United States Securities and Exchange Commission
Washington, D.C. 20549

NOTICE OF EXEMPT SOLICITATION
Pursuant to Rule 14a-103

Name of the Registrant: Microsoft Corporation
Name of persons relying on exemption: National Legal and Policy Center
Address of persons relying on exemption: 107 Park Washington Court, Falls Church, VA 22046

Written materials are submitted pursuant to Rule 14a-6(g) (1) promulgated under the Securities Exchange Act of 1934. Submission is not required of this filer under the terms of the Rule but is made voluntarily in the interest of public disclosure and consideration of these important issues.

PROXY MEMORANDUM

TO: Shareholders of Microsoft Corporation
RE: The case for voting ***FOR*** Proposal 9 on the 2024 Proxy Ballot ("Report on AI Data Sourcing Accountability")

This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card; National Legal and Policy Center is not able to vote your proxies, nor does this communication contemplate such an event. NLPC urges shareholders to vote for Proposal 9 following the instructions provided on management's proxy mailing.

The following information should not be construed as investment advice.

Photo credits follow at the end of the report.

National Legal and Policy Center ("NLPC") urges shareholders to vote **FOR** Proposal 9, which it sponsors, on the 2024 proxy ballot of Microsoft Corporation ("Microsoft" or the "Company"). The "Resolved" clause of the proposal states:

Shareholders request the Company prepare a report, at reasonable cost, omitting proprietary or legally privileged information, to be published within one year of the Annual Meeting and updated annually thereafter, which assesses the risks to the Company's operations and finances, and to public welfare, presented by the real or potential unethical or improper usage of external

data in the development and training of its artificial intelligence offerings; what steps the Company takes to mitigate those risks; and how it measures the effectiveness of such efforts.

Introduction

Artificial intelligence (AI) is one of the most transformative innovations in modern history – reshaping industries, revolutionizing business practices, and influencing how individuals and governments engage with technology. AI's potential to improve everything from healthcare to financial services is undeniable, yet it comes with great risks. Microsoft, with its substantial AI investments, stands at a pivotal juncture where adopting strong privacy-centered policies could set it apart as a trusted leader.

Data is the lifeblood of AI. Machine learning models require massive datasets to learn, adapt, and improve their performance over time. This insatiable hunger for data drives developers to seek out large quantities of information via the Internet and other digital sources, some of which may be obtained unethically or illegally. AI models may incorporate data on human behavior, speech, images, and other sensitive content, making their development and deployment a privacy concern.

As AI matures, so does public awareness of AI data ethics. Consumers, regulators, and governments increasingly ask tough questions about where AI developers obtain the data used to train their models. Data scraping, unauthorized collection, and the use of proprietary or copyrighted content without permission have become focal points in the debate over AI ethics. Without proper internal checks and balances, Microsoft's AI development may violate data privacy laws, infringe on intellectual property rights or utilize personal information without consent.

The report requested in the Proposal would increase shareholder value by improving disclosure of Microsoft's strategy for ethical usage of user data in AI development. This report seeks to encourage Microsoft to adopt a more ambitious pro-privacy stance, which may provide the Company a strong competitive advantage.

Privacy and Ethical Challenges Facing Microsoft in AI Development

Microsoft is a leading player in the AI space, thanks largely to its partnership with OpenAI. The Company's position provides a platform to define expectations for responsible AI development.

The data-gathering practices that underpin Microsoft's AI models raise ethical concerns. As mentioned in the Proposal, these include the Company's partnership with OpenAI,[1] its ties to the United States Intelligence Community,[2] [3] copyright infringement,[4] and questionable privacy features.[5] [6]

Microsoft's organizational size, scope, and influence – the Company is one of the largest in the world by market capitalization,[7] revenue,[8] and headcount[9] – invite distrust. Public scrutiny is further amplified by Microsoft's relationships with other power players in the industry as well as the federal government.

For example, why were Microsoft and Apple both offered special seats on OpenAI's board? Are they not competitors? The two rivals only dropped their seats after antitrust concerns were raised.[10]

Microsoft's partnership with OpenAI raises other issues. OpenAI has faced multiple allegations of unethical data collection practices, including data scraping without consent. Reports indicate that OpenAI has incorporated vast amounts of personal, copyrighted, and proprietary information into its AI models without notifying data owners or obtaining their permission. Such practices have led to legal action, including a high-profile lawsuit by the *New York Times* over alleged copyright infringement. Finally, Paul Nakasone, the former director of the National Security Agency, now sits on OpenAI's board of directors. Under his tenure, he pushed to renew the expanded surveillance powers[11] awarded to the NSA after 9/11, which have since been abused to spy on political opponents of the national security apparatus.[12]

