PX14A6G 1 p425191px14a6g.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: Sisters of St. Joseph of Brentwood, Azzad Asset Management, Maryknoll Sisters, Sisters of St. Francis Charitable Trust, Sisters of St. Francis of Philadelphia

Address of persons relying on exemption: 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 Item #6 on the proxy, the Shareholder Proposal on Risks of Sales of Facial Recognition Software at the Amazon.com, Inc. Annual Meeting on May 22, 2019.

1

IMPORTANT PROXY VOTING MATERIAL

Shareholder Rebuttal to Amazon.com, Inc.
Requesting a Ban on Sales of Rekognition to Government Agencies Subject to Board Evaluation

The Sisters of St. Joseph of Brentwood and 4 co-filers urge you to vote **FOR** Item #6 on the proxy, the Shareholder Proposal on Risks of Sales of Facial Recognition Software at the Amazon.com, Inc. Annual Meeting on May 22, 2019.

Support for this resolution is warranted because:

1. Amazon is exposed to financial, reputational, regulatory, legal and human capital management risk due to its sales of facial recognition technology to government, and these risks can only be mitigated by stopping sales to government until risks are fully assessed.
2. Amazon's existing management systems and processes fail to address the societal risks of violating privacy rights, freedom of association and assembly, and the right to non-discrimination. Therefore, an independent assessment is needed to ensure Rekognition will not cause harm before proceeding with sales to government.
3. Amazon lags peers in governance, oversight and management practices to assess and address the ethical, legal, and reputational risks associated with the use of its products. Investors are requesting the board conduct the necessary due diligence to evaluate human rights risks around the sale of Rekognition to government, and that Amazon fulfill its obligations as a manufacturer to assess and address risks prior to sales, not after.

SUMMARY OF RESOLUTION

RESOLVED, shareholders request that the Board of Directors prohibit sales of facial recognition technology to government agencies unless the Board concludes, after an evaluation using independent evidence, that the technology does not cause or contribute to actual or potential violations of civil and human rights.

SUPPORTING STATEMENT: Proponents recommend the Board consult with technology and civil liberties experts and civil and human rights advocates to assess:

- The extent to which such technology may endanger or violate privacy or civil rights, and disproportionately impact people of color, immigrants, and activists, and how Amazon would mitigate these risks.
- The extent to which such technologies may be marketed and sold to repressive governments, identified by the United States Department of State Country Reports on Human Rights Practices.

2

ARGUMENTS IN FAVOR OF THE RESOLUTION ON RISKS OF SALES OF FACIAL RECOGNITION SOFTWARE

1. **Amazon is exposed to financial, reputational, regulatory, legal, and human capital management risk due to its sales of Rekognition to government.**

Investors are concerned by sales of Rekognition to government in the United States and globally because this highly controversial technology poses tremendous risks involving civil and human rights and government surveillance.

Rekognition is a facial recognition technology tool that is being deployed for facial recognition and recognition of other imagery in photographic and video recordings as one application available through Amazon Web Services (AWS). AWS offers cloud-based products including "compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security and enterprise applications."[1] As promoted on the AWS web site, Rekognition is marketed in a suite of apps; it is offered "free" to new AWS subscribers.[2] AWS's apparent intention is to offer apps that will induce subscribers to use more of AWS's cloud services.

AWS is by far the largest provider of Internet "cloud" services in the world, with 2018 revenue of $25.6 billion.[3] AWS currently provides cloud services for all 17 United States intelligence agencies, as well as for government agencies internationally[4] in the United Kingdom, Italy, Singapore, Belgium, Canada, and Turkey. The FBI is testing Amazon's Rekognition[5], and Amazon is attempting to sell Rekognition to Immigration and Customs Enforcement (ICE)[6]. Florida's Orlando Police Department (OPD) and the city of Orlando, in July 2018, announced it would continue to use Rekognition after an initial pilot program.[7] Amazon lists the Washington County Sheriff's Office in Oregon, WA as a Rekognition customer.[8]

According to the United Nations Guiding Principles on Business and Human Rights (Principle 17),[9] Amazon has a responsibility for the use of its products, and human rights due diligence should cover "impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships."

