PX14A6G 1 d54211px14a6g.htm

United States Securities and Exchange Commission
Washington, D.C. 20549

Notice of Exempt Solicitation
Pursuant to Rule 14a-103

Name of the Registrant: Amazon.com, Inc.

Name of persons relying on exemption: The Sisters of St. Joseph of Brentwood; American Baptist Home Mission Society; Friends Fiduciary Corporation; Maryknoll Sisters; Robeco Institutional Asset Management B.V.; Sisters of Charity of St. Elizabeth, NJ; Sisters of St. Dominic of Amityville; Sisters of St. Francis of Philadelphia; and Unitarian Universalist Association.

Address of persons relying on exemption: Investor Advocates for Social Justice, 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 proponent urges you to vote FOR the Shareholder Proposal calling for a Report on Customer Due Diligence, **Item 4** at the Amazon Annual Meeting of Shareholders on **May 26, 2021.**

Summary of the Proposal

Item 4 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 of adverse impacts in the hands of Amazon customers include the Ring Doorbell and the Neighbors App, facial recognition surveillance technology, and Amazon Web Services platforms. These products increase widespread surveillance and may be used to further racial discrimination in policing and immigration enforcement, infringe on privacy, and violate civil liberties.

2. **Failure to have an effective system to monitor customers' use of products and services for potential human rights violations exposes Amazon to legal, financial, human capital, and regulatory risks, as well as loss of consumer trust.** Legislators, customers, investors, and employees have requested increased oversight.

3. **Amazon's current systems for oversight of customer use of its high-risk products and the steps it has taken to respond to human rights risks, including a temporary moratorium on facial recognition sales, are insufficient** and do not effectively address the significant risks.

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 technologies, products, and services that raise serious concern for their actual or potential civil and human rights impacts.**

Those products and services, and associated risks, include:

Amazon Web Services (AWS), with 45% of the global market, is by far the largest provider of Internet "cloud" services in the world, with 2020 revenue of $45 billion.[1] AWS currently provides cloud services for over 6,500 government agencies, including the U.S. Department of Defense and the U.S. intelligence community, as well as for governments and government agencies internationally.[2] AWS GovCloud will host the Department of Homeland Security's **Homeland Advanced Recognition Technology (HART)** system, which will enable unprecedented levels of surveillance of immigrants and U.S. citizens by DHS. [3] The database will house **sensitive biometric and biographical data** on hundreds of millions of people, including iris scans, voiceprints and palmprints, and, in some cases, DNA samples. AWS also contracts with Palantir Technologies to provide technical infrastructure to Immigration and Customs Enforcement (ICE), which has violated human rights.[4] AWS made the decision to remove the controversial **Parler** app from its server, in spite of longstanding violent, hateful and racist speech on the platform, only after Parler was associated with the deadly attack on the U.S. Capitol on January 6, 2021. A more robust, proactive customer due diligence system could have addressed this risk earlier and in a less ad-hoc and more transparent manner.[5]

Rekognition is a facial surveillance technology app marketed through AWS.[6] Rekognition allows customers to "perform face verification... by comparing a photo or selfie with an identifying document such as a driver's license" and to "understand the average age ranges, gender distribution and emotions expressed by the people, without identifying them." In April 2021, The Seattle Times reported "**Amazon is the largest provider of facial recognition technology to U.S. law enforcement, including federal immigration agencies and the FBI.**"[7] In June 2020, Amazon put in place a one-year moratorium on police use of Rekognition in connection with criminal investigations; however little disclosure on the process, scope, or impact of this is available. Amazon's moratorium on police use of Rekognition did not address concerns about police use of Ring data or other services.

Amazon has disputed numerous studies that have found Rekognition to be racially biased and inaccurate[8], misidentifying people of color at far higher rates than white people. In the hands of Rekognition's police customers[9], racially biased facial recognition technology could exacerbate existing systemic racism and racial profiling in policing, including police disproportionately targeting people of color for crimes they did not commit.[10] For example, in August 2020, a Black man in Detroit, Robert Williams, was falsely arrested and detained for 30 hours by police after being falsely identified by facial recognition technology.[11] At least three other men are known to have been falsely arrested, and detained in jail, due to police use of facial recognition technology — they are all Black.[12] **In fact, even Amazon's efforts to "improve" the ability of its facial recognition technology to recognize people of color have violated laws and threatened civil liberties.** Along with Microsoft, Amazon's use of Diversity in Faces, a dataset of 1 million facial images that is intended to train facial recognition algorithms to better recognize faces of color, violated the Illinois Biometric Information Privacy Act (BIPA), which prohibits companies from profiting off individuals' biometric data without their consent.[13]

