Notice of Exempt Solicitation
Pursuant to Rule 14a-103

Name of the Registrant: Amazon.com

Name of persons relying on exemption: The Sisters of St. Joseph of Brentwood; American Baptist Home Mission Society; Maryknoll Sisters; Province of St. Joseph of the Capuchin Order (Midwest Capuchins); Sisters of Charity of St. Elizabeth, NJ; Sisters of St. Francis of Philadelphia; Sisters of St. Joseph of Peace, NJ; Sisters of the Holy Names of Jesus and Mary, US Ontario Province; and Unitarian Universalist Association.

Address of persons relying on exemption: Investor Advocates for Social Justice (formerly Tri-State Coalition for Responsible Investment), 40 S Fullerton Ave Montclair, NJ 07042

Written materials are submitted pursuant to Rule 14a-6(g) (1) promulgated under the Securities Exchange Act of 1934. Submission is not required of this filer under the terms of the Rule, but is made voluntarily in the interest of public disclosure and consideration of these important issues.

The proponents urge you to vote FOR the Shareholder Proposal calling for a Report on Customer Due Diligence, Item 6 at the Amazon Annual Meeting of Shareholders on May 27, 2020.
Summary of the Proposal

Item 6 asks Amazon to commission an independent third-party report assessing its 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.

Support for this Proposal is warranted because:

1. Amazon sells products and services that pose risks to human rights, including civil rights. Products posing high risk in the hands of Amazon customers include the Ring Doorbell and the Neighbors App, facial recognition surveillance technology, and elements of Amazon Web Services. These products may be used to further discrimination in policing, infringe on privacy, or violate civil liberties.
2. Failure to have an effective system to monitor customers’ use of products and services exposes Amazon to legal, financial, human capital, and regulatory risks, as well as loss of consumer trust. Legislators, customers, and potential employees have requested increased oversight.
3. Amazon’s current systems for oversight of customer use of its high-risk products are insufficient to address potential risks.
4. Increased customer due diligence would mitigate risks to human rights, including civil rights. The request is for a report to describe the process and management systems to demonstrate that they are effective, rather than provide specific information about each customer.

Rationale for Support of the Proposal

1. Amazon.com is best known as the world’s largest e-commerce platform. But the company has expanded rapidly with the introduction of new technology products and services that raise serious concern for their actual or potential role in violating civil and human rights.

Those products and services include:

- Amazon Web Services (AWS) is by far the largest provider of Internet “cloud” services in the world, with 2019 revenue of $35 billion.¹ AWS currently provides cloud services for over 6,500 U.S. government agencies, including the Department of Defense and the U.S. intelligence community, as well as for governments and government agencies internationally.²
- Rekognition is a facial surveillance technology app marketed through AWS.³
- Ring⁴ is a home security and “smart home” company purchased by Amazon in 2018 for approximately $839 million.⁵ While Amazon does not disclose sales for Ring, the company has acknowledged that “Ring has millions of users.”⁶ Ring’s online sales in the U.S. grew 180 percent in December 2019 compared with a year earlier, with monthly sales of nearly 400,000 devices, according to Jumpshot, a data analytics firm.⁷
- Neighbors is a social media application targeting Ring customers which “enables community members – and, in some cases, law enforcement – to work together in order to reduce crime,” according to the company.⁸
In addition, Amazon markets the Echo, Dot, and Alexa smart speakers which use a voice-control system. The company has also applied for patents on technologies that would expand the use of facial recognition technology. Specifically, Ring is seeking to patent a technology to identify a partial facial image by combining images from two or more cameras, a powerful surveillance tool that can be used by neighborhood watch groups or municipal camera systems.

2. Amazon’s due diligence systems do not adequately ensure oversight of customer use of its technology and surveillance products, which may be used in ways that threaten civil and human rights and present material risks.

   A. Customer due diligence processes are used by companies in a number of sectors to evaluate risks associated with potential clients in order to prevent and mitigate possible misuse of products and services.