In the hands of government, Rekognition threatens civil liberties and civil rights for all members of society, and especially for people who are more likely to be surveilled, profiled and targeted, including people of color and immigrants. Clare Garvie, of Georgetown Law's Center on Privacy & Technology, has written[10]: "A mistake by a face-scanning surveillance system on a body camera could be lethal. An officer, alerted to a potential threat to public safety or to himself, must, in an instant, decide whether to draw his weapon. A false alert places an innocent person in those crosshairs."

The American Civil Liberties Union (ACLU)[11] has noted that facial recognition technology threatens to "chill First Amendment-protected activity like engaging in protest or practicing religion, and it can be used to subject immigrants to further abuse from the government."

Amazon has repeatedly responded to the controversy in defense of Rekognition. In February 2019, AWS's Global Public Policy VP published a blog post outlining key areas where the Company was taking the unusual step of calling for enhanced regulatory policies surrounding facial recognition technology, especially when used by police.[12] **Amazon's blog post is a clear recognition that the Company has placed onto the market a technology that is most inadequately controlled and regulated.** Public expectations of privacy and respect for civil rights are not presently protected, and Rekognition should not be sold until it is regulated.

3

While the accuracy of Rekognition's technology is a concern — multiple studies by M.I.T. researchers and the ACLU have found that racial and gender bias is embedded in Rekognition[13] — there are more fundamental issues, including whether facial recognition should be deployed at all because of the role the technology plays in enabling ubiquitous government surveillance.

Indeed, scientific and academic research suggests that over time the societal risks embedded in a technology such as Rekognition may not decline but may instead increase quickly and dramatically as Rekognition is deployed more widely. In April 2019, 25 prominent artificial-intelligence researchers — including experts at Amazon competitors Google, Facebook and Microsoft, and a winner of the prestigious Turing Award — called on Amazon to stop selling Rekognition to government.[14] "There are no laws or required standards to ensure that Rekognition is used in a manner that does not infringe on civil liberties," the AI researchers wrote.

This is particularly concerning for those whose human rights are neglected by autocratic government regimes. Human rights organizations cite the deployment of facial recognition in China, where, according to one expert, "surveillance technologies are giving the government a sense that it can finally achieve the level of control over people's lives that it aspires to."[15]

Scholars Woodrow Hartzog and Evan Selinger have written[16]: "We believe facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented...when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering."

Amazon is reported to be the second most trusted institution in the United States[17], and sales of Rekognition threaten this extraordinary relationship of trust on which the Company relies for success. Given the serious potential risks outlined above, manifestation of these potential harms could result in a negative financial impact on Amazon, through, for example, a decrease in sales or contracts due to diminished consumer trust that negatively impacts the demand for Amazon products and services and increases the cost of business. Research shows that being linked to adverse human rights impacts can negatively impact a company's reputation and harm its potential to secure future contracts. A recent study quantifying the material impact of the reputational harm for Energy Transfer Partners (ETP) due to its inadequate stakeholder consultation and public pressure from the Standing Rock Sioux Tribe to the Dakota Access Pipeline demonstrated that social tension negatively impacted stock price and ETP underperformed relative to market expectations as a result of the controversy. Growing and widespread social controversy and public pressure surrounding Rekognition may negatively impact Amazon's financial performance.

Privacy as a material financial risk

Rekognition, as a potential tool for surveillance when sold to government, already presents material issues for Amazon regarding consumer privacy. According to the Sustainability Accounting Standards Board (SASB)[18], which identifies environmental, social and governance factors most likely to materially impact the financial condition or operating performance of companies in an industry, consumer privacy is likely to be a material issue for companies operating in technology and communications. This includes the management of risks related to the use of personally identifiable information (such as biometric data collected through facial recognition technology), social issues that may arise from a company's collecting information (such as public controversies surrounding the collection of facial imagery), and managing evolving regulation (such as regulation around the commercial use of facial recognition).