Amazon does not know how many customers are using Rekognition, which is a prerequisite to effective customer oversight. In a 2020 PBS documentary, AWS CEO Andy Jassy said about police use of Rekognition,: "I don't think we know the total number of police departments that are using facial recognition technology."[14]

Ring[15] is a home security and "smart home" doorbell system that brings unprecedented surveillance to neighborhoods and through collaborations with police departments. Without delivering any measurable increase to achieve its so-called purpose to improve "safety",[16] Ring cameras pose a threat to basic privacy rights, disproportionately impacting communities of color. Customers of Ring cameras have experienced racist attacks[17], ransom demands, harassment, and threats, including attacks targeted at children[18]. In 2020, an Amazon engineer stated publicly[19]: "[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[20] its own employees for watching customers' videos demonstrates the security vulnerabilities with its products.

Ring-police partnerships present civil rights and civil liberties concerns: according to the Electronic Frontier Foundation[21], 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. The relationship between police and Ring leaves communities of color and all communities vulnerable to discriminatory and unjust surveillance in the absence of clear guidance, oversight, and accountability over potential misuse. In February 2021, emails obtained by the Electronic Frontier Foundation confirmed that "**the LAPD sent requests to Amazon Ring users specifically targeting footage of Black-led protests against police violence that occurred in cities across the country last summer.**"[22] In August 2021, a Newsweek headline read: "Police Are Monitoring Black Lives Matter Protests With Ring Doorbell Data and Drones, Activists Say."[23]

Ring benefits as police and local governments advertise[24] Ring products in exchange for access to data. In 2019, *The Guardian* revealed that "Ring uses corporate partnerships to shape the communications of police departments it collaborates with, directing the departments' press releases, social media posts and comments on public posts."[25] Yet, Ring has tried to downplay the extent to which police are able to access customer footage.

Reports[26] suggest Ring is considering adding facial recognition technology, Rekognition[27], to its products. 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.[28]

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.[29] In 2020, Neighbors reached 10 million users.[30] While the Neighbors app guidelines prohibit hate speech and racial profiling, these incidents occur on the platform.

In 2021, a security flaw in Ring's Neighbors App exposed the exact locations and home addresses of Ring users.[31] A similar incident was reported in 2019, when potential locations of up to tens of thousands of Ring cameras were revealed using data on Neighbors.[32] In these incidents, Amazon violated customers' privacy by enabling customer misuse of Ring and Neighbor users' data.
Ring's partnerships with thousands of local police and fire departments[33] poses civil rights risks.

In addition, Amazon markets the **Echo**, **Dot**, and **Alexa** smart speakers; Amazon customers have connected 100 million home devices to Alexa.[34] Amazon has begun integrating Alexa across non-Amazon products including cars, shopping, entertainment, and "smart home" devices; Fiat Chrysler has begun using Alexa Custom Assistant in its vehicles.[35] Each of these connected devices pose privacy risks if private customer voice data were to be exposed.

In 2020 and so far in 2021, Amazon has introduced several new, currently unregulated technology products, services and patents, each of which collect **large amounts of highly personal data and pose surveillance, civil liberties, and civil and human rights concerns**. The collection and analysis of bodily characteristics (biometrics) is an invasion of privacy. Effective, independently reviewed, and accountable preventative risk mitigation strategies, including customer due diligence, are needed. As these products come to market, controls must be put in place to ensure that its customers do not use these products in a matter that infringes on human rights and civil liberties and that Amazon will not share this data with government entities or other third parties who may use the data to violate civil and human rights and civil liberties. New technologies and potential risks include :

- **Ring Always Home Cam,**[36] an autonomous flying surveillance drone intended for home use.[37]
- **Halo**, a wearable fitness and health tracker that tracks, monitors and analyzes a person's tone of voice ("emotional tone"), body fat, body temperature, sleep patterns, and other biometric data in real time.[38] It is seeking a patent for "predicted personalized 3D body models of the body when one or more body measurements (e.g. body fat, body weight, muscle mass) are changed[39]