Nakasone's appointment to OpenAI's board raises the broader issue of government interference with AI development and Microsoft's extensive relationship with the federal government. Microsoft derives a significant portion of its revenue from government contracts. The federal government spends between $10 billion and $15 billion on contracts for IT and software

---

[1] https://www.businessinsider.com/openai-chatgpt-generative-ai-stole-personal-data-lawsuit-children-medical-2023-6

[2] https://www.foxbusiness.com/politics/us-spies-use-secretive-ai-service-from-microsoft

[3] https://www.newsweek.com/edward-snowden-open-ai-nsa-warning-1913173

[4] https://www.reuters.com/legal/transactional/ny-times-sues-openai-microsoft-infringing-copyrighted-work-2023-12-27/

[5] https://time.com/6980911/microsoft-copilot-recall-ai-features-privacy-concerns/

[6] https://www.theverge.com/2024/6/7/24173499/microsoft-windows-recall-response-security-concerns

[7] https://companiesmarketcap.com/

[8] https://companiesmarketcap.com/largest-companies-by-revenue/

[9] https://companiesmarketcap.com/largest-companies-by-number-of-employees/

[10] https://www.theguardian.com/technology/article/2024/jul/10/microsoft-drops-observer-seat-on-openai-board-amid-regulator-scrutiny

[11] https://www.cbsnews.com/news/nsa-director-us-surveillance-power-paul-nakasone/

[12] https://apnews.com/article/election-2020-b9b3c7ef398d00d5dfee9170d66cefec

services.[13] Microsoft dominates the market for these contracts,[14] winning 25-30 percent of them without a competitive bidding process, "meaning they're likely marked up."[15] As the federal government seeks to gain control over AI distribution for the purpose of controlling free speech,[16] it is entirely possible that the government might use Microsoft's contracts as leverage to gain concessions, effectively entangling one of the world's largest corporations with state interests. For example, the "Twitter files" revealed that the FBI and CIA played a major role in content moderation at Twitter – prior to its purchase by Elon Musk – by flagging posts or accounts deemed "misinformation" and recommending their removal.[17] Shareholders and citizens alike should be concerned that US intelligence agencies are attempting a similar play with the major AI developers, whose tools may eventually eclipse social media for their power to shape the global discourse.

Microsoft's immense power, coupled with its close relationship with the federal government, represents a significant threat to individual liberty in American society and elsewhere. Combined, the two have unprecedented access to the personal information of millions of citizens through Microsoft's platforms, products, and services. In an era of big data, where personal information is increasingly treated as a commodity, this relationship raises red flags about the potential for mass surveillance and erosion of privacy.

Further, with Microsoft's AI tools and technologies increasingly embedded in public infrastructure,[18] the lines between Microsoft and the national security state are increasingly blurred.[19] The potential for these technologies to be used as tools of control —whether for monitoring dissent, limiting freedom of expression, or tracking citizens— cannot be dismissed. In this context, Microsoft's AI development is not simply about technological progress. More importantly, it is about the unchecked growth of surveillance power in the hands of a corporation that has demonstrated willingness to align with government interests, even at the cost of individual freedoms.

In addition, Microsoft's algorithms are secret. As these systems become more integrated into daily life, shaping decisions from loan approvals to hiring, the lack of transparency around their inner workings poses significant ethical risks.

At the heart of AI development are machine-learning algorithms that rely on massive datasets to make predictions, detect patterns, and recommend actions. How these algorithms weigh certain variables, prioritize specific outcomes, and arrive at decisions often remains hidden in a "black box." This lack of transparency is more than a technical issue; it raises fundamental questions about accountability, trust, and fairness. If these algorithms are used in critical areas, such as healthcare diagnostics[20] or criminal justice risk assessments,[21] the consequences could include

[13] https://prospect.org/power/2024-06-11-defense-department-microsofts-profit-taking/

[14] https://ccianet.org/news/2021/09/new-study-shows-microsoft-holds-85-market-share-in-u-s-public-sector-productivity-software/

[15] https://prospect.org/power/2024-06-11-defense-department-microsofts-profit-taking/

[16] https://www.csis.org/analysis/distrust-everything-misinformation-and-ai

[17] https://nypost.com/2022/12/24/latest-batch-of-twitter-files-shows-cia-fbi-involved-in-content-moderation/

[18] https://wwps.microsoft.com/blog/ai-public-sector

[19] https://theintercept.com/2024/10/25/africom-microsoft-openai-military/

[20] https://www.forbes.com/sites/saibala/2023/01/23/microsoft-is-aggressively-investing-in-healthcare-ai/

[21] https://councilonj.org/the-implications-of-ai-for-criminal-justice/

unfair outcomes or even life-altering mistakes. For Microsoft, this opacity may protect proprietary information and intellectual property, but it ultimately raises questions about whether the company values profit and competitive advantage over transparency and accountability.

