence (AI) and cloud services is fuelling a parallel surge in energy and water consumption by hyperscale data centers. Despite public commitments and significant investments in renewable energy by major tech firms, the scale of this growth is outpacing sustainability efforts, creating a fundamental tension between business expansion and environmental responsibility.

On the corporate ethics front, major technology companies, including Google and Microsoft, are facing unprecedented scrutiny and legal risk over their military and government contracts. The report details growing shareholder and employee activism demanding greater transparency and due diligence, particularly in response to allegations linking these companies' technologies to human rights abuses in conflict zones. The admission by one company of a "due diligence gap" highlights a new form of material financial risk tied to ethical governance.

The report concludes that a viable ecosystem of ethical alternatives exists. Browsers such as Mozilla Firefox, Brave, and the Tor Browser are distinguished by their non-profit status or privacy-centric business models. By understanding the incentives that drive these different models, users can make informed choices that contribute to a more responsible and equitable digital future. The final section offers concrete, actionable recommendations for users to make these ethical switches, demonstrating that what seems like a small personal choice can have a measurable impact on the broader technology landscape.

Part I: The Browser Ecosystem and the Power of Default

1. The Global Web Browser Market: A Study in Concentration

The global web browser market is characterized by a stark concentration of power, with a few key players holding a commanding share of internet traffic. Current data from multiple sources consistently places Google Chrome in a position of overwhelming dominance. In recent analyses, Chrome's market share has been reported to be as high as 68% globally, with figures from different measurement services placing it in the range of 56.2% to 68% [1]. This makes Chrome the most widely used browser on both desktop and mobile platforms [2].

A distant but strong second place is held by Apple's Safari, which commands a significant share of the market, particularly in the United States, where it leads in mobile usage [2]. Globally, Safari's market share typically hovers between 16% and 24% across various platforms, a position reinforced by its status as the default browser on all Apple devices, including iPhones, iPads, and

Macs [1, 2]. The rest of the market is fragmented among a handful of other browsers. Microsoft Edge, which is bundled with Windows operating systems, holds a smaller share, generally

between 4.5% and 5.7% [1]. Mozilla Firefox, a long-standing competitor, typically secures a share of around 2.2% to 5.8% [1]. Other browsers with a notable, albeit smaller, presence include Samsung Internet, which holds a third-place ranking in the mobile market, and Opera [2, 3].

The dominance of Chrome and Safari is not solely a product of their features or performance but is also a direct consequence of a fundamental structural advantage. Both Google and Apple are the leading developers of mobile operating systems—Android and iOS, respectively—and control the hardware that billions of people use daily [2]. This control allows them to pre-install their own browsers as the default option on these devices. This creates a powerful and self-reinforcing dynamic. Most users, guided by convenience and a lack of awareness, simply use the browser that came pre-loaded on their device. This massive, pre-existing user base then allows the companies to gather an immense amount of user data, which can be used to further refine the product and improve its features. This, in turn, attracts more users and developers to create extensions, cementing their market position and making it exceptionally challenging for independent competitors to gain a foothold. The market's concentration is thus less of a purely meritocratic outcome and more a consequence of vertically integrated business models.

2. The Anatomy of a Browser: How Data is Collected

At its core, a web browser is a data collection device. This process is complex and involves multiple mechanisms designed to gather information about a user's online behavior. One of the most common methods involves the use of cookies, which are small pieces of text that a website sends to a user's browser [4]. Cookies can be either first-party or third-party [5]. First-party cookies are created by the website a user is directly visiting and are essential for basic functionality, such as remembering login details, language preferences, or the contents of a shopping cart [4].

Third-party tracking cookies, on the other hand, are created by external servers via a piece of code loaded on the visited website. These are typically set by advertisers, data aggregators, or social media plugins and are designed to collect data on a user's online behavior, including clicks, shopping preferences, search history, and location [5]. Because third-party cookies can be accessed across different websites, they enable cross-site tracking, allowing advertising networks like Google and Amazon to build a comprehensive profile of a user's browsing activity [5]. This information is then used for online advertising and retargeting, often without the user's explicit consent [5].

Beyond cookies, a more advanced and difficult-to-block form of data collection is known as browser fingerprinting. This technique does not rely on text files but instead collects information about a user's unique device and browser configuration [5]. This data includes the browser type and version, the operating system, active plugins, screen resolution, and time zone [5]. While no single piece of this information directly identifies a user, the combination of these elements creates a unique "fingerprint" that is highly unlikely to be shared by another user. This makes it an effective, and often invisible, method for tracking users across the web [5].