4

Reputational risk posed by sales of Rekognition to government

The public controversy surrounding Rekognition presents critical risks to the Company's reputation, including the willingness of consumers to trust the company to safeguard their privacy and civil and human rights because storing your data on their cloud requires that you trust them to keep your data safe. Therefore, consumer trust is one of Amazon's most important intangible assets. This comes as Amazon, with its leadership position in the technology sector, confronts growing public criticism regarding the role of technology companies, including Amazon.com, and its products and services, in societies and economies around the world. Thus, proponents believe Rekognition also threatens Amazon's long-term prospects.

Amazon is the subject of mounting public controversy because of this product. In May 2018, the ACLU, along with a coalition of civil rights organizations, sent a public letter to the Company demanding that it stop selling Rekognition to government.[19] In January 2019, over 85 activist groups – including the ACLU, the National Lawyers Guild chapters, and Freedom of the Press Foundation — signed an open letter expressing their concern for how Rekognition technology threatens community safety, privacy, and human rights.[20]

The increasing controversy surrounding Rekognition highlights the fragile relationship of trust between the Company and its consumers, employees, and the public at large. A number of the Company's products – Alexa, Ring, and Eero — could face a spillover effect if Amazon's ability to maintain the trust of customers is breached by concerns about privacy and surveillance. Moreover, in addition to the Company's unique exposure to risk by virtue of it being a business operating in the technology sector, it also has a product pipeline and pending patent applications which demonstrate the trajectory of the Company will confront just such concerns. For example, two facial recognition-related patent applications filed by the Company feature a technology that could use multiple cameras to create a composite image of a person's partially seen face, and could then automatically alert law enforcement if a "suspicious" person or known criminal is in view of Ring's cameras.[21] Only this month, multiple media outlets sparked controversy with reports that Amazon employees were "listening" to recordings from Alexa devices in the home.[22]

A degraded reputation has also had a negative impact on the company's social license to operate. In 2019, Amazon's reputation fell in the Axios Harris Poll 100 Reputation Ratings[23], which ranks the reputation of the most visible companies in the U.S:

> "For three years, America voted Amazon its top company for corporate reputation. ...But suddenly, amid a high profile search and last minute cancellation for HQ2, and the ensuing fallout with Alexandria Ocasio-Cortez and company, America still loves its smiling boxes, but are beginning to grow uneasy with Amazon's reach and power…while the public ranked Amazon #2 for Products & Services, they ranked Amazon much lower for ethical attributes like "speaking out on social issues that are important to me" (#36), "maintains high ethical standards" (#16) , and "looks like a good company to work for" (#12)."

5

The deal for a major new HQ2 facility in New York City recently fell through. While Rekognition was not the main issue raised in the controversial discussions, it was cited prominently by a number of key community leaders, including New York City Council members, U.S. Representative Alexandria Ocasio-Cortez, and numerous immigrant rights groups concerned by the threat to immigrant communities posed by facial recognition technology in the hands of government, including ICE.

Regulatory risk posed by sales of Rekognition to government

Amazon's sales of Rekognition to government faces regulatory risk and an environment of uncertainty. In December 2018, the AI Now Institute at New York University warned the "urgent need" for stricter regulation of facial recognition technology.[24]

Members of Congress have written multiple letters to CEO Jeff Bezos expressing concerns about Amazon's Rekognition product.[25]

In July 2018, five U.S. Senators called on the federal government's General Accounting Office (GAO) to investigate the commercial and government use, and potential abuse, of facial recognition technology.[26] This month, GAO wrote[27] to the Dept. of Justice saying the agency had failed to appease GAO's stated concerns about FBI use of face recognition technology (the FBI is piloting Rekognition).