In response, citizens and consumers have begun to demand increased protections for data privacy. At its core, the debate centers around who truly "owns" the data generated by users—be it personal information, behavioral patterns, or digital content—and what rights individuals have over how their data is used, stored, or shared.[22] These evolving expectations have created challenges for companies like Microsoft and OpenAI, especially as they collect vast amounts of data to train and refine artificial intelligence (AI) systems.

The European Union has emerged as a global leader in the push for stronger data rights through the General Data Protection Regulation (GDPR), which was enacted in 2018.[23] GDPR represents one of the most comprehensive data privacy laws on the planet, fundamentally changing how companies collect, process, and store personal data for EU citizens. It grants individuals greater control over their data, including the right to access, correct, or delete their information, and the right to be informed about how their data is used. GDPR enforces strict penalties for non-compliance, with fines reaching up to four percent of a company's global annual revenue, creating a powerful incentive for companies to adhere to the principles of transparency, accountability, and user control. For companies like Microsoft, which operates on a global scale, GDPR has raised the stakes of data ethics.

In the United States, data privacy laws have traditionally been less stringent than those in the EU, with no comprehensive federal data privacy law akin to GDPR. However, this landscape is changing. States have begun to adopt their own data protection regulations, reflecting a growing recognition of the need for privacy protections. California, for example, enacted the California Consumer Privacy Act (CCPA) in 2020,[24] giving residents similar rights to those under GDPR, such as the right to know what personal information is being collected, the right to delete that information, and the right to opt out of its sale.

The movement for data privacy is gaining momentum in other states as well, creating a patchwork of state-level regulations that corporations like Microsoft must navigate. These new expectations around data privacy indicate a shift in public attitudes toward data ownership, with Americans increasingly demanding the right to control their digital information.

---

[22] https://www2.deloitte.com/us/en/insights/topics/digital-transformation/data-ownership-protection-privacy-issues.html

[23] https://gdpr-info.eu/

[24] https://oag.ca.gov/privacy/ccpa

The aforementioned lawsuit filed by the *New York Times* against Microsoft and OpenAI serves as a high-profile example of how changing expectations around data ownership intersect with legal challenges. The *Times* has accused OpenAI of scraping its copyrighted content to train AI models without permission or compensation, thereby infringing on intellectual property rights.[25] If the *Times* lawsuit succeeds, it could set a precedent that imposes greater restrictions on data scraping, especially when it involves proprietary or copyrighted content. This would create additional hurdles for Microsoft and OpenAI, forcing them to either secure permission from data sources or reconsider their datasets.

By continuing its current practices, Microsoft risks becoming entangled in more lawsuits and regulatory actions that could erode shareholder value and harm its reputation. Additionally, as consumers become more privacy-conscious, they may choose to support companies that demonstrate a genuine commitment to respecting data rights.

Increasing Shareholder Value and Building Competitive Advantage Through Privacy Leadership

Consumers have consistently expressed concern with the lack of control they have over their personal data.[26] McKinsey & Company has argued that companies that prioritize data privacy will build a competitive advantage over their competitors that do not.[27]

> As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage.
>
> Given the low overall levels of trust, it is not surprising that consumers often want to restrict the types of data that they share with businesses. Consumers have greater control over their personal information as a result of the many privacy tools now available, including web browsers with built-in cookie blockers, ad-blocking software (used on more than 600 million devices around the world), and incognito browsers (used by more than 40 percent of internet users globally). However, if a product or service offering—for example, healthcare or money management—is critically important to consumers, many are willing to set aside their privacy concerns.

---

[25] https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

[26] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[27] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

> Consumers are not willing to share data for transactions they view as less important. They may even “vote with their feet” and walk away from doing business with companies whose data-privacy practices they don’t trust, don’t agree with, or don’t understand.

The authors add:

> Our research revealed that our sample of consumers simply do not trust companies to handle their data and protect their privacy. Companies can therefore differentiate themselves by taking deliberate, positive measures in this domain. In our experience, consumers respond to companies that treat their personal data as carefully as they do themselves.

The report drives home the reality that as data privacy concerns grow, consumers increasingly favor companies that prioritize ethical data handling and transparency. This underscores the reality that companies with transparent, privacy-focused practices have a strategic advantage in a market where trust is paramount.