A common misconception is that using a browser's "Incognito" or "Private" mode offers a significant degree of protection against these tracking methods. However, this is an incomplete

view of the functionality. While Incognito mode on browsers like Chrome, Firefox, and Edge clears local browsing history, cookies, and site data after the session ends, it does not provide true anonymity [6]. The research indicates that a user's internet service provider and the websites they visit can still see their activity [6]. The primary function of these modes is to prevent a user's activity from being stored on the local device, thereby hiding it from other individuals who might use the same computer [6]. The feature addresses a local, personal privacy concern but does nothing to combat the systemic, corporate-level data collection that is a fundamental aspect of the web today.

3. The Fine Print: Privacy Policies of Dominant Browsers

An examination of the privacy policies of the dominant browsers reveals that data collection is not a secondary function but a central pillar of their business models. Google's privacy statement explains that the company uses the information it collects from all its services to "provide our services," "maintain & improve," and "personalize" the user experience [7]. The data collected is extensive, including search terms, browsing history, device information, and location data [7, 8]. This information is linked across services to provide a "seamless experience" for users with a Google account [8]. For example, information from a search query can be used to influence a user's experience on YouTube or Google Maps [4, 7]. While the company states it does not share personally identifiable information with advertisers without user consent, it does allow "specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies" [7].

Similarly, Microsoft's privacy statement details the collection of "required diagnostic data" to ensure the browser is functioning properly, as well as optional diagnostic data that includes browsing history and search terms [9, 10]. This data is used to provide personalized experiences and "show more interesting ads" [9]. The company also notes that it obtains data from affiliates and third parties to augment its collection [10]. Both companies provide users with privacy dashboards to manage some of this data, such as changing ad settings or deleting browsing history [9, 10].

The language used in these policies, however, reveals a fundamental asymmetry of power. The documents frequently present data collection as a prerequisite for using the service. For example, Microsoft's privacy statement notes that users can decline to provide personal data, but this is immediately followed by a warning that "we will not be able to enter into the contract; or if this relates to an existing product you are using, we may have to suspend or cancel it" [10]. This is not a true choice but a form of "take it or leave it" consent, where the fundamental nature of the service requires a continuous flow of data. The for-profit, ad-driven business models of these companies create a direct and powerful incentive to maximize data collection. The "free" browser is not a gift to the user but a strategic entry point to a larger, monetized ecosystem, and the user's data is the currency that fuels it.

Part II: The Unseen Costs of a Connected World

1. The Environmental Footprint of Digital Infrastructure

Every click, search, and digital interaction we perform on a web browser has a physical and environmental consequence. The backbone of the digital world is a vast network of hyperscale data centers—immense facilities that store and process information on the cloud [11]. The environmental impact of these facilities is multi-faceted, encompassing mining for rare-earth minerals to manufacture hardware, land use for construction, and a staggering demand for energy and water for operation [11].

The energy consumption of data centers, particularly those optimized for AI workloads, has reached unprecedented levels. A single AI-focused data center can consume as much electricity as a small city [12]. For context, Google's data centers used 30.8 million MWh of electricity in 2024, accounting for nearly 96% of the company's total consumption [13]. This marks a colossal 7x increase over the course of a decade, and more than double the energy consumed by its data centers in 2020 [13]. Beyond energy, these facilities require vast amounts of water for cooling. Research estimates that for every kilowatt hour of energy consumed by a data center, it requires approximately half a gallon of water for cooling [11]. A striking example is Google's data centers in Dalles, Oregon, which in 2022 used more than a quarter of the city's water supply [11].

Despite these figures, major technology companies are publicly committed to aggressive sustainability goals, such as becoming carbon negative and water positive [14]. Google claims to have achieved 100% renewable energy matching globally since 2018, and its clean energy purchases in 2024 reportedly avoided 8.2 million metric tons of CO2e emissions [13]. Microsoft, for its part, has contracted 34 gigawatts of carbon-free electricity since 2020 [15]. Both companies are also making progress in improving the energy efficiency of their facilities, with Google's Power Usage Effectiveness (PUE) for 2024 closing in on the theoretical minimum [13].

However, the sheer scale of the problem reveals a fundamental paradox. While these companies are making commendable investments in sustainability, the exponential growth of their services, particularly in AI, is creating a demand for power that is outpacing these efforts. Google's total electricity consumption rose 27% year-over-year in 2024 [13], while Microsoft's total emissions increased by 23.4% due to "growth-related factors such as AI and cloud expansion" [15]. This indicates that the energy savings from efficiency improvements are being overwhelmed by the massive increase in demand for compute power. The companies' core business model, driven by growth and consumer demand for digital services, is accelerating a problem that their sustainability initiatives are designed to solve, creating a continuous feedback loop that is inherently at odds with true environmental sustainability.

