

RESOLVED: Shareholders request that the Board of Directors commission an independent third-party report, at reasonable expense and excluding proprietary information, on NVIDIA Corporation's (NVIDIA) customer due diligence process to determine whether customers' use of its products or services with surveillance technology and artificial intelligence (AI) capability or of its components that support autonomous military and police vehicles, contributes to human rights harms.

WHEREAS: NVIDIA's Code of Conduct commits the company to, "complying with all applicable laws; respect internationally recognized human rights where we operate" and "not engaging in ... forced, bonded, or indentured labor"¹;

Human rights risks are acute in conflict-affected and high-risk areas (CAHRA), characterized by widespread human rights abuses and violations of national or international law.² Surveillance technologies and autonomous vehicles are associated with human rights and material risks, as evidenced by stakeholder efforts to limit, place moratoriums on, and/or ban certain products and services;

NVIDIA is providing products and services to customers in CAHRA that are contributing to human rights harms, including:

1. Selling microchips to Urumqi Cloud Center in Xinjiang Uyghur Autonomous Region, used by the Chinese government to surveil, detain, and force into labor, ethnic Uyghurs;³
2. Partnering with and investing in AnyVision, whose facial recognition technology is used to surveil Palestinians in the occupied West Bank and East Jerusalem;⁴
3. Building an AI and deep learning cloud infrastructure with Saudi Telecom Company, implicated in the surveillance and detention of human rights defenders in Saudi Arabia;^{5,6} and,
4. Partnering with the U.S. Department of Defense to accelerate the adoption of fully autonomous military vehicles;^{7,8}

Human rights and conflict are material risks. According to US SIF's *2020 Trends Report*, conflict risk was the leading environmental, social, and governance criterion among investors representing over \$6 trillion in assets under management.⁹ Companies have mitigated the risks of surveillance

¹ <https://www.nvidia.com/content/dam/en-zz/Solutions/about-us/documents/NVIDIA-Code-of-Conduct-external.pdf>

² <http://dx.doi.org/10.1787/9789264185050-en>

³ <https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html>

⁴ <https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf>

⁵ <https://www.hpcwire.com/off-the-wire/stc-and-nvidia-team-up-to-build-saudi-arabias-first-ai-and-deep-learning-cloud-infrastructure/>

⁶ <https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us>

⁷ <https://www.aerodefensetech.com/component/content/article/adt/features/articles/35360>

⁸ <https://www.mrcy.com/capabilities/partners/nvidia>

⁹ <https://www.ussif.org//Files/Trends/2020%20Trends%20Report%20InfoGraphic%20-%20Institutional%20Investors.PDF>

technologies, including Microsoft's divestment from AnyVision and exit from the facial recognition market¹⁰ and Amazon's moratorium on police using its "Rekognition" software;¹¹

Policymakers are responding to risks with regulation, legislation, and public calls, including American states and cities limiting or banning the use of facial recognition by police,¹² U.S. Presidential executive orders prohibiting investment in Chinese surveillance companies,¹³ and the European Union's Dual Use Regulation¹⁴ and Artificial Intelligence Act;¹⁵

To mitigate risks associated with customer conduct, leading companies conduct "Know Your Customer" (KYC) due diligence. The process helps determine if a company's products and services may be used to facilitate human rights harms. In November 2021, the Atlantic Council recommended the United States and NATO develop KYC policies for companies in the surveillance industry.¹⁶

SUPPORTING STATEMENT

Shareholders seek information, at board and management discretion, through a report that:

- Discusses how human rights risks in CAHRA are identified, assessed, prevented, and mitigated; and
- Assesses if a customer due diligence process is needed to address these risks.

¹⁰ <https://www.reuters.com/article/us-microsoft-anyvision/microsoft-to-divest-anyvision-stake-end-face-recognition-investing-idUSKBN21E3BA>

¹¹ <https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/>

¹² <https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175>

¹³ <https://www.washingtonpost.com/technology/2021/06/03/investment-ban-chinese-surveillance-tech/>

¹⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821>

¹⁵ <https://www.eipa.eu/publications/briefing/the-artificial-intelligence-act-proposal-and-its-implications-for-member-states/>

¹⁶ <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/>