In March 2019, two U.S. Senators introduced the Commercial Facial Recognition Privacy Act of 2019 that would prohibit commercial users of facial recognition technology "from collecting and re-sharing data for identifying or tracking consumers without their consent."[28]

In the United States, legislation that would ban government use of facial recognition technology has been recently introduced in the states of Massachusetts[29] and Washington[30] and in the city of San Francisco.[31]

The Company has itself noted the potential materiality of risks associated with a regulatory framework that has not yet caught up with such emerging technologies in its discussion of risk factors in its 2019 10-K[32]:

> "It is not clear how existing laws governing issues such as property ownership, libel, data protection, and personal privacy apply to the Internet, e-commerce, digital content, web services, and artificial intelligence technologies and services. Unfavorable regulations, laws, and decisions interpreting or applying those laws and regulations could diminish the demand for, or availability of, our products and services and increase our cost of doing business."

Legal risk posed by sales of Rekognition to government

Meanwhile, as Amazon continues to sell Rekognition in a largely unregulated environment, consumers as well as local, state and federal government actors may escalate legal challenges to the company to establish stronger precedents around consumer privacy, posing the risk of major fines charged for regulatory violations and litigation.

The Illinois Supreme Court in January 2019 expanded the potential liability for companies that sell facial-recognition technology under the state's Biometric Information Privacy Act by ruling that plaintiffs only need to prove technical violations rather than actual injury or damages, further clearing the way for potential lawsuits involving facial technology.

6

Investors should have disclosure from the Company about how Amazon assesses legal risk. **Halting sales of Rekognition to government would allow the board to properly understand and convey to shareholders the extent to which these sales present legal risks, and the company's plan to mitigate those risks, before it is too late.**

Human capital management risk posed by sales of Rekognition to government

Amazon's status as an employer of choice, and Amazon's ability to be consistent with the values of its employees, is being undermined by the Company's internal management and potential sale of surveillance technologies, including Rekognition. The company's lack of transparency about the nature of its sales and failure to respond to employees who do not want to use their time and talent in support of selling surveillance technology to government may be hurting Amazon's ability to attract, hire, retain, and maintain good relations with employees. Amazon risks losing top new talent as millennials in the workforce seek employment from companies who can match their values. An Accenture report found that 70% of 2016 college graduates prefer an employer who offers a positive social atmosphere, and companies that "do good", over a higher salary; 92% said it was important their employer demonstrate social responsibility.[33]

The Company's attempt this past June to sell Rekognition to ICE fueled a backlash among Amazon employees, 450 of whom signed an open letter to the Company in protest, saying:

> "...We learn from history, and we understand how IBM's systems were employed in the 1940s to help Hitler. IBM did not take responsibility then, and by the time their role was understood, it was too late. We will not let that happen again. The time to act is now. We call on you to: Stop selling facial recognition services to law enforcement."[34]

In addition to products that present these concerns, surveillance issues raised by Rekognition are mirrored within the Company itself in how it tracks its own employees. The Company was granted two patents recently that would allow it to track its workers' hand movements through wristbands. By tracking detailed movements through artificial intelligence technologies, the Company can also obtain and record highly private information, such as when an employee takes a bathroom break. This degree of monitoring adds Fourth Amendment privacy intrusion concerns to the mix of a work culture already criticized for pressuring employees to work long hours and perform above all else, threatening the long-term performance and health of the company overall.

Halting sales of Rekognition to government is an application of the precautionary principle

Independently assessing risks posed by potential human rights impacts and other critical issues *prior* to sales of a product not only protects stakeholders who may be harmed by company operations, but also helps businesses minimize expensive legal, operational, and reputational risks, benefiting Amazon's – and in turn, shareholders' – bottom lines.