2. AI and Sustainability: A Paradox

Artificial intelligence presents a unique challenge to corporate sustainability efforts, simultaneously being hailed as a solution to climate change and identified as a major new source of environmental strain. The development and operation of AI models are immensely energy intensive. Training a sophisticated model like GPT-4 required an estimated 30 megawatts of power [16]. The energy cost of generating AI outputs can also be significant. Research on 88 different models found that generating 1,000 images consumed 2.907 kWh, which is equivalent to almost 250 smartphone charges [17].

Major tech companies like Microsoft acknowledge this challenge, but also present a compelling counter-narrative, positioning AI as a powerful tool to address environmental problems. Microsoft's Copilot, for instance, can be used to help track total energy usage and identify areas for efficiency improvements [18]. AI can also optimize operations by predicting equipment failures, analysing data from sensors, and forecasting energy demand to improve resource allocation [18]. The argument is that AI can help to ensure operations are more reliable, efficient, and cost-effective [18].

This dynamic, however, highlights a classic economic principle known as the Jevons Paradox. This paradox suggests that an increase in the efficiency of a resource can lead to an increase in the demand for that resource, thereby negating the initial savings. The more efficient AI becomes at managing energy use, the more widely and critically it is adopted across a company's operations. This increased adoption then drives an even larger overall increase in demand for AI compute, which requires a commensurate increase in power and water consumption. Consequently, the energy saved by using AI to optimize data center operations may be eclipsed by the energy required to train and run the AI models themselves on an exponentially growing scale. The central question for the future is whether AI can truly be a net positive for the environment if its growth trajectory is inherently tied to a continuously escalating demand for power and water.

Part III: Corporate Ethics and Geopolitical Risk

1. The Human Rights Imperative in Technology

The past several years has seen an increase in scrutiny on the role of major technology companies in global conflicts, particularly in the context of government and military contracts. This has led to serious allegations of complicity in human rights abuses. Recent reports have linked the technologies of Google and Microsoft to the conflict in the Palestinian territories. For example, a joint $1.22 billion contract between Google and Amazon, known as "Project Nimbus," provides cloud computing infrastructure and AI services to the Israeli government and military [19]. Other sources allege that Microsoft's Azure cloud and AI systems have enhanced the capabilities of the Israeli military, with leaked documents indicating that Azure usage by the military surged by 155% in a recent period [20]. A UN report has named Microsoft as part of the "economy of genocide" in Gaza, and media outlets have alleged that Microsoft's technology may have been used for tasks like analysing satellite imagery and managing logistics [19, 20, 21, 22].

In response to these allegations, Microsoft has issued statements affirming its commitment to human rights and noting that internal and external reviews found no evidence that its technologies were used to "target or harm people in the conflict" [23]. The company maintains that its contracts are standard commercial agreements [23]. However, this official position is complicated by an admission that the company "does not have visibility into how customers use our software on their own servers or other devices" [20, 21]. This "blind spot" is a crucial point of contention and a source of significant concern for investors and activists. The inability to verify or prevent military clients from using its tools to target civilians exposes the company to potential legal and reputational fallout [21].

It is also important to note that the Palestinian territories are home to a vibrant and innovative technology sector, with companies specializing in a wide range of services from software development and mobile applications to AI and machine learning [24, 25]. The Palestinian Information Technology Association (PITA) serves as a unified voice for this community, which includes tech start-ups and outsourcing firms serving global clients [25]. This context offers a counter-narrative to the idea of a one-sided technology landscape, highlighting the resilience and capabilities of the Palestinian tech community.

2. Shareholder and Employee Activism: A New Era of Accountability

The ethical and legal complexities surrounding technology in conflict zones have become a central concern for institutional investors, activists, and employees. This has led to a new wave of shareholder and employee activism demanding greater accountability from major tech companies. A coalition of over 60 investors, representing approximately $80 million in Microsoft stock, filed a resolution demanding a public report on how the company mitigates the risk of its technologies being misused in conflict zones [20, 21].

The research indicates that this resolution is a strong signal that shareholders are beginning to prioritize "ethical governance over short-term profit" [21]. The pressure is not limited to investor groups; employees at Google and Microsoft have organized campaigns and staged walkouts to protest their companies' contracts with the Israeli military [19, 21, 23]. The core argument driving this movement is that ethical lapses are no longer just a matter of corporate philanthropy but have become a tangible financial risk. The research explicitly links a single incident of alleged human rights violations to "stock volatility, regulatory scrutiny, and brand damage" [20, 21].

