

PX14A6G 1 o55262px14a6g.htm

Notice of Exempt Solicitation Pursuant to Rule 14a-6(g)

Name of the Registrant:

Alphabet Inc.

Name of persons relying on exemption:

Zevin Asset Management, LLC

Address of persons relying on exemption:

2 Oliver Street, Suite 806, Boston, MA 02119

Vote FOR Proposal #11: Shareholder proposal requesting that Alphabet publish a report assessing risks arising from gaps in its policies, controls, and oversight of customer and user data processed through Google Services and Google Cloud.

The attached written materials are submitted pursuant to Rule 14a-6(g)(1) promulgated under the Securities Exchange Act of 1934.

This is NOT a solicitation of authority to vote your proxy.
Please DO NOT send us your proxy card as it will not be accepted.

Zevin Asset Management, LLC (“Zevin”) urges shareholders to vote FOR Proxy Item number 11, a **Report assessing risks arising from gaps in company policies, controls, and oversight of customer and user data processed through Google Services and Google Cloud**. The proposal will be voted on at the June 5, 2026, annual general meeting of Alphabet Inc (“Company” or “Alphabet”).

RESOLVED:

Shareholders request the Board of Directors issue public reporting, prepared at reasonable cost and omitting proprietary information, assessing operational, reputational, regulatory, and legal risks to Alphabet, Inc. arising from gaps in the Company’s policies, controls, and oversight systems of customer and user data processed through Google Services and Google Cloud. The report should evaluate how governance gaps could lead Google’s products, infrastructure, or cloud services to facilitate surveillance, censorship, profiling, and targeting in contexts of governmental overreach and recommend risk-mitigation measures.

The proposal requests information regarding the effectiveness of Alphabet’s governance systems over the deployment of Google Cloud and other data processing products in high-risk contexts. The purpose of this request is to ensure shareholders have sufficient information to determine whether Alphabet is properly mitigating the salient and material risks arising from its customer’s use of its products and the associated data processing. This request is jurisdiction-agnostic, seeking a global framework that addresses systemic risks inherent in Alphabet’s role as an important infrastructure provider. The central question is whether Alphabet retains sufficient control, contractual authority, and oversight mechanisms to manage risks when its technologies and data are used by customers or accessed by government actors in sensitive applications. This proposal is supported by a group of institutional investors representing significant assets under management, reflecting growing concern regarding Alphabet’s governance, contractual controls, and oversight of data and cloud deployments in high-risk contexts.

1. Alphabet Expansion into Sensitive Applications Raise Salient Human Rights Risks

Alphabet’s Google services and cloud technologies are a critical piece of internet communication infrastructure used to support the daily lives of billions of people around the globe. However, in addition to purely civilian use, Alphabet is also providing cloud and artificial intelligence (AI) services in sensitive applications (e.g., military, security, border enforcement) and geographies (e.g., conflict-affected and high-risk areas). In such high-risk applications, these technologies underpin data-driven targeting, surveillance, and intelligence systems that are the most susceptible to facilitating salient human rights harms.

These capabilities are increasingly deployed by governments where their use may directly affect decisions involving civilian populations and protected infrastructure and occur in environments where significant allegations and reporting of violations of international humanitarian and human rights law have arisen. Specifically, these deployments involve dual-use technologies that enable large-scale data integration, pattern recognition, and operational decision-making including in combat operations. Recent reporting on military operations in high-risk geographies has documented significant civilian harm linked to incomplete or outdated targeting intelligence.¹ Analysis from policy and national security experts has identified systemic weaknesses in target identification and collateral damage assessment processes, particularly in environments characterized by compressed decision timelines, reliance on probabilistic data, and unprecedented operational tempo. These conditions may increase the likelihood that errors in data, model outputs, or analytical processes translate into real-world harm.²

¹ Reuters, "U.S. May Have Struck Iranian Girls’ School after Using Outdated Targeting Data," March 11, 2026, <https://www.reuters.com/world/middle-east/us-may-have-struck-iranian-girls-school-after-using-outdated-targeting-data-2026-03-11>; Reuters, "How Many People Have Been Killed in the U.S.-Israel War with Iran?," March 31, 2026, <https://www.reuters.com/world/middle-east/how-many-people-have-been-killed-us-israel-war-iran-2026-03-31>.

