

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. (the Company) 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.

Alphabet's business model depends heavily on the processing and storage of user and enterprise customer data across Google Services and Google Cloud. When customers misuse Google products, or when the Company's own data-governance practices contradict their terms of service, Alphabet risk exposure includes:

- Operational risk when misuse triggers regulatory intervention, including mandated tool restrictions, audits, or requirements to modify or localize cloud infrastructure. For example, Google settled a lawsuit in 2023 alleging that the Company collected personal information from users browsing with Chrome's "incognito mode."¹
- Reputational risks tied to data access and misuse in jurisdictions with expansive government access to personal data. Misuse of Google Cloud infrastructure can lead to violations of service-level agreements or data-processing terms if cloud tools are misused by customers or accessed by government actors beyond terms of service. For example, Google's participation in Project Nimbus may not align with its data-governance principles that prohibit uses that "violate, or encourage the violation of, the legal rights of others," or for any "invasive" purpose, or anything "that can cause death, serious harm, or injury to individuals or groups of individuals."² By accepting alert mechanisms and contract terms that limit Google's ability to restrict governmental use of its cloud services, the Company appears to conflict with its acceptable use policy.³
- Regulatory penalties leading to fines under the European Union's General Data Protection Regulation (GDPR) of up to 4% of global annual revenue.⁴ Google has already faced major GDPR actions, including a €50 million fine from France's data protection authority for inadequate transparency and consent processes.⁵
- Litigation and class-action exposure when data is collected, processed, or accessed in ways inconsistent with user expectations or product disclosures. For example, in 2025, a U.S. federal jury ordered Google to pay US\$425 million in damages for violating the privacy rights of almost 100 million users who alleged Google continued collecting device and usage data after they disabled tracking settings.⁶

¹ <https://www.theguardian.com/technology/2024/apr/01/google-destroying-browsing-data-privacy-lawsuit>

² <https://cloud.google.com/terms/aup>

³ <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>

⁴ <https://gdpr-info.eu/issues/fines-penalties/>

⁵ https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

⁶ <https://news.bloomberglaw.com/class-action/google-violated-privacy-of-nearly-100-million-users-jury-finds>

Alphabet's current risk disclosures address data security, government access, and reputational exposure but do not discuss downstream risks associated with customer deployments of Google Cloud or scenarios in which government access requirements or custom contracting terms may substantially increase risk. Shareholders would benefit from greater transparency into Google's protocol to comply with its own privacy and data protection standards.