   The lack of robust customer due diligence mechanisms exposes Amazon to increased regulatory risks. For example, in April 2020, in the midst of the COVID-19 pandemic, European Commissioner for Justice Didier Reynders announced that the European Commission will introduce legislation in 2021 to make human rights due diligence mandatory for EU companies. This will align with expectations in the UN Guiding Principles on Business and Human Rights. Amazon has substantial business interests in the EU and will therefore be required to identify, prevent, mitigate and account for its human rights impacts. This comes weeks after investors with $5 trillion in assets under management released a statement in support of this growing momentum, calling on governments to put in place regulatory measures to require mandatory human rights due diligence. Amazon has substantial business interests in the EU and will therefore be required to identify, prevent, mitigate and account for its human rights impacts. This comes weeks after investors with $5 trillion in assets under management released a statement in support of this growing momentum, calling on governments to put in place regulatory measures to require mandatory human rights due diligence. Customer due diligence and oversight is appropriate given the nature of the products being used, the high likelihood of potential harm, and the severity of the harm that may be caused. Impacts may interfere with rights to privacy, freedom of expression, rights to association and assembly, religious beliefs, non-discrimination, and public participation. The requested disclosure would describe the customer due diligence processes and are analogous to Know Your Customer processes used in other sectors such as banking or finance. In spite of the existing systems that Amazon points to in its Statement of Opposition to the Proposal as sufficient, given the prevalence and frequency of data breaches, and infringement on human rights including privacy, as outlined below, it is clear that existing systems are ineffective at managing the risks.

   B. Amazon’s customers’ use of its tech products and services present civil and human rights risks. Failure to manage these risks presents material regulatory, legal, human capital management, and risks to consumer trust. It has not adequately addressed critical questions raised by legislators and the public about these risks.

   For E-Commerce and Software & IT companies such as Amazon, the Sustainability Accounting Standards Board (SASB) has identified Privacy and Data Security as issues that are financially “material.” In the related Sustainability Accounting Standard, SASB provides a “minimum set of industry-specific disclosure topics reasonably likely to constitute material information”, including “how management or mismanagement of each topic may affect value creation.” To measure a company’s performance for each topic, SASB provides a “set of quantitative and/or qualitative accounting metrics.” For example, SASB requires that such companies describe their due diligence practices and procedures with respect to data security, including “Description of approach to identifying and addressing data security risks” and for privacy including, “Number of users whose information is used for secondary purposes” and “Description of policies and practices relating to behavioral advertising and user privacy.” Disclosure on these metrics is lacking.
Amazon is the subject of significant negative public attention which threatens its reputation, ability to attract and retain employees, and maintain public trust.

It is failing to take meaningful steps to address the problems identified by critics in the following areas:

**AWS** - Amazon’s contract with AWS customers associated with human rights violations may negatively impact the company’s ability to recruit top talent. Amazon faces backlash from employees and the public over its direct and indirect ties to human rights violations carried out by U.S. Immigration and Customs Enforcement (ICE). Amazon’s contract with Palantir Technologies, an AWS customer accused of enabling ICE’s human rights abuses, is particularly controversial, and has prompted public opposition from hundreds of employees. Thousands of students at dozens of top universities—including Stanford, M.I.T., U.C. Berkeley and other schools Amazon relies on for talent—have protested recruitment fairs over their refusal to work in tech company roles that enable harmful immigration enforcement in the United States. In September 2019, Harvard students protested at Amazon’s recruitment booth on campus saying, “Working for any company that is contributing to these evils is a choice.”

**RING** - Ring poses reputational, human capital, legal and regulatory risk due to customer’s use of its products for surveillance, and due to customers’ ability to abuse the company’s apparently poor cybersecurity and data privacy protocols.

Ring faces a $5 million class action lawsuit over its failure to keep customers safe from cyberattacks. Customers of Ring cameras have experienced racist attacks, ransom demands, harassment and threats, including attacks targeted at children, posing reputational and legal risk for the company. In 2020, an Amazon engineer stated publicly that: “[Ring’s] privacy issues are not fixable with regulation and there is no balance that can be struck. Ring should be shut down immediately.” The fact that Ring has even fired its own employees for watching customers’ videos demonstrates the security vulnerabilities with its products.

In December 2019, nine national consumer advocacy groups issued a Ring product warning, creating reputational risk for the company. The warning stated: “The dangers associated with these products pose a threat to families and the public. As groups dedicated to protecting consumers’ privacy and safety, we are issuing this official product warning: Do not buy Amazon Ring cameras.”