² Center for American Progress, "Loss of Innocents: The U.S. Strike on an Iranian School and Implications for America at War," YouTube video, 1:12:05, March 18, 2024,

In addition, risks arise from the use of cloud and AI systems in surveillance, censorship, and repression in environments with expansive state access powers and limited legal recourse. Alphabet's deployment in these sensitive contexts raises risks of facilitating unlawful and exploitative surveillance practices, resulting in the detention, harassment, and suppression of human rights defenders and marginalized communities.

Alphabet has high-risk customers deploying its cloud, AI, and other data processing systems in these sensitive contexts, including government agencies engaged in recent or active military and immigration enforcement operations. This includes the U.S. Department of Defense's Project Maven,³ U.S. Immigration and Customs Enforcement (ICE) operations, and the Israeli government's Project Nimbus. In addition, Alphabet is expanding into other high-risk jurisdictions, such as Saudi Arabia—where legal and governance constraints may limit Alphabet's oversight.

For example, Alphabet was selected as a key partner in Project Maven to apply the company's machine learning to drone and satellite imagery, enabling automated identification of objects and accelerating battlefield analysis.⁴ Similarly, an ICE cloud initiative has been authorized to use Google Cloud services through a contractor, placing Alphabet's infrastructure within a domestic enforcement and surveillance context.⁵ Independent research has documented that ICE has developed extensive data-driven surveillance capabilities, including access to large-scale personal data systems used for immigration enforcement, often with limited transparency or public oversight.⁶

Alphabet provides cloud and AI infrastructure to the Israeli government under Project Nimbus, which includes support for government ministries and the military.⁷ These deployments place the Company's technologies within a high-risk operational context, where data processing and AI capabilities may support security, intelligence, and operational decision-making. Following the October 7, 2023, Hamas attacks, a July 2025 UN report confirmed that Project Nimbus provided critical AI and cloud infrastructure to the Israeli military when its internal cloud system failed.⁸ Internal company documents further show that the company expanded services to the Israel Ministry of Defense and the Israel Defense Forces during the war to automate administrative tasks, enhance surveillance, and potentially support AI-driven targeting decisions.⁹ Finally, while the provided infrastructure also supports civilian applications, Israeli military official, Gaby Portnoy, publicly indicated Project Nimbus "play[s] a significant part in the victory" of its military operations.¹⁰

³ Scott Shane and Daisuke Wakabayashi, "The Business of War": Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018, <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>.

⁴ Deputy Secretary of Defense, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," memorandum, April 26, 2017, <https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf>.

⁵ Allison McDonald et al., "American Dragnet: Data-Driven Deportation in the 21st Century," Georgetown Law Center on Privacy & Technology, May 2022, updated 2025, <https://www.law.georgetown.edu/privacy-technology-center/publications/american-dragnet-data-driven-deportation-in-the-21st-century/>.

⁶ Ibid.

⁷ Steven Scheer, "Israel Picks Amazon's AWS, Google for Flagship Cloud Project," *Reuters*, April 21, 2021, <https://www.reuters.com/world/middle-east/israel-picks-amazons-aws-google-flagship-cloud-project-2021-04-21>.

⁸ Human Rights Council, *From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967*, Francesca Albanese, UN Doc. A/HRC/59/23 (June 30, 2025), <https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf>.

⁹ Gerrit De Vynck and Chris Dehghanpoor, "Google Rushed to Sell AI Tools to Israel's Military after Hamas Attack," *Washington Post*, January 21, 2025, <https://www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/>; Rabia Ali, "Project Nimbus Key Asset in Israel's War on Gaza, Occupied Palestine," *Anadolu Agency*, April 18, 2024, <https://www.aa.com.tr/en/middle-east/-project-nimbus-key-asset-in-israel-s-war-on-gaza-occupied-palestine-/3195224>.

¹⁰ Gerrit De Vynck, "Google rushed to sell tools to Israel after Hamas attacks," *The Washington Post*, January 21, 2025, <https://www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/>.