By supporting this Proposal, investors are applying the "precautionary principle." Adopted globally in 1992 as part of the United Nations Rio Convention on sustainable development, the precautionary principle implies that where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing protective measures. It has been deployed by companies in decisions to phase out the use of toxic chemicals and in legislation on environmental and health protection. This approach is consistent with prudent risk management. For Amazon's Rekognition, investors are applying the precautionary principle by pausing to assess risk.

7

Amazon's Rekognition technology poses a powerful and potentially irreversible threat to civil and human rights. As a consequence, it also jeopardizes shareholder value. The precautionary approach, by halting sales of facial recognition to government agencies and by assessing and reporting on these impacts and risks, is therefore necessary here to ensure sound stewardship at the Company. The Proposal suggests that the Company can and should undertake more high-level oversight of these issues before marketing the technology, especially for use by government and police. This is especially the case because experts warn that facial recognition software gives the government the power to violate civil liberties – targeting immigrants, religious minorities, and people of color, in new, hyper-powered ways.

In the technology industry overall, companies often seek to gain market advantage by establishing their place as the first mover of a new product or technology; however, in the case of Rekognition, the application of the precautionary principle is warranted because the extensive, aforementioned risks of marketing the technology far outweigh any potential benefits of being a first mover of this dangerous technology.

2. Amazon's existing management systems and processes fail to address the risks of sales of Rekognition and an independent assessment is needed to ensure it will not cause harm.

Amazon's existing policy to mitigate risks of sales of Rekognition are insufficient and ineffectual

In its Opposition Statement, Amazon argued that the AWS Acceptable Use Policy protects against risks posed by illegal or harmful use of Rekognition. Amazon asserts in the Opposition Statement that customers who gain access to deploy Rekognition must comply with its Acceptable Use Policy which prohibits the use of its products "for any illegal, harmful, fraudulent, infringing or offensive use," including the violation of laws related to privacy, discrimination and civil rights, and that Amazon has not received a single report of Rekognition being used in a harmful manner as posited in the proposal. Recent experience, however, demonstrates that the Acceptable Use Policy is no guarantee that the AWS platform will not be used in a harmful manner. According to multiple media reports[35], a Mexico-based news site used Amazon servers to openly store 540 million records on Facebook users, including identification numbers, comments, reactions and account names. The problem was detected by researchers at an independent security firm which reportedly sent emails to Amazon "over many months" to alert it to the problem. Amazon reportedly failed to respond to those messages.

Amazon itself has shifted its stated position that existing company policies protect users and the Company from significant risk. For example, in the face of the groundswell of concern by NGOs and civil liberties experts, a leading company spokesman, as discussed above and in the Opposition Statement to the Proposal, tempered the Company's position, calling for government regulation and "dialogue" among stakeholders, including shareholders. It is frankly difficult to understand why the company is opposing the current Proposal, as the Proposal itself seems to provide the opportunity to fulfill exactly the terms of Amazon's own invitation for "open, honest, and earnest dialogue" with the Company's shareholders.

Shareholders are concerned with violations by government customers particularly. Currently, the FBI is petitioning for face recognition systems to be exempt from the prohibitions on tracking people during the exercise of their right to free speech.[36] In addition, long-standing rules that have precluded the FBI and Department of Homeland Security from tracking the identity of individuals during the exercise of free speech appear to be at risk.[37] Therefore, the Acceptable Use Policy provisions are far from self-executing, and as the example of the FBI request for waiver of normal civil liberties protections demonstrates, the evidence shows that the Acceptable Use Policy is ineffective at protecting people from the harms of surveillance technology in the hands of government.