**The use of Ring and the connected Neighbors app by hundreds of local police department ‘partners’ and millions of Ring customers, poses civil rights risks.**

The supposedly mutually beneficial relationship between police and Ring leaves potentially impacted individuals vulnerable in the absence of clear guidance, oversight, and accountability over potential misuse by customers and secondary users. Police are able to ask Ring customers for access to their data. Ring benefits as police and local governments advertise Ring products. In 2019, someone identified as a Houston police officer posted on the social media app NextDoor: “The Houston Police Department has teamed up with Ring to fight crime...I will host a meeting...and give a presentation on the app Neighbors...I will also be handing out the Ring doorbell cameras.”
These Ring-police partnerships present civil rights and civil liberties concerns: according to the Electronic Frontier Foundation, even if Ring customers choose not to give police the option of contacting them for their data, police may still gain access to customer data by delivering a warrant to Amazon. Reports suggest Ring is considering adding facial recognition technology, Rekognition, to its products.

In November 2019, five U.S. senators wrote to Amazon CEO Jeff Bezos requesting information about Ring’s data security practices. They wrote: “If hackers or foreign actors were to gain access to [Ring] data, it would not only threaten the privacy and safety of the impacted Americans; it could also threaten U.S. national security.”

U.S. Senator Ed Markey (D-MA)’s 2019 investigation of Ring found it to be “an open door for privacy and civil liberty violations,” noting the company’s lack of due diligence, specifically: “[Ring has] no oversight/compliance mechanisms in place to ensure that users don’t collect footage from beyond their property…. to ensure that users don’t collect footage of children…. to prohibit law enforcement from requesting and obtaining footage that does not comply with Ring’s Terms of Service.”

In addition to threatening public safety by presenting civil rights and civil liberties issues, Ring police partnerships also do not deliver on their intended purpose of lowering crime rates in neighborhoods — and may even have the opposite effect. In March 2020, CNET secured property-crime statistics from three of Ring’s police partners in Wisconsin, Illinois and Florida, and compared monthly theft rates before and after police began using the technology. They found that Ring had “minimal impact...The data shows that crime continued to fluctuate, and analysts said that while many factors affect crime rates, such as demographics, median income and weather, Ring’s technology likely wasn’t one of them.” CNET also noted that police partnering with Ring agreed that the product did nothing to slow crime. In 2018, the M.I.T. Technology Review conducted an independent review of Amazon’s 2015 claim that a police pilot of Ring reduced burglaries in neighborhoods by “as much as 55%”, disputing that claim and noting instead that “the only study carried out independently of Ring found that neighborhoods without Ring doorbells were actually less likely to suffer break-ins than those with them.” Furthermore, MIT noted that “though burglary rates dropped over a 10-month period, it was a 42% reduction, not the 55% in six months that Ring claims. Within a year after the study, that neighborhood saw its most burglaries in seven years.” Ultimately, “concerns over the company’s handling of user privacy led CNET to withdraw our recommendations of Ring products across the board.”

**REKOGNITION** - Rekognition is an AWS facial recognition technology that allows customers to “perform face verification... by comparing a photo or selfie with an identifying document such a driver's license” and to “understand the average age ranges, gender distribution and emotions expressed by the people, without identifying them.”

Amazon has disputed numerous studies that have found Rekognition to be racially biased and inaccurate, misidentifying people of color at far higher rates than white people. In the hands of Rekognition’s police customers, racially biased facial recognition technology could exacerbate existing systemic racial injustice in the criminal justice system. This includes the frequency of police disproportionately targeting people of color for crimes they did not commit, something the technology may facilitate, posing civil rights concerns.
Congress has held multiple hearings on oversight of facial recognition to examine private sector use, potential transparency, privacy, accuracy, ownership, and security implications involved in its use and the partnerships companies develop with government entities, and potential legislative solutions. Lawmakers have questioned whether the technology should be used at all, even if it is 100% accurate. In part due to misuse and inadequate oversight, there is a growing movement to ban facial recognition technology nationwide. Multiple jurisdictions have completely banned government use of the technology. California has enacted a 3-year moratorium on police use of facial recognition technology on police body cameras. In January, dozens of leading consumer, privacy, and civil liberties organizations wrote to the Congressional Privacy and Civil Liberties Oversight Board to “recommend to the President and the Secretary of Homeland Security the suspension of facial recognition systems.” Poor oversight and management may threaten the future of this business.

Amazon’s lack of oversight of customer usage of its products could hinder customers’ trust and comfort with Amazon platforms.

In 2019, a class action lawsuit alleged AWS was culpable for a Capital One data breach that impacted over 106 million people, arguing Amazon knew, but did nothing to address, a security vulnerability exploited by the hacker. Also last year, thousands of patients were impacted by a security breach of AWS customer Sunshine Behavioral Health; reports indicate that even after the customer was notified of the breach, files remained exposed on the AWS platform. Recently thousands of Zoom meeting cloud recordings with personal and intimate information that were stored on an unprotected AWS platform were exposed on the web.