- **Alexa for Residential,** a program which encourages property managers and landlords to add Alexa devices to their buildings and rental units "to offer custom voice experiences that go beyond the walls of their apartments."[40] Amazon also rolled out **Blink Outdoor and Indoor** smart home security cameras.[41]

- **Amazon One**, palm scanning technology, which enables customers to purchase items by waving their hand over the scanning device.[42] It has been introduced into Whole Foods and Amazon Go stores and signed up thousands of users to this system, and Amazon reportedly seeks sell to retailers, stadiums, and office buildings.[43]

Amazon continues to share customer information with the government. In 2020, Amazon reported in its Transparency Report an increasing number of demands for user data made by U.S. federal and local law enforcement compared to the prior year, noting that the company received 23% more search warrants and subpoenas, and a 29% increase in court orders.[44] The number of requests to AWS also increased from Amazon.com retail storefront, Amazon Echo devices and its Kindle and Fire tablets.

2. **Amazon's existing due diligence systems do not ensure effective 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.**

Customer due diligence and oversight, and transparent disclosure about these practices, is appropriate, especially given the nature of the products being used, the high likelihood of potential harm, the sensitivity of the data (e.g. biometric data, video footage inside the home), and the severity of the harm that may be caused.[45] **A customer use agreement without adequate and transparent systems in place to ensure it is effective is meaningless. While its Statement in Opposition to the proposal references enhanced legal terms and customer use agreements, in the absence of an independent third-party report demonstrating these are effective to mitigate risks associated with customers' use of its products, the Company and its shareholders remain exposed to significant risks. The AWS Trust and Safety team reportedly has only 100 workers to monitor a business that has 45% of the global market for data storage and processing services.**[46] **The company appears to leave monitoring in the hands of its customers.** 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. "[47] Amazon also states: "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."[48]

While Amazon indicates in its Opposition Statement that the Board has reviewed Ring and Rekognition, it does not clarify whether the Board members have adequate expertise on human rights to evaluate these risks nor does it explain how its measures address the request of the proposal to evaluate whether the use of its products and services harm human rights and civil liberties.

The requested disclosure describing Amazon's customer due diligence processes that better control or limit future use cases would be beneficial for respecting human rights,[49] and is analogous to Know Your Customer reporting used in other sectors such as banking or finance. Given the prevalence and frequency of data breaches, and infringement on privacy and civil rights, it is clear that Amazon's existing systems — primarily, its contractual obligations with customers and Acceptable Use Policy — are ineffective at managing risks.

The processes Amazon references in its Opposition Statement to Item 4 fail to evaluate whether customers are using technologies in ways that violate human rights and do not demonstrate that the requested report is unnecessary. The chart below notes key gaps in information regarding Amazon's measures, as well as unaddressed concerns for shareholders related to customer due diligence:

Text from Amazon's Opposition Statement to Item 4	Unaddressed Customer Due Diligence Concerns
"...we have contractual restrictions that prohibit the use of Amazon Rekognition for anything illegal, harmful, fraudulent, infringing, or offensive, as well as specific guidance and requirements regarding public disclosure, training, and other safeguards."	● How does Amazon **monitor** or **enforce** its contractual restrictions for Rekognition customers? ● If Amazon does not know how many law enforcement customers use Rekognition, how would Amazon know if a law enforcement customer had misused the technology or violated its contractual restrictions? ● Does the referenced guidance address human rights impacts?
"We also have a mechanism to allow third parties to report potential abuses of the technology, and in the four-plus years AWS has been offering Amazon Rekognition, we have not received a single report of use in the harmful manner posited in the proposal."	● How does Amazon monitor third parties using its surveillance, cloud or computer vision technologies? ● To what extent does Amazon rely on customers to report customer misuse of its products? ● How would an average person be aware that Rekognition was being used, and that it was connected to a negative impact, and that a grievance mechanism is available and accessible to them?
"Ring limits potential misuse of its products and services in numerous ways, including designing its Neighbors App to allow users to choose whether and what to share, enforcing strict limitations on a public safety agency's use of Neighbors to ask users for video recordings, and requiring users to abide by community guidelines that prohibit racial profiling, hate speech, and other forms of discrimination."	● How does Ring monitor or enforce the Neighbor's App community guidelines, and what data demonstrate the effectiveness of this enforcement in preventing racial profiling, hate speech and other forms of discrimination on the platform? ● How does Ring protect the privacy of people (including non-customers) whose video or image is collected and shared — including with police — on the Neighbors App? ● If a Ring customer consents to police use of their data, how does Ring respect the rights of people whose data are captured in the video footage, yet whose consent cannot be given, and who may not even be aware that the data collected about them exists in the first place because it was captured by a surveillance device?