Furthermore, Alphabet's aggressive expansion into jurisdictions with poor human rights records—such as Saudi Arabia—demonstrates that governance risks are not confined to active conflict zones but are structural and jurisdictional. The Saudi government has a well-documented record of using digital infrastructure for unlawful surveillance and the suppression of dissenting voices, as well as weak protections against government access to, and exploitation of, personal data.¹¹ Investors require clarity on how Alphabet's stated AI Principles survive in jurisdictions where local laws require data access that directly contradicts the Company's human rights commitments.

2. Alphabet's Exposure to Sensitive Contexts Further Presents Material Risks

Alphabet's exposure to violations of international humanitarian law (IHL) and international human rights law through its customer's use of cloud, data, or AI services further raises material legal, regulatory, operational, and reputational risks that must be properly addressed. Alphabet has already faced millions of dollars in penalties and damages for privacy violations around the world. For example, the French regulator CNIL fined Google €50 million for inadequate transparency and consent practices, and a federal jury in *Rodriguez et al. v. Google LLC (N.D. Cal.)* awarded approximately \$426 million after finding Google unlawfully collected user data.

The deployment of already risky technologies in sensitive contexts presents even greater material risks. Where technologies are linked to military, intelligence, or security functions, Alphabet may face heightened exposure to retaliation, disruption, or reputational harm. Alphabet's infrastructure in geopolitically sensitive environments has faced infrastructure targeting, cyber threats, service disruption, and risks to personnel. In addition to infrastructure risks, Alphabet has faced physical and operational risks affecting facilities, contractors, and employees in geopolitically unstable regions, particularly in the event of escalation or conflict spillover. For example, in response to the U.S. military operations in Iran, Alphabet's Middle Eastern assets were specifically identified as potential targets for drone strikes in public statements and threats from the Iranian Revolutionary Guard.¹²

Internal pressures also create operational risks. In April 2026, hundreds of Google employees urged CEO Sundar Pichai to refuse to make the company's AI tools available for the Pentagon in classified settings. In an open letter, employees emphasized that Google's AI systems, used for military applications, could "cause irreparable damage to Google's reputation, business and role in the world."¹³ Google employees have previously called on the company to avoid providing technology services to agencies such as the U.S. Department of Homeland Security and ICE, citing concerns about human rights, surveillance, and civil liberties.¹⁴ Furthermore, the UN Special Rapporteur has called on the company to cease providing technology facilitating violations of IHL in the Occupied Palestinian Territory (OPT).

¹¹ SMEX, "AI Investments in the Gulf: Opportunities and Surveillance Risks," May 19, 2025, <https://smex.org/ai-investments-in-the-gulf-opportunities-and-surveillance-risks/>.

¹² "Enemy Technology Infrastructure: Iran Threatens Amazon, Google and Microsoft Assets in Middle East," *Euronews*, March 12, 2026, <https://www.euronews.com/next/2026/04/01/enemy-technology-infrastructure-iran-threatens-amazon-google-and-microsoft-assets-in-midd>; "Remote Work, Offices Shut as Tech Firms Respond to Escalating Middle East Tensions," *BBC News*, April 2, 2026, <https://www.bbc.com/news/articles/c99jlr7d40yo>.

¹³ Megan Cerullo, "Hundreds of Google Workers Urge CEO to Refuse Classified AI Work with Pentagon," *CBS News*, April 27, 2026, <https://www.cbsnews.com/news/google-ai-pentagon-classified-use-employee-letter/>.

¹⁴ Tonya Mosley, "Google Employees Call for Pledge Not to Work with ICE," *KQED*, August 15, 2019, <https://www.kqed.org/news/11767929/google-employees-call-for-pledge-not-to-work-with-ice>.

3. Material Changes in 2025/2026 Necessitate New Shareholder Action

Significant shifts in Alphabet's policies and the global regulatory landscape since the previous proxy season have created a new, urgent mandate for reporting. In February 2025, Alphabet removed key commitments from its AI principles, dropping previous pledges not to pursue technologies that could "cause or are likely to cause overall harm," including weapons development and surveillance tools.¹⁵ What was once a "red line" for the Company has been replaced by a discretionary framework, leaving investors with no objective metrics to assess when or how Alphabet will refuse to operate or sell products in high-risk contracts.