Insufficient board oversight of risks related to Rekognition

Governance of the significant risks presented by Rekognition is lacking. Instead of company oversight, it appears that the responsibility falls to the customer for ensuring that the technology is not used in illegal or harmful ways that threaten shareholder value. This is too significant of an issue for the company to abdicate its responsibility to protect human rights. The Proponents are concerned that the Amazon board is not equipped to adequately identify and assess the risks posed by Rekognition. The directors overall lack expertise that would give them the background or tools to assess the human rights impacts of machine learning, artificial intelligence, and the primary technologies behind a product like Rekognition. One possible exception is director Daniel Huttenlocher, who holds a Ph.D in Computer Science from MIT and hails an interest in "emerging technologies." The board also lacks any governance committee tasked with overseeing these risks. This is another reason why sales should be stopped until an independent group of experts has the ability to assess the risks and advise the board on whether or how it could proceed with sales of Rekognition to governments.

3. Amazon lags peers in governance, oversight and management practices to assess and address the ethical, legal, and reputational risks associated with the use of its products.

Amazon's peer companies in the technology sector have implemented stronger governance mechanisms to oversee human rights and ethics concerns posed by the sale of technologies. Amazon maintains three board committees: a Leadership Development and Compensation Committee, an Audit Committee, and a Nominating and Corporate Governance Committee. None of the committee charters make mention of human rights concerns or ethics in any manner. For a company as large as Amazon with business interests with implications in as many areas of society as Amazon, this is an especially egregious omission of purpose.

Alphabet, parent of Google and competitor to Amazon in the technology field, in December 2018 said it has opted to not yet offer facial recognition technology: "...unlike some other companies, Google Cloud has chosen not to offer general-purpose facial recognition APIs before working through important technology and policy questions."[38] This is clearly a reference to Amazon, which faced extensive public criticism and reputational damage during this time period for its pursuit of sales of Rekognition. Google dropped out of the bidding for a $10 billion Department of Defense cloud contract, JEDI, due to factors including ethical concerns.[39]

Brad Smith, president of Microsoft, called in June 2018 for government regulation of facial recognition technology. At the same time, shareholders were publicizing a letter to Amazon asking the company to halt sales of its facial recognition product and advocate researchers were making known errors in the quality of Amazon's product. Google also spoke up at this time to announce a formal review structure to assess new projects, products and deals called Responsible AI Practices, a set of quarterly-updated technical recommendations and results to share with the wider AI ecosystem.

9

Similarly, in May 2018 Facebook announced an "AI ethics team" in order to "ensure that its artificial intelligence systems make decisions as ethically as possible, without biases."

In the March of the same year, Microsoft formed the AI and Ethics in Engineering and Research (AETHER) Committee bringing together senior leaders from across the company to focus on proactive formulation of internal policies and how to respond to specific issues in a responsible way. Amazon has no similar effort. Microsoft's committee however, set clear guidelines to identify, study and recommend policies, procedures, and best practices on questions, challenges, and opportunities coming to the fore on influences of AI on people and society, and invest in strategies and tools for detecting and addressing bias in AI systems and implementing new requirements established by the GDPR. Microsoft's cleaner reputation in this area is a result of these measures.

Even without committees, companies demonstrate their commitment to establish an ethical framework with new technologies by taking measures to call for their regulation, refusing to bid on or pursue contracts with the government, or establishing specialty leadership roles. This month, Microsoft turned down a sale of facial recognition software to a CA law enforcement agency, citing human rights concerns.[40] Salesforce, for example, employs a chief ethical and humane use officer. In all three of these proposed avenues, Amazon goes against the grain.

Conclusion

Proponents of the resolution urge investors to **vote in favor** of Risks of Sales of Facial Recognition Software at Amazon.com, Inc. because:
1. Amazon is exposed to financial, reputational, regulatory, legal, and human capital risk due to its sales of Rekognition.
2. Amazon is failing to address the risks of sales of Rekognition and an independent assessment is needed to ensure it will not cause harm.
3. Amazon lags peers in governance, oversight and management practices to assess and address the ethical, legal, and reputational risks associated with the use of its technology products.