"On June 10, 2020, AWS implemented a one-year moratorium on use of Amazon Rekognition's face comparison feature by police departments in connection with criminal investigations."	● Does AWS' Rekognition moratorium include all law enforcement use? Does it include immigration enforcement use of Rekognition? Is police use of Rekognition outside of criminal investigations acceptable use during the moratorium? ● How is Amazon addressing the underlying risks that required the moratorium in the first place?
"Ring strives to fulfill its mission to help make neighborhoods safer by assisting community members in sharing important safety information and connecting with each other, as well as helping reunite families with their missing loved ones."	● How does Ring ensure that it is not facilitating the over-policing and surveillance of Black and Brown communities? ● Will Ring prohibit Immigration and Customs Enforcement (ICE) from obtaining or using any Ring customer data (including data shared by Ring customers with police) to carry out deportation efforts and contribute to family separation?
"...if a law enforcement agency uses Amazon Rekognition in connection with criminal investigations, AWS legal terms require it to publicly disclose its use of facial recognition systems, summarize the safeguards in place to prevent violations of civil liberties or equivalent human rights, and make the disclosure easily accessible."	● How is Amazon enforcing its legal terms requiring law enforcement agencies to publicly disclose the use of Rekognition, summarize the safeguards in place to prevent violations of civil liberties or equivalent human rights, and make these disclosures easily accessible? ● This is not transparent. Shareholders are unable to locate any disclosures or summaries of this sort.
"AWS will suspend or terminate access to Amazon Rekognition if we determine a customer is violating our AUP or the updated terms mentioned above."	● What is the scope of risks covered in the AUP (e.g. data security, privacy, discrimination including based on ethnicity and race, inappropriate use of products or services by not following directions for use, etc.) and what constitutes a violation? ● How does AWS determine when a customer has misused its products or violated its Acceptable Use Policy? What enforcement oversight mechanisms are in place? How frequently has this happened? ● What if an AWS customer uses technology in a way that is consistent with the AUP, but which violates human rights and civil liberties?

A recent Investor Update by Ranking Digital Rights,[50] stated: "Amazon ranked dead last among digital platforms in the 2020 RDR Index due to the company's abject failure on governance and accountability. The company makes few public commitments related to human rights and offers **no evidence of any due diligence or oversight around digital rights risks and harms**." It found Amazon is not only facing regulatory scrutiny but also has lax security and careless handling of users' data and "**disclose[s] no information of substance about its internal processes to ensure the security of its products and services."**

For E-Commerce and Software & IT companies such as Amazon, the Sustainability Accounting Standards Board (SASB) has identified Customer Privacy and Data Security as issues that are financially "material."[51] This includes metrics on data security risks, users whose information is used for secondary purposes, and policies and practices relating advertising and privacy. While these metrics do not address the full range of relevant disclosure on human rights and civil liberties risk, they are still not disclosed by Amazon.

3. Amazon faces scrutiny from regulators and lawmakers on its oversight and due diligence.

Amidst growing support for mandatory due diligence legislation, Amazon's lack of robust customer due diligence mechanisms exposes the Company to increased regulatory risks. In March 2021, the European Parliament voted by an overwhelming majority in support of EU legislation that would require companies to conduct human rights due diligence aligned with the UN Guiding Principles on Business and Human Rights.[52] Amazon has substantial business interests in the EU and will therefore be required to identify, prevent, mitigate and account for its human rights impacts. In April 2021, the European Commission published a Proposal for a Regulation on a European approach for Artificial Intelligence (the "Artificial Intelligence Act"),[53] a regulatory framework for AI and "high risk" AI systems, which include any systems using remote biometric identification in real time, including facial recognition technology. This is in addition to national and regional movements for mandatory HRDD,[54] which investors strongly support.[55]

