**RESOLVED**, Shareholders request the Board of Directors commission an independent third-party report, at reasonable cost and omitting proprietary information, assessing Amazon's process for customer due diligence, to determine whether customers' use of its surveillance and computer vision products or cloud-based services contributes to human rights violations.

**WHEREAS,** the use of Amazon's surveillance technology and cloud services in law enforcement and immigration contexts that have existing systemic inequities may replicate, exacerbate, and mask these inequities.[1]It may also compromise public oversight and contribute to widespread government surveillance. According to the UN Special Rapporteur on freedom of opinion and expression, surveillance tools may "interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation."[2]

Government contracts for cloud services and surveillance technology, which lack transparency, are an increasing revenue source for Amazon Web Services (AWS), growing tenfold in five years.[3]AWS is mission-critical for government agencies. Amazon's partnership with Palantir, the subject of employee and customer protests, enables Immigration and Customs Enforcement to identify, detain, and deport individuals and families, often violating human rights.[4]

Companies use "Know Your Customer" (KYC) due diligence to evaluate and mitigate clients' potential risks. For example, financial services companies use KYC to prevent money laundering. Companies selling high-risk technologies might consider using similar processes, with participation from civil rights experts and impacted stakeholders, to assess customers' suitability, human rights record, and likely end use of products.

Amazon's surveillance technologies compound historical and systemic inequity, including disproportionate use of surveillance on communities of color, even if used according to Amazon's guidelines. Customers may use technologies in ways Amazon warns against, as happened with an Oregon Sherriff's office use of Rekognition,[5]and this may violate rights.

Amazon partners with over 600 police departments, providing police with access to Ring doorbell video surveillance data. Amazon is contemplating integrating face surveillance capabilities into Ring.[6]Senator Markey's investigation on Ring found Amazon has "no oversight/compliance mechanisms" to protect consumers' privacy rights.[7]Amazon's Neighbors application allows customers to post Ring footage, which police may request or subpoena. While Neighbors prohibits discrimination,

racist speech is prevalent.[8]Ring and Neighbors blur the line between private and government functions and enable a climate of fear and distrust by misleading customers to believe crime rates exceed actual levels.

While Amazon has adopted a Human Rights Policy, it lacks information on embedding, independent oversight, and applicability to end users. Amazon fails to disclose Conditions of Use agreements, efforts to evaluate customer compliance therewith, or analysis of said agreements' effectiveness at preventing harmful use.

Inadequate due diligence around customers' use of surveillance and cloud technologies presents privacy and data security risks, which the Sustainability Accounting Standards Board identifies as material for E-Commerce companies.

Amazon is responsible for ensuring its customers do not use surveillance and cloud products to violate human rights.