C. There are gaps in Amazon’s processes to ensure its surveillance and tech products are not being used by customers in ways that threaten civil and human rights.

Customer due diligence would ameliorate this.

There are significant gaps in Amazon’s existing practices to oversee customer use of its products and services. If Amazon implemented customer due diligence processes for high risk products, this would provide assurance to shareholders that Amazon is managing potential risks associated with customer use and is well positioned to meet evolving regulatory expectations.

Such due diligence processes might include disclosure of relevant information such as:

- The terms of customer use agreements, what constitutes a violation of use agreements, and whether these use agreements are binding;
- The scope of risks covered (e.g. data security, privacy, discrimination including based on ethnicity and race, ineffective use by not following directions, etc.);
- How Amazon conducts oversight to ensure compliance, especially, though not only in relation to, customers’ privacy rights. The conditions under which the company investigates violations of the AWS Acceptable Use Policy, which it indicates it has the right, but not the obligation to do;
- How someone would determine if they experienced a harm that was caused by an Amazon product, and whether method they could use to file a complaint is accessible and effective; and
- The measures Amazon takes if a customer uses a product or service in a way that violates the use agreement and how frequently it enforces use agreements to terminate customer access.

While AWS may provide guidance on best practices for use of facial surveillance technology, it is not clear if there are ramifications for customers or consequences when a customer does not follow that guidance that would prevent future harm, or if there are guardrails in place to ensure that failure to follow the guidance does not violate human rights.
In fact, Amazon recognizes the importance of due diligence in its relationships with customers and vendors on its e-commerce platform. But the company has failed to adopt robust due diligence for surveillance products and AWS, which is the company’s fastest growing business unit and where risks to privacy and security associated with secondary purposes are significant.

Due diligence has been a long-standing practice in Amazon’s e-commerce platform and is expanding. According to multiple media reports, Amazon is piloting new “seller-verification processes” aimed at validating the identity of third-party sellers over video conferencing. Amazon claims seller-verification stopped 2.5 million suspected bad actors from publishing their products on Amazon’s platform in 2019. The system analyzes “hundreds of different data points to identify potential risk,” with the sellers’ applications reviewed by trained investigators before being approved.48

- In its Opposition Statement, Amazon points to its Terms of Use Agreements, but does not disclose how these are monitored or enforced, which fails to address the central question of the proposal.

Given the sensitive nature of content (e.g. biometric data, video footage inside the home) on the AWS platforms and other services, Amazon has a heightened responsibility to monitor customer use of what it calls “computer vision” products and services. Yet that is not the case with the Ring doorbell technology, for example. In response to questions about Ring posed by Senator John Markey, Amazon’s Vice President for Public Policy, Brian Huseman, wrote:

“Ring’s Terms of Service state that users are responsible for their use of our products and services, including use in accordance with any applicable privacy laws. Ring does not view users’ videos to verify compliance with its Terms of Service.”49

And in response to a question from Sen. Markey regarding security measures for video obtained from customers by law enforcement, Amazon said:

“Each law enforcement agency has its own requirements, protocols, and security measures for materials stored in its files. Ring does not impose requirements beyond law enforcement’s own procedures.”50

- Amazon does not know how many customers are using Rekognition. This demonstrates both that it is failing to conduct oversight and under its current approach, oversight may be impossible.

Information about who its customers are, which technology they are using, and how they are using a technology is a prerequisite to conducting oversight. However, it appears Amazon does not have this information and therefore oversight is not happening.51 In a 2020 PBS documentary, “Amazon Empire: The Rise and Reign of Jeff Bezos,” a PBS interviewer asks AWS CEO Andy Jassy about police use of Rekognition, saying: “…it's been difficult to know how many police departments are using [facial recognition], and there's been no public auditing around complaints of abuse, how would the public ever know?” Jassy responds: “I don't think we know the total number of police departments that are using facial recognition technology… we know of some, and the vast majority of those that are using it are using it according to the guidance that we prescribe, and when they're not, we have conversations, and if we find they're using it in some irresponsible way, we won't allow them to use the service and the platform.”
· Amazon’s grievance mechanism is lacking.

In its Statement of Opposition to the Proposal, the company argues that in the more than three years that AWS has offered its “computer vision” service, AWS has not received “a single report of the service being used” in a harmful manner. The company fails to explain how an average citizen would be aware that the service was being used and was connected to a negative impact, and whether a grievance mechanism is available and accessible to them.