In addition, in September 2020, **the U.S. Department of State published "Guidance on Implementing the 'UN Guiding Principles' for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities**"[56] to address potential misuse including stifling dissent, harassment of human rights defenders, targeting political opponents or interfering arbitrarily or unlawfully with privacy. The State Department suggests the following to companies: "Review product or service and conduct assessments to determine if the product or service could be misused to violate or abuse human rights;" "Review stakeholders involved in the transaction (including end-user and intermediaries such as distributors and resellers);" and refer to the U.S. Dept. of Commerce Business and Industry Standards Know Your Customer Guidance.[57] Amazon does not appear to undertake these steps. The Federal Trade Commission also plans to regulate artificial intelligence.[58]

Amazon is the subject of increasing scrutiny from legislators and regulators.

- The European Commission has launched an antitrust investigation into Amazon.[59]
- The House Judiciary Committee reported that Amazon exploits data for its own product development and that Alexa gathers significant private data from within users' homes which is "at risk" of internal abuse and breach.[60]
- In July 2020, Rep. Raja Krishnamoorthi, the Chairman of the Subcommittee on Economic and Consumer Policy, wrote to Amazon twice asking if Ring Inc. will abide by Amazon's announced moratorium on law enforcement's use of facial recognition technology and what changes Ring will make to its concerning police surveillance partnerships and its Neighbors app.[61]
- In November 2019, five U.S. senators wrote to Amazon CEO Jeff Bezos requesting information about Ring's data security practices.[62]
- U.S. Senator Ed Markey'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."**[63]
- Congress has held multiple hearings on oversight of facial recognition.[64] Lawmakers have questioned whether the technology should be used at all,[65] even if it is 100% accurate. There is a growing movement to ban facial recognition technology nationwide.[66] In January 2020, 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."[67]
- In June 2020, four members of Congress introduced the Facial Recognition and Biometric Technology Moratorium Act, "bicameral legislation to stop government use of biometric technology, including facial recognition tools."[68]
- Multiple jurisdictions have completely banned government use of facial recognition technology.[69] California has enacted a 3-year moratorium on police use of facial recognition technology on police body cameras.[70] In September 2020, the Mayor and City Council of Portland, Oregon unanimously voted to ban the use of facial recognition technology by the government and private actors. In April 2021, over 20 civil and human rights organizations called on government officials at the local, state, and federal level to ban all forms of private and corporate use of facial recognition technology,[71] and specifically called out Amazon's use of the technology.

Amazon is exposed to legal and regulatory risks and stronger oversight and management of potential customer use cases that violate human rights is needed.

4. **Failure to manage the civil and human rights risks associated with the use of its products 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.**

Amazon is the subject of significant negative public attention which threatens its reputation, and its ability to attract and retain employees. AWS faces backlash from employees[72] and the public[73] over its direct and indirect ties to human rights violations carried out by U.S. Immigration and Customs Enforcement (ICE) and associated with Palantir.[74] Thousands of students have protested Amazon recruitment fairs[75] over their refusal to work in tech company roles that enable harmful immigration enforcement in the United States.

Amazon faces legal risk due to customers' use of its products for surveillance, and customers' ability to abuse the company's apparently poor cybersecurity and data privacy protocols. Ring faces a $5 million class action lawsuit[76] over its failure to keep customers safe from cyberattacks, racism, ransom demands, harassment, and threats. 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.[77]

Amazon faces loss of consumer trust and reputational risk. AWS security breaches, including of health information, affected thousands of patients.[78] In 2020, thousands of Zoom meeting cloud recordings stored on an unprotected AWS platform were exposed on the web.[79]

In December 2019, nine national consumer advocacy groups issued a Ring product warning, citing risks to privacy and safety[80], creating reputational risk for the company and harming consumer trust in its products as it warned: "Do not buy Amazon Ring cameras."

In March 2021, over 20 civil society organizations released a joint letter calling on the editors of product review websites to "rescind their recommendations of Amazon Ring cameras given the threats Ring technology poses to Black and brown communities.[81] Arisha Hatch, Vice President of Color Of Change, stated[82]: "...Since 2018, Color Of Change and our millions of members have demanded that Amazon address the concerns of civil rights advocates and the larger public about the company's attempts to peddle products, such as Ring, that enable state-sponsored discrimination and police violence against Black and brown communities." Petitions against Amazon and pressure from consumers continues to grow.[83]

5. **Amazon's support for federal regulations of its surveillance technologies and a temporary moratorium on sales of Rekognition 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."[84] In 2020, Amazon introduced a 1-year moratorium on police use of Rekognition to allow the government time to pass regulation to address potential misuse.