The shift in expectations around data ownership represents an opportunity for Microsoft to position itself as a leader in ethical AI by adopting transparent and consent-driven data practices. Such a shift would not only help Microsoft avoid legal challenges but would also build consumer trust, aligning the company with global standards that prioritize the individual’s right to control their own data.

For Microsoft, this means that transparent and privacy-respecting AI practices can foster customer loyalty and reduce churn. The financial benefits of customer retention are well-documented, as retaining an existing customer is often significantly less expensive than acquiring a new one.

Moreover, a privacy-centric approach aligns with the growing “techno-optimism” movement, which advocates for technology that empowers individuals rather than exploits them. Champions of this movement, such as venture capitalist Marc Andreessen,[28] argue that technology should decentralize power, enhance transparency, and empower users. By supporting these values, Microsoft can attract a growing demographic of users who view technology as a tool for personal empowerment rather than corporate control. This alignment would not only attract consumers but also influence public perception, positioning Microsoft as a leader in ethical AI.

Finally, the emphasis on privacy and transparency could reduce Microsoft’s vulnerability to regulatory backlash and legal issues. With stricter data privacy regulations emerging globally and cases like the *New York Times* lawsuit against OpenAI highlighting the risks of unethical data practices, Microsoft can preemptively mitigate risks by setting a high standard for transparency.

Microsoft’s competitors, including Apple, Meta, Alphabet, and Anthropic, vary significantly in their approaches to privacy, reflecting their values, business models, and strategic goals.

---

[28] https://a16z.com/the-techno-optimist-manifesto/

Understanding how each company handles privacy provides insight into the broader landscape of AI ethics, transparency, and consumer trust.

Apple

Apple, while not primarily focused on AI, has highlighted its user privacy protections as a priority.[29] Unlike Meta and Alphabet, Apple's primary business model does not rely on advertising, allowing it to enhance user privacy without compromising its revenue model. Apple says its AI-driven products, like Siri, are designed with privacy-enhancing technologies, including on-device processing, which minimizes data collection and promotes user control over personal information.

Apple's emphasis on privacy has provided an additional degree of assurance for privacy-conscious consumers, allowing it to maintain a loyal user base, giving the company a competitive advantage.

Meta

Meta has faced scrutiny over data privacy issues, particularly regarding how user data informs targeted advertising algorithms.[30] [31] In recent years, however, Meta has made strides toward increasing transparency in its AI research. Its release of the open-source Llama AI tool stands as a testament to its new direction, signaling a willingness to contribute to transparent and accessible AI development. Open-source AI models, like Llama, allow researchers and developers to examine and modify the code, increasing transparency.

Despite this open-source shift, privacy concerns persist due to Meta's reliance on user data for advertising revenue. Meta's AI algorithms extensively leverage personal data to generate targeted ads,[32] which raises concerns about whether the open-source commitment will extend to the company's most valuable and sensitive data-driven algorithms. The public scrutiny Meta has faced in recent years, including the Cambridge Analytica scandal,[33] has also impacted trust. Although open-sourcing Llama may signal greater transparency, questions remain about whether Meta's privacy improvements go far enough.

---

[29] https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business-advantage.html

[30] https://www.theguardian.com/technology/2023/jul/11/threads-app-privacy-user-data-meta-policy

[31] https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html

[32] https://www.reuters.com/technology/meta-gets-11-eu-complaints-over-use-personal-data-train-ai-models-2024-06-06/

[33] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Alphabet

Alphabet, via subsidiary Google, commands a powerful position in AI, utilizing vast data resources to fuel services like search engines and voice assistants.[34] However, its data practices, deeply tied to advertising revenue, have drawn consistent criticism for prioritizing user data collection over privacy.[35] Alphabet's extensive data tracking for targeted ads has repeatedly sparked privacy concerns, leading to significant fines, particularly under the EU's GDPR, for lack of transparency in data use. Despite implementing features like "auto-delete" options and experimenting with federated learning, where data is stored on devices instead of centralized databases, these measures are limited in scope and appear reactive rather than foundational.

Alphabet's reputation suffers further from incidents like tracking user location data even when location services are off,[36] highlighting inconsistencies between its public privacy commitments and real-world practices. Critics argue Alphabet treats user privacy as secondary to its ad-driven business, contrasting sharply with companies like Apple, which prioritize data minimization. As privacy expectations grow, Alphabet's reliance on extensive data collection may increasingly conflict with consumer demands for transparency and data sovereignty, ultimately challenging the sustainability of its approach.

