

Amazon Web Services markets and sells to government a facial recognition system (Rekognition), that may pose significant financial risks due to privacy and human rights implications;

Human and civil rights organizations are concerned facial surveillance technology may violate civil rights by unfairly and disproportionately targeting and surveilling people of color, immigrants and civil society organizations;

Nearly 70 organizations asked Amazon to stop selling Rekognition, citing its role enabling “government surveillance infrastructure”;

The American Civil Liberties Union found Rekognition matched 28 members of Congress, incorrectly identifying them as individuals who have been arrested for a crime, then found Rekognition falsely matched 1 in 5 California lawmakers. Other research shows Rekognition is worse at identifying black women than white men and misgenders nonbinary people;

Multiple cities and states have banned government facial technology. In 2021, a federal ban was reintroduced, and United Nations High Commissioner for Human Rights urged a moratorium on the sale and use of artificial intelligence systems until adequate safeguards exist, also calling for a ban on artificial intelligence applications inconsistent with international human rights law.¹

There is little evidence our Board of Directors, as part of its fiduciary oversight, has rigorously assessed risks to Amazon’s financial performance, reputation and shareholder value associated with privacy and human rights threats to customers and stakeholders;

For 3 years, similar Amazon proposals have received increasing shareholder support. In 2021, it received 34.3 percent support.

Responding to the growing movement against police brutality and criminal justice bias, Amazon issued an indefinite moratorium on Rekognition for use by police departments. While this ban indicates acknowledgment of Rekognition’s risks, it is unclear whether it includes other government agencies. A 2021 Government Accountability Office report

¹ [OHCHR | Artificial intelligence risks to privacy demand urgent action – Bachelet](#)

found 19 of 24 United States government agencies surveyed were using some form of facial recognition.²

Microsoft banned face recognition sales to police awaiting federal regulation, while IBM stopped offering the software. Following a lawsuit alleging nonconsensual use of facial recognition on residents resulting in a \$550 million settlement with Illinois, Facebook recently declared it will cease using facial recognition.³

RESOLVED: Shareholders request the Board of Directors commission an independent study of Rekognition and report to shareholders regarding:

- The extent to which such technology may endanger, threaten or violate privacy and/ or civil rights, and unfairly or disproportionately target or surveil people of color, immigrants and activists in the United States;
- The extent to which such technologies may be marketed and sold to authoritarian or repressive governments, including those identified by the United States Department of State Country Reports on Human Rights Practices;
- The potential loss of good will and other financial risks associated with these human rights issues;

The report should be produced at reasonable expense, exclude proprietary or legally privileged information and be published no later than September 1st, 2022.

² [Facial Recognition Technology: Current and Planned Uses by Federal Agencies | U.S. GAO](#)

³ <https://www.theguardian.com/technology/2021/nov/03/why-is-facebook-shutting-down-its-facial-recognition-system-and-deleting-faceprints>