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. This exposes the company and its shareholders to significant risk.

Conclusion

Support for **Item 4** 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 4 at Amazon on May 26, 2021.

For questions regarding Item #4 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 4, 2021

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.

[1] https://s2.q4cdn.com/299287126/files/doc_financials/2021/ar/Amazon-2020-Annual-Report.pdf

[2]https://aws.amazon.com/government-education/government/

[3] https://www.nextgov.com/it-modernization/2020/05/homeland-securitys-biometrics-database-its-way-amazon-cloud/165186/

[4] https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf; https://www.business-humanrights.org/en/usa-palantir-is-allegedly-enabling-ice%E2%80%99s-human-rights-violations-against-migrants-asylum-seekers-incl-company-response; https://www.forbes.com/sites/rachelsandler/2019/07/11/internal-email-amazon-faces-pressure-from-more-than-500-employees-to-cut-ties-with-palantir-for-working-with-ice/#5b0e2e897539

[5] https://www.eff.org/deeplinks/2021/01/beyond-platforms-private-censorship-parler-and-stack

[6] https://aws.amazon.com/rekognition/

[7] https://www.seattletimes.com/business/technology/facial-recognition-lawsuits-against-amazon-and-microsoft-can-proceed-judge-rules/

[8] https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

[9] https://www.nytimes.com/2018/05/22/technology/amazon-facial-recognition.html

[10] https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf

[11] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[12] https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[13] https://www.seattletimes.com/business/technology/facial-recognition-lawsuits-against-amazon-and-microsoft-can-proceed-judge-rules/

[14] https://www.youtube.com/watch?v=RVVfJVj5z8s&t=5007s

[15] https://www.amazon.com/stores/Ring/Ring/page/77B53039-540E-4816-BABB-49AA21285FCF

[16] https://www.cnet.com/news/rings-cameras-come-with-privacy-concerns-what-about-the-smart-lights/; https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/. 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.

[17]https://abcnews.go.com/US/ring-security-camera-hacks-homeowners-subjected-racial-abuse/story?id=67679790

[18]https://markets.businessinsider.com/news/stocks/couple-sues-ring-after-hackers-spied-on-eight-year-old-2020-1-1028797710

[19]https://medium.com/@amazonemployeesclimatejustice/amazon-employees-share-our-views-on-company-business-f5abcdea849

[20] https://www.vice.com/en_us/article/y3mdvk/ring-fired-employees-abusing-video-data

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

[22] https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests

[23] https://www.newsweek.com/amazon-ring-drones-monitor-protests-1523856

[24] https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money

[25] https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor

[26]https://www.digitaltrends.com/home/ring-may-want-to-add-facial-recognition-and-licence-plate-reading-to-cameras/

[27] https://aws.amazon.com/rekognition/

[28]http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180341835%22.PGNR.&OS=DN/20180341835&RS=DN/20180341835