This marks a significant redefinition of corporate responsibility, where human rights due diligence is now being framed as a core fiduciary duty. The due diligence gap admitted by Microsoft is seen by activists and investors as a material financial risk, as a company's potential complicity in international crimes could lead to severe reputational damage and long-term harm to shareholder value [20, 21]. The activism suggests that the traditional balance between technological innovation and ethical responsibility is being redefined, and that the ability to maintain long-term market leadership may now depend on a company's willingness to close the due diligence gap and address these ethical concerns directly.

Part IV: Towards a More Ethical Digital Future

1. Introducing the Ethical Alternatives

While the market is dominated by a few players with business models reliant on data collection, a vibrant ecosystem of ethical alternatives exists. These browsers offer a path to a more private and responsible digital experience.

Mozilla Firefox

Firefox stands out as a popular and privacy-focused alternative. It is an open-source browser led by the Mozilla Foundation, a non-profit organization whose mission is to promote an open and accessible internet [26, 27]. Firefox's core identity is rooted in its public-good mission, which sets it apart from its for-profit counterparts [27]. It offers strong security and privacy features, including third-party cookie blocking, and is praised for its frequent updates and customizable settings [28]. While its market share is small compared to Chrome and Safari, it is a distant second to Chrome among the alternatives [29]. The majority of its revenue is generated through royalties from search engine partnerships, with Google being the largest contributor [30, 31].

Brave

Brave is a browser built with privacy at its core. It is an open-source project based on the Chromium browser, which allows it to maintain a familiar interface and compatibility with many Chrome extensions [29]. Its primary distinction is its privacy-by-default design. It comes with a built-in ad-blocker and cross-site tracker blocking, and it includes strong fingerprinting protection [28]. A unique feature of Brave is its ad-reward model. Users can opt-in to view privacy-respecting ads and earn Brave's own cryptocurrency, Basic Attention Tokens (BAT), which can be cashed out or used to tip online content creators [29]. Brave also offers a built-in Tor mode for enhanced anonymity [6, 29].

Tor Browser

The Tor Browser is considered the gold standard for anonymity and privacy protection. It is an open-source browser designed to prevent tracking and surveillance by routing internet traffic through a vast network of volunteer-run servers. This "onion routing" process encrypts traffic multiple times, concealing a user's IP address and location from their internet provider and the websites they visit [6, 28]. While it is not designed for casual browsing due to its slower speed, it provides the highest level of anonymity available [6]. The Tor Project is a non-profit organization funded by a diverse range of sources, including US federal agencies, private foundations, and individual donors [32, 33, 34].

Other notable browsers include Vivaldi, which offers a highly customizable interface with built-in productivity tools and a customisable ad-blocker [35], and DuckDuckGo and Epic, which are also praised for their privacy-first design and built-in tracker-blocking features [28].

2. Feature Comparison and Business Models

The single most predictive factor of a browser's privacy posture is the business model of its parent organization. This can be clearly seen when comparing the dominant players to the ethical alternatives. Google and Microsoft are publicly traded companies whose primary revenue streams are directly or indirectly tied to data-intensive services like advertising and cloud

computing [7, 9, 10]. This creates a direct incentive to maximize data collection to improve ad targeting and "personalize" services, even as they provide user controls to opt-out [5].

In contrast, the business models of the alternatives are fundamentally different. Mozilla is a non-profit foundation whose financial operations are secondary to its mission to promote an open internet for the public good [26, 27]. Its revenue from search engine deals, while significant, is used to fund this mission, which includes developing a more private browser [30]. The Tor Project is funded by donations and grants from organizations committed to human rights and internet freedom [32, 33, 34], ensuring its incentives are purely aligned with user anonymity [6]. Brave's unique ad-reward model attempts to reconcile the two opposing forces of advertising and privacy by placing the user in control of the data exchange [29]. When the business model is to sell ads, the user is the product, and data is the currency. When the business model is to serve the public good, user privacy becomes the core product.

The following table provides a side-by-side comparison of the features and business models of these ethical alternatives.