This erosion of principles is compounded by structural changes in oversight. While the Company points to its 2025 committee restructuring, the resulting Audit Committee and Risk & Compliance Committee charters notably removed existing language relating to civil and human rights oversight. The silence of these formal governing documents on AI and human rights—at a time when the Company has nearly doubled its AI infrastructure spend—constitutes a material governance gap.

Furthermore, the risks described in this proposal have evolved into systemic, cross-jurisdictional threats. As a globally important infrastructure provider, the failure to maintain enforceable safeguards in any single jurisdiction, whether the United States or abroad, creates a "contagion risk" for the Company's global reputation and its ability to withstand regulatory scrutiny across multiple markets.

4. Limited Visibility into Alphabet's End Use of Technology and Alphabet's Governance over These Risks

These risks are relevant to investors insofar as they may affect operational continuity, asset security, and the Company's ability to manage risks associated with higher-risk deployments. Alphabet provides limited disclosure regarding how it assesses and mitigates these risks, including whether conflict-sensitive risk assessments, contingency planning, and operational safeguards are in place to protect personnel and ensure continuity of services.

Investors also face limited visibility into how Alphabet monitors and governs downstream use once technologies are operational. As dual-use, highly scalable technologies, Alphabet's products and services are often difficult to monitor after deployment. Furthermore, the Company's technologies collect and process massive volumes of personal data across its services, and investors have limited insight into how it governs data collection, responds to government access requests, and manages risks associated with the use of data in surveillance or enforcement contexts.

These visibility constraints are particularly relevant in military, intelligence, and government deployments, where downstream operational use may be difficult to audit once systems are integrated into customer workflows. In the context of recent military operations widely criticized by legal scholars, including those in the OPT, Venezuela, and Iran, the need for this downstream visibility has never been more acute.

Alphabet maintains that its AI Principles, acceptable use policies, and multi-layered governance systems are sufficient to manage these risks. However, available evidence suggests these frameworks may not operate as enforceable constraints in sensitive deployments. For example, investigative reporting suggests that certain contract structures may further constrain provider discretion and cloud providers may have limited visibility into how sovereign customers use infrastructure, reducing their ability to detect misuse or intervene.¹⁶ In addition, some reporting highlights mechanisms that may reduce external visibility into data access in certain legal contexts, raising further questions about oversight and accountability.¹⁷

¹⁵ Miles Kruppa and Robert McMillan, "Google Quietly Revises AI Principles, Removing Categorical Ban on Harmful Applications," *Wall Street Journal*, February 4, 2025, <https://www.wsj.com/tech/ai/google-quietly-revises-ai-principles-removing-categorical-ban-on-harmful-applications-4c8d5f32>; Alphabet Inc., "Our AI Principles," archived February 2025 (comparing 2024 and 2025 versions), <https://ai.google/responsibility/principles/> (accessed May 4, 2026).

¹⁶ Billy Perrigo, "Exclusive: Google Contract Shows Deal with Israel Defense Ministry," *Time*, April 12, 2024, <https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war>.

¹⁷ Julia Carrie Wong, "Revealed: Israel Demanded Google and Amazon Use Secret 'Wink' to Sidestep Legal Orders," *Guardian*, October 29, 2025, <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>.

These constraints are not limited to contractual terms but may also arise from operational integration. In high-pressure environments, conditions may compress decision timelines, increasing reliance on probabilistic data and automated outputs, which raises the likelihood that errors translate into real-world harm. In such jurisdictions, companies may also face legal obligations to provide data access, limited oversight mechanisms, and constraints on challenging government requests. These conditions create a structural tension between Alphabet's stated commitments to user rights and the realities of operating in environments where government authority may supersede company policy.

Furthermore, while Alphabet's acceptable use policies prohibit uses that may cause harm, violate legal rights, or enable harmful surveillance or targeting, reporting indicates that in large-scale government deployments, providers may have limited ability to monitor downstream use or intervene once systems are operational, particularly where contractual structures or jurisdictional constraints limit enforcement.¹⁸

Alphabet has publicly committed to responsible AI and to respecting human rights, but investors have limited visibility into whether these commitments are consistently operationalized in high-risk contexts. Given the 2025 shift toward a more discretionary, risk-based framework,¹⁹ investors must rely almost exclusively on the Company's contractual safeguards, escalation mechanisms, and governance structures to assess how risks are managed in practice. Currently, there is insufficient disclosure to determine whether mitigation measures are accurately defined, implemented, or effective.