Anthropic

Anthropic, an AI research lab founded by former OpenAI employees, has positioned itself as a company dedicated to "alignment" and AI safety. Its primary mission is to develop AI systems that are aligned with human interests, prioritizing safety and ethics over rapid deployment.[37] Although Anthropic is smaller than Microsoft, Meta, or Alphabet, its focus on long-term AI safety makes it a relevant player in the privacy conversation.[38]

Anthropic emphasizes transparency in AI behavior and is cautious about deploying its models in commercial applications without rigorous testing. While Anthropic's approach does not specifically prioritize privacy in the same way as Microsoft or Meta, its emphasis on safety, alignment, and ethical concerns indirectly supports a privacy-conscious framework. By promoting transparency and caution in deployment, Anthropic positions itself as an organization willing to sacrifice rapid growth for responsible, user-centered AI practices.

Given that Anthropic is still relatively new, it has yet to encounter significant regulatory or public scrutiny. Yet its foundational principles suggest a commitment to ethical practices, which could offer a competitive advantage as privacy expectations evolve.

Microsoft, Meta, Alphabet, Anthropic, and Apple each approach privacy differently, reflecting their distinct business models and consumer expectations. While Microsoft and Apple promote privacy as a competitive advantage, Alphabet and Meta face challenges due to their reliance on

---

[34] https://www.thestreet.com/investing/stocks/analyst-update-alphabet-stock-price-target-after-ai-event

[35] https://www.bloomberg.com/news/articles/2022-02-28/all-the-ways-google-is-coming-under-fire-over-privacy-quicktake

[36] https://time.com/6209991/apps-collecting-personal-data/

[37] https://www.anthropic.com/

[38] https://etc.cuit.columbia.edu/news/ai-community-practice-hosts-anthropic-explore-claude-ai-enterprise

advertising revenue. Anthropic's focus on long-term safety and ethical alignment positions it as a distinct player in the privacy conversation, especially as AI continues to evolve. As consumer demand for privacy grows, these varying approaches will shape the public's perception of each company's commitment to responsible AI.

For one reason or another, each of Microsoft's competitors have barriers preventing them from staking out a dominant position in the AI industry as a leader in both quality and privacy. Taking a strong, privacy-centered stance could set Microsoft apart from competitors and align it with modern values, thereby strengthening both consumer trust and shareholder value.

The economic benefits could be tremendous to Microsoft. The *New York Times* lawsuit alone could be billions of dollars, as could the penalties for violating the GDPR or CCPA. However, the more important issue is that the generative AI market could reach $1.3 trillion by 2032,[39] and small percentage changes in market share will be worth tens of billions of dollars. Microsoft's competition is too strong and potential reward to big to not take data ethics and privacy seriously.

Conclusion

By prioritizing privacy and ethical AI, Microsoft can distinguish itself in an industry where consumer trust is critical. As regulatory pressures grow and public expectations shift towards data transparency and control, Microsoft's commitment to responsible AI would not only safeguard its reputation but also enhance shareholder value. Embracing a privacy-first approach positions Microsoft as a leader in ethical technology, aligning it with both consumer and societal values. This strategic shift can help Microsoft gain a sustainable competitive advantage, fostering long-term growth and making a positive impact on the industry as a whole. For these reasons, we urge shareholders to support Proposal 9.[40]

Photo credits:
Page 2 – Microsoft building, Cologne, Germany/Rawpixel.com (Creative Commons)
Page 3 – Paul Nakasone/INSA Events, Creative Commons
Page 5 – OpenAI graphic/focal5, Creative Commons
Page 6 – New York Times headquarters/Jessohackberry, Creative Commons
Page 8 – iPhone/YouTube screen grab

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY.

---

[39] https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/

[40] https://view.officeapps.live.com/op/view.aspx?src=https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/2024_Proxy_Statement

THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY THE FILERS.

THE INFORMATION CONTAINED HEREIN HAS BEEN PREPARED FROM SOURCES BELIEVED RELIABLE BUT IS NOT GUARANTEED BY US AS TO ITS TIMELINESS OR ACCURACY, AND IS NOT A COMPLETE SUMMARY OR STATEMENT OF ALL AVAILABLE DATA. THIS PIECE IS FOR INFORMATIONAL PURPOSES AND SHOULD NOT BE CONSTRUED AS A RESEARCH REPORT.

PROXY CARDS WILL NOT BE ACCEPTED BY US. PLEASE DO NOT SEND YOUR PROXY TO US. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.

For questions regarding Microsoft Corporation Proposal 9 – requesting the Board of Directors to produce a "Report on AI Data Sourcing Accountability," submitted by National Legal and Policy Center – please contact Luke Perlot, associate director of NLPC's Corporate Integrity Project, via email at lperlot@nlpc.org.