3. Amazon’s support for federal regulations of its surveillance technologies does not exempt the company from its responsibility to properly vet customers who may use those technologies in ways that harm civil and human rights in the interim.

In its Statement of Opposition, Amazon indicates its support for a regulatory framework to ensure appropriate use of its products. In September 2019, Amazon CEO Jeff Bezos said: “Our public policy team is actually working on facial recognition regulations, and it makes a lot of sense to regulate that. ...there’s lots of potential for abuses with that kind of technology, and so you do want regulations.”

It is difficult to reconcile the company’s support for regulation—and acknowledgement of the potential misuse of its own technology—with its simultaneous willingness to actively risk this misuse by selling its technologies in the currently unregulated environment. In fact, AWS customers’ egregious data privacy and cybersecurity practices could lead to stronger regulation that puts further constraints on Amazon’s business in the future.

Potential positive use cases have no bearing on Amazon’s responsibility to ensure other users are not contributing to violations.

4. Amazon lags peers in practices to assess and address the ethical, legal, and reputational risks associated with customers’ use of its products.

Amazon does not appear to be limiting its customer base in any way or taking steps to reduce the likelihood of its products being used by a customer with a high likelihood of potential misuse, in contrast with peers. Microsoft has declined selling its facial recognition products to police customers due to concerns that police would use the technology in ways that violate human rights. In March 2020, Microsoft announced its decision to divest from AnyVision, an Israeli company whose facial recognition technology was being used to surveil Palestinians in the occupied West Bank, after an audit of AnyVision conducted by former U.S. Attorney General Eric Holder. Microsoft’s statement announcing the decision highlighted the company’s due diligence procedures for the use of its surveillance technologies: “For Microsoft, the audit process reinforced the challenges of being a minority investor in a company that sells sensitive technology, since such investments do not generally allow for the level of oversight or control that Microsoft exercises over the use of its own technology.” Like its peers, Amazon should take practical steps to conduct customer due diligence, gathering the information necessary to make informed decisions about how to mitigate business risks.
Conclusion

Support for Item 6 is warranted because:

1. Amazon is exposed to legal, financial, reputational, and human capital management risks if it fails to adequately manage the potential abuses of its products and services by its customers.
2. Amazon and AWS products and services including Ring, Neighbors app, cloud services, and Rekognition have significant potential for misuse and abuse, especially against communities of color.
3. Amazon’s existing systems to oversee customer use of its products and services are inadequate, and therefore an independent evaluation would be beneficial for shareholders and may mitigate risks.

Shareholders are encouraged to vote FOR Item # 6 at Amazon on May 27th.

For questions regarding Item #6 at Amazon on Customer Due Diligence please contact: Mary Beth Gallagher, Investor Advocates for Social Justice, mbgallagher@iasj.org.

Sincerely,

Mary Beth Gallagher
Executive Director
Investor Advocates for Social Justice

Date: May 14, 2020

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY ONE OR MORE OF THE CO-FILERS. PROXY CARDS WILL NOT BE ACCEPTED BY ANY CO-FILER. PLEASE DO NOT SEND YOUR PROXY TO ANY CO-FILER. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.

2 https://blog.ring.com/2019/02/14/how-rings-neighbors-creates-safer-more-connected-communities/
3 https://aws.amazon.com/rekognition/
5 https://aws.amazon.com/edgar/data/1018724/000101872419000004/amzn-20181231x10k.htm
6 https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html
8 https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html
9 https://www.sec.gov/Archives/edgar/data/1018724/000121465920004536/j514203px14a6g.htm
11 https://www.ohchr.org/EN/Issues/Business/Pages/CorporateHRDueDiligence.aspx
12 https://investorsforhumanrights.org/news/investor-case-for-mhrdd


https://medium.com/@amazonemployeesclimatejustice/amazon-employees-share-our-views-on-company-business-5fabcede849


https://www.ringsafetywarning.com/


https://www.eff.org/deeplinks/2020/02/what-know-you-buy-or-install-your-amazon-ring-camera


https://aws.amazon.com/rekognition/


https://www.sanfranciscostandard.com/2019/05/14/us-facial-recognition-ban-san-francisco.html

https://eff.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf

https://www.gizmodo.com/amazon-capital-one-face-lawsuits-massive-hack-affects-106m-customers-1840852238


https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

https://aws.amazon.com/aup/