These dynamics raise a central governance question: whether Alphabet retains sufficient control and enforcement capability to ensure that its technologies are used in accordance with its own policies in high-risk, high-harm contexts. Taken together, these factors suggest that Alphabet's governance framework may describe intended safeguards but does not provide investors with sufficient evidence that those safeguards are enforceable in practice.

The Proposal seeks disclosure that would enable investors to assess whether Alphabet's governance, escalation, and enforcement mechanisms are sufficient to ensure that its stated policies are implemented consistently and effectively in practice.

5. CURRENT BOARD OVERSIGHT MAY NOT MATCH RISK EXPOSURE

Alphabet states in its Opposition Statement that oversight of AI-related risks is addressed at the Board and Audit and Compliance Committee levels. However, public disclosures provide limited clarity on how these governance structures are aligned with the Company's expanding exposure to high-risk AI and cloud deployments. For example, Alphabet does not disclose how high-risk contracts are escalated for Board or committee review, what criteria trigger heightened review or intervention, whether directors review deployment-specific risk assessments, or how the Board monitors whether mitigation measures are implemented and effective in practice.

¹⁸ Dhruv Mehrotra, "The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military," *WIRED*, July 10, 2024, <https://www.wired.com/story/google-amazon-project-nimbus-israel-military>.

¹⁹ Google, "AI Principles," updated February 4, 2025, <https://ai.google/principles>; Naomi Tiku and Gerrit De Vynck, "Google Drops Pledge Not to Use AI for Weapons or Surveillance," *Washington Post*, February 4, 2025, <https://www.washingtonpost.com/technology/2025/02/04/google-ai-policies-weapons-harm/>; Dan Milmo, "Google Owner Drops Promise Not to Use AI for Weapons," *Guardian*, February 5, 2025, <https://www.theguardian.com/technology/2025/feb/05/google-owner-drops-promise-not-to-use-ai-for-weapons>.

Critically, the Audit and Compliance Committee charter does not explicitly reference AI governance or the management of dual-use technologies, despite AI being the primary driver of Alphabet's growth and risk profile. This silence in the Company's formal governing documents constitutes a structural oversight gap.

Investors currently lack sufficient evidence to assess whether Alphabet's governance systems are effective in practice, specifically regarding identifying high-risk deployments, maintaining enforceable controls, monitoring downstream use, and responding appropriately to escalation signals. Under widely recognized frameworks such as the United Nations Guiding Principles on Business and Human Rights, companies are expected to conduct due diligence that is ongoing, risk-based, and integrated into decision-making processes. Where companies lack the ability to enforce safeguards in practice, it signals a material governance gap.

Furthermore, providing a report on the effectiveness of Alphabet's policies and practices will not impede the Company's ability to engage in new contracts or otherwise negatively impact the bottom line. In contrast, a report identifying gaps in Alphabet's governance will only serve to ensure the Company is mitigating risks that could otherwise lead to financial impact.

CONCLUSION

The central question for investors is whether Alphabet retains enforceable safeguards in high-risk deployments. While the Company maintains that policies and governance frameworks are in place, available evidence raises questions about whether those safeguards are consistently operationalized and enforceable in practice, particularly in large-scale government, military, and high-risk jurisdictional contexts.

This proposal does not seek to prescribe operational decisions. Rather, it requests disclosure sufficient for investors to assess whether Alphabet's governance, oversight, and control systems function effectively when risks materialize. A vote "AGAINST" this proposal is an argument for continued opacity in a year where AI risk has reached an inflection point. **A vote FOR this proposal supports improved transparency and enables investors to evaluate whether Alphabet's governance systems are adequately aligned with its risk exposure and fiduciary responsibilities.**

Additional note: The Anti-Defamation League (ADL) and its affiliate JLens have filed an exempt solicitation that mischaracterizes Proposal 11 in an attempt to distract fellow shareholders from material and legal risks by injecting highly politicized and divisive rhetoric into a standard corporate governance matter.²⁰ In a political attack that seeks to undermine the very accountability that corporate governance exists to enforce, the ADL and JLens claim Proposal 11 is designed to stigmatize Alphabet's commercial relationships with a single nation. This claim is factually unsupported and intellectually dishonest. The request clearly seeks greater insights into Alphabet's governance processes covering multiple high-risk and sensitive contexts globally, as Alphabet is an infrastructure provider for governments and security systems across the world. Nothing in the proposal requests a specific assessment of Alphabet's role in Project Nimbus, but rather an objective analysis of the Company's risks regarding its customers' end use.