[29] https://blog.ring.com/2019/02/14/how-rings-neighbors-creates-safer-more-connected-communities/
[30] https://www.androidcentral.com/ring-neighbors-hits-10-million-users-gaining-end-end-encryption-soon
[31] https://techcrunch.com/2021/01/14/ring-neighbors-exposed-locations-addresses/
[32] https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279
[33] https://www.documentcloud.org/documents/6603014-Response-Letter-on-Ring-1-6-2020.html#document/p2/a545936
[34] https://s2.q4cdn.com/299287126/files/doc_financials/2021/ar/Amazon-2020-Annual-Report.pdf
[35] https://gizmodo.com/amazon-wants-other-companies-to-make-their-own-voice-as-1846074862
[36] https://blog.ring.com/2020/09/24/introducing-ring-always-home-cam-an-innovative-new-approach-to-always-being-home/
[37] https://www.wired.com/story/amazon-drone-camera-go-palm-data-privacy/
[38] https://www.cnet.com/news/amazon-halo-new-health-app-fitness-tracker-metrics-include-body-fat-tone-of-voice/
[39] https://pdfaiw.uspto.gov/.aiw?Docid=20210097759
[40] https://www.theverge.com/2020/9/3/21419812/amazon-alexa-residential-apartment-privacy
[41] https://press.aboutamazon.com/news-releases/news-release-details/amazons-blink-unveils-new-wireless-security-cameras-hd-video
[42] https://www.cnbc.com/2021/04/21/amazon-whole-foods-getting-palm-scanning-payment-system.html
[43] https://www.wired.com/story/amazon-drone-camera-go-palm-data-privacy/
[44] https://techcrunch.com/2020/07/30/amazon-police-data-demands/
[45] https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards- evaluating-domestic
[46] https://www.washingtonpost.com/technology/2021/01/13/amazon-parler-takedown/
[47]https://www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%209.26.19.p
[48]https://www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%209.26.19.pdfdf
[49]https://www.humanrights.dk/sites/humanrights.dk/files/media/document/Phase%204_%20Impact%20prevention%2C%20mitigation%20and%20remediation_n.pdf
[50] https://rankingdigitalrights.org/wp-content/uploads/2021/04/Spring-2021-Investor-Update.pdf
[51] See the SASB Material Map for "E-Commerce and Software & IT" at https://materiality.sasb.org/. The Standard can be downloaded at https://www.sasb.org/wp-content/uploads/2018/11/E_Commerce_Standard_2018.pdf
[52] https://www.natlawreview.com/article/eu-mandatory-environmental-and-human-rights-due-diligence-law-what-you-need-to-know; https://www.ohchr.org/EN/Issues/Business/Pages/CorporateHRDueDiligence.aspx
[53] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence
[54] https://www.business-humanrights.org/en/latest-news/national-regional-movements-for-mandatory-human-rights-environmental-due-diligence-in-europe/
[55] https://investorsforhumanrights.org/news/investor-case-for-mhrdd
[56] https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf
[57] https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/47-know-your-customer-guidance
[58] https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai
[59] https://ec.europa.eu/commission/presscorner/detail/pl/ip_19_4291
[60] https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519
[61] https://oversight.house.gov/news/press-releases/krishnamoorthi-seeks-commitment-from-ring-on-facial-recognition-moratorium-and
[62] https://theintercept.com/document/2019/11/20/senators-letter-to-amazon-on-ring-cameras/
[63]https://www.markey.senate.gov/news/press-releases/senator-markey-investigation-into-amazon-ring-doorbell-reveals-egregiously-lax-privacy-policies-and-civil-rights-protections
[64] https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-iii-ensuring-commercial-transparency
[65] https://www.cnet.com/news/facial-recognitions-accuracy-is-the-least-of-our-worries-lawmakers-say/

[66] https://www.banfacialrecognition.com/

[67] https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf

[68] https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology

[69] https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[70] https://www.aljazeera.com/news/2019/09/california-moves-ban-facial-recognition-police-body-cameras-190913014509067.html

[71] https://thehill.com/policy/technology/548037-civil-rights-organizations-call-for-ban-on-corporate-use-of-facial

[72] https://www.businessinsider.com/amazon-employees-letter-protest-palantir-ice-camps-2019-7

[73] https://thehill.com/policy/technology/technology/460193-12-arrested-at-amazon-building-in-protest-demanding-amazon-stop

[74] https://www.forbes.com/sites/rachelsandler/2019/07/11/internal-email-amazon-faces-pressure-from-more-than-500-employees-to-cut-ties-with-palantir-for-working-with-ice/#5b0e2e897539

[75]https://www.latimes.com/business/technology/story/2019-12-07/students-protest-tech-companies-ice-contracts

[76] https://abcnews.go.com/US/amazon-ring-face-million-proposed-class-action-lawsuit/story?id=67948687

[77] https://www.geekwire.com/2019/amazon-capital-one-face-lawsuits-massive-hack-affects-106m-customers/

[78] https://www.hipaajournal.com/93000-files-belonging-to-california-addiction-treatment-center-exposed-online/

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

[80] https://www.ringsafetywarning.com/

[81] https://www.fightforthefuture.org/news/2021-03-24-joint-letter-from-20-racial-justice-and-civil/

[82] https://www.fightforthefuture.org/news/2021-03-24-20-civil-rights-groups-demand-tech-reviewers-stop/

[83] https://breakupwithamazon.org/

[84]https://www.cnbc.com/2019/09/25/jeff-bezos-says-amazon-is-working-on-face-recognition-regulations.html