Table 2: Ethical Alternatives: Features & Business Models

Browser	Open Source	Tracker Blocking	Fingerprinting Protection	Business Model
Mozilla Firefox	☑ Yes [28]	☑ Needs user adjustment [28]	☑ With tuning [28]	Non-profit; majority revenue from search engine royalties [30, 31]
Brave	☑ Yes [28]	☑ Built-in [28]	☑ Strong [28]	For-profit; ad-reward model pays users for viewing private ads [29]
Tor Browser	☑ Yes [28]	☑ By design [28]	☑ Strong [28]	Non-profit; funded by grants and individual donations [32, 33]
DuckDuckGo	⊘ No [28]	☑ Built-in [28]	⊘ Limited [28]	For-profit; search engine revenue [6, 28]
Epic	⊘ No [28]	☑ Built-in [28]	☑ Strong [28]	For-profit; details not specified [28]

Conclusion & Recommendations: The Power of Choice

Browsing the web is not a neutral act. The choice of which browser to use carries significant implications for personal privacy, corporate accountability, environmental sustainability, and geopolitical ethics. The analysis indicates a series of fundamental paradoxes: a market dominated by a duopoly that co-exists with a fragmented ecosystem of independent alternatives; public corporate sustainability goals that are challenged by the exponential energy demands of AI; and human rights commitments that are undermined by the inability to track technology misuse by customers.

However, the analysis also validates the assertion that shifting to a more ethical browser can be one of the easiest, most painless, and free changes a user can make. These choices, while seemingly small, can collectively influence corporate behavior and contribute to a healthier, more transparent digital landscape.

Based on the findings of this report, the following actionable recommendations are provided:

1. **Choose a Browser Based on Your Needs:** Select an alternative browser that aligns with your personal privacy requirements. Brave is an excellent choice for a seamless transition with strong, built-in privacy features [29]. Firefox offers a powerful balance of features, customization, and a mission-driven organization [29]. For maximum anonymity, the Tor Browser is the definitive choice, though it requires a willingness to sacrifice browsing speed [6].
2. **Modify Your Settings:** For users who are unable to switch from a dominant browser, it is crucial to modify default settings. This includes disabling optional diagnostic data collection and personal ad tracking via the browser's privacy dashboard [9, 10].
3. **Use Privacy-Enhancing Tools:** Further protect your browsing activity by installing privacy-focused browser extensions. Tools like uBlock Origin and Privacy Badger can effectively block third-party trackers and ads, preventing many forms of data collection [28].
4. **Consider a VPN:** A browser-based solution is only one part of a comprehensive privacy strategy. A Virtual Private Network (VPN) offers an additional layer of protection by encrypting all traffic on a device, not just that within the browser [6].

Ultimately, the power to make conscious digital choices rests with the user. By understanding the incentives and impacts of the tools we use daily, it is possible to reclaim a degree of agency and contribute to a digital future that prioritizes transparency, ethics, and sustainability.

References:

1. Usage share of web browsers - Wikipedia
2. Understanding Browser Market Share: Which browsers to test on in 2024 | BrowserStack
3. Mobile Browser Market Share Worldwide | Statcounter Global Stats
4. How Google uses cookies – Privacy & Terms
5. What are Tracking Cookies & How to Block Them - CookieYes
6. The Complete Guide to Private Browsers - Security.org
7. Privacy Policy – Privacy & Terms – Google
8. Privacy Policy – Privacy & Terms – Google
9. Microsoft products and your data – Microsoft privacy
10. Microsoft Privacy Statement – Microsoft privacy
11. Measuring the environmental cost of artificial intelligence and their data centers
12. What Are the Environmental Impacts of Artificial Intelligence?
13. Google's data centers using more power than ever before as AI ...
14. Sustainability | Microsoft CSR
15. 2025 Microsoft Environmental Sustainability Report
16. Power for AI: Easier Said Than Built | BloombergNEF
17. How much electricity does AI consume? - Windows Copilot News
18. Sustainability – Microsoft Adoption
19. No Tech for Oppression, Apartheid or Genocide | BDS Movement
20. Unprecedented investor action demands Microsoft answer for reported involvement in Gaza genocide | American Friends Service Committee
21. Microsoft Faces Human Rights Heat Amid AI Activism | KnowESG
22. Which companies are complicit in Israel's genocide and occupation of Palestine - YouTube
23. Inside the Microsoft protests: Fired engineer speaks out on Palestine, Israel, AI, and big tech
24. Top 20+ IT Companies in Palestinian Territory (2025) - TechBehemoths
25. PITA | Leading Palestine's Technology & Innovation Economy
26. Mozilla Foundation - Wikipedia
27. Who we are - Mozilla Foundation
28. The 5 Best (& Worst) Secure Web Browsers for Privacy 2025
29. 6 Alternatives to Chrome for 2025 | Best Privacy Browsers
30. Mozilla's Data Privacy FAQ
31. Mozilla Corporation - Wikipedia
32. Who funds Tor? | Tor Project | Support
33. Supporters - Tor Project
34. The Tor Project - Wikipedia
35. The Best Web Browsers for 2025: Expert Recommendations for a Superior Internet Experience | TechRadar