²⁰ JLens, "The Case to Vote Against Proposal 11: Shareholder Proposal Regarding a Report on Data Privacy on Alphabet's 2026 Proxy Statement," May 1, 2026, <https://www.jlensnetwork.org/the-case-to-vote-against-proposal-11-shareholder-proposal-regarding-a-report-on-data-privacy-on-alphabets-2026-proxy-statement>; JLens, "The Case to Vote Against Proposal 7: Shareholder Proposal Requesting Report on Defense-Related Products on GE Aerospace's 2026 Proxy Statement." April 13, 2026. <https://www.jlensnetwork.org/the-case-to-vote-against-proposal-7-shareholder-proposal-requesting-report-on-defense-related-products-on-ge-aerospaces-2026-proxy-statement>.

This attack on Proposal 11 is part of a predictable, repeatable playbook JLens uses to obstruct shareholder processes across multiple major corporations. Whether opposing data privacy at Alphabet, or human rights due diligence reporting at Intel and GE Aerospace, JLens consistently relies on *ad hominem* attacks and “guilt by association” claims to falsely rebrand standard governance requests as malicious “BDS” campaigns.²¹ By doing so, JLens manufactures a “single-nation” focus while deliberately ignoring the global scope of the proposals. Just as proponents at GE Aerospace pointed out when facing an identical attack, JLens ignores the global and systemic scope of the proposal in favor of a “narrow political narrative.”

This tactic ignores the reality at Alphabet: Proposal 11 is backed by a coalition of 34 co-filers representing over \$2.2 billion in Alphabet shares, and a broader group of over 40 institutional investors representing \$1.15 trillion in assets under management who have formally raised these exact governance concerns with the Board.²²

With a more than 25-year history as a sustainable investment manager, Zevin has consistently sought to align its investment strategy with rights-respecting principles and risk minimization across all geographic exposures, having led or participated in shareholder engagements on human rights risks in diverse contexts including China, Myanmar, Russia, Ukraine, Saudi Arabia, India, and the U.S.-Mexico border. Rather than addressing whether Alphabet retains sufficient Board-level oversight and escalation mechanisms to manage the risks of deploying AI and cloud technology in surveillance and military contexts, JLens offers no evidence that Alphabet's oversight of customer data is sufficient. In repeating these attacks, JLens is engaging in an obvious effort to obstruct shareholders from supporting an objective, globally recognized framework. By opposing this resolution, JLens is effectively arguing that Alphabet should be exempt from standard human rights due diligence. If the questions raised in our proposal about the material financial risks of global data governance constitute a targeted attack on a single region, the ADL's argument has already collapsed.

CONTACT DETAILS

For questions, please email marcela@zevin.com.

IMPORTANT NOTICE:

The views expressed are those of the authors as of the date referenced and are subject to change at any time based on market or other conditions. These views are not intended to be a forecast of future events or a guarantee of future results. These views may not be relied upon as investment advice. The information provided in this material should not be considered a recommendation to buy or sell any of the securities mentioned. It should not be assumed that investments in such securities have been or will be profitable. To the extent specific securities are mentioned, they have been selected by the authors on an objective basis to illustrate views expressed in the commentary and do not represent all of the securities purchased, sold or recommended for advisory clients. 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.

²¹ JLens, "The Case to Vote Against Proposal 7: Report on Intel's Human Rights Due Diligence Process on Intel's 2026 Proxy Statement," March 30, 2026, <https://www.jlensnetwork.org/the-case-to-vote-against-proposal-7-report-on-intels-human-rights-due-diligence-process-on-intels-2026-proxy-statement>.

²² Steven Scheer, "Alphabet Investors Push Safeguards on Use of Its Cloud, AI Tech," *Reuters*, April 29, 2026, <https://www.reuters.com/sustainability/boards-policy-regulation/alphabet-investors-push-safeguards-use-its-cloud-ai-tech-2026-04-29>.