For questions regarding the Amazon.com, Inc. Proposal on Risks of Sales of Facial Recognition Software at the Amazon.com please contact: Mary Beth Gallagher, Tri-State Coalition for Responsible Investment, (973) 509-8800 or mbgallagher@tricri.org

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://aws.amazon.com/products/?hp=tile&so-exp=below

[2] https://aws.amazon.com/rekognition/pricing/

[3] https://ir.aboutamazon.com/static-files/ce3b13a9-4bf1-4388-89a0-e4bd4abd07b8

[4] https://aws.amazon.com/solutions/case-studies/government-education/all-government-education-nonprofit/

10

[5] https://www.dailymail.co.uk/sciencetech/article-6555213/FBI-tests-Amazons-controversial-facial-recognition-way-catch-criminals.html

[6] https://www.seattletimes.com/business/amazon/amazon-officials-pitched-their-facial-recognition-software-to-ice/

[7] https://mashable.com/article/orlando-rekognition-amazon-surveillance/

[8] https://aws.amazon.com/rekognition/customers/

[9] https://globalnaps.org/ungp/guiding-principle-17/

[10] https://www.washingtonpost.com/opinions/facial-recognition-threatens-our-fundamental-rights/2018/07/19/a102703a-8b64-11e8-8b20-60521f27434e_story.html?utm_term=.2a5a34faf3e0

[11] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falselymatched-28

[12] https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/

[13] https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html?module=inline

[14] https://www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html

[15] https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.c8c25f7ba1f0

[16] https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 August 2, 2018

[17] https://www.vox.com/the-goods/2018/10/25/18022956/amazon-trust-survey-american-institutions-ranked-georgetown

[18] https://materiality.sasb.org/

[19] Iqra Asghar and Kade Crockford, Amazon Should Follow Google's Lead and Stop Selling Face Surveillance Tech to Cops, PRIVACY SOS (June 2, 2018), https://privacysos.org/blog/amazon-follow-googles-lead-stop-selling-facesurveillance-tech-cops/.

[20] Open Letter to Amazon Against Police and Government Use of Rekognition, International Committee for Robot Arms Control, https://www.icrac.net/open-letter-to-amazon-against-police-and-government-use-of-rekognition/.

[21] https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology/?utm_term=.eda50202710d

[22] https://www.abc15.com/decodedc/technology/bloomberg-amazon-workers-can-hear-what-you-say-to-alexa

[23] https://theharrispoll.com/HarrisPoll_Axios_MostVisible_2019.pdf

[24] https://ainowinstitute.org/AI_Now_2018_Report.pdf.

[25] https://www.markey.senate.gov/news/press-releases/after-false-matches-by-facial-recognition-technology-senator-markey-and-representatives-gutirrez-desaulnier-question-amazon-about-its-sale-of-rekognition-to-law-enforcement

[26] https://nadler.house.gov/press-release/nadler-wyden-coons-markey-booker-ask-gao-study-commercial-and-government-use-facial

[27] https://www.gao.gov/assets/700/698610.pdf

[28] https://www.blunt.senate.gov/news/press-releases/blunt-schatz-introduce-bipartisan-commercial-facial-recognition-privacy-act

[29] https://malegislature.gov/Bills/191/SD671

[30] https://app.leg.wa.gov/billsummary?BillNumber=5528&Year=2019&Initiative=false

[31] https://www.theverge.com/2019/1/29/18202602/san-francisco-facial-recognition-ban-proposal

[32] Amazon 10K for 2019 - Risk Factors discussion.

[33] https://newsroom.accenture.com/news/2016-us-college-graduates-value-culture-over-compensation-according-to-accenture-strategy-research.htm

[34] https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509

[35] https://adage.com/article/digital/millions-facebook-records-found-amazon-cloud-servers/317225

[36] https://www.perpetuallineup.org/findings/free-speech

[37] https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and

[38] https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/

[39] https://www.businessinsider.com/amazon-jedi-cloud-contract-snag-2019-2

[40] https://www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV