UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

April 3, 2019

Ronald O. Mueller
Gibson, Dunn & Crutcher LLP
shareholderproposals@gibsondunn.com

Re: Amazon.com, Inc.
Incoming letter dated March 29, 2019

Dear Mr. Mueller:

This letter is in response to your correspondence dated March 29, 2019 concerning the shareholder proposals (the "Proposals") submitted to Amazon.com, Inc. (the "Company") by the Sisters of St. Joseph of Brentwood et al. and John C. Harrington (the "Proponents"). We also have received correspondence on the Proponents' behalf dated April 2, 2019. On March 28, 2019, we issued a no-action response expressing our informal view that the Company could not exclude the Proposals from its proxy materials for its upcoming annual meeting. You have asked us to reconsider our position. After reviewing the information contained in your correspondence, we find no basis to reconsider our position.

Under Part 202.1(d) of Section 17 of the Code of the Federal Regulations, the Division may present a request for Commission review of a Division no-action response relating to Rule 14a-8 under the Exchange Act if it concludes that the request involves "matters of substantial importance and where the issues are novel or highly complex." We have applied this standard to your request and determined not to present your request to the Commission.

Copies of all of the correspondence on which this response is based will be made available on our website at http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8.shtml. For your reference, a brief discussion of the Division's informal procedures regarding shareholder proposals is also available at the same website address.

Sincerely,

Elizabeth M. Murphy
Associate Director

Enclosure

cc: Sanford J. Lewis
sanfordlewis@strategiccounsel.net

DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the company in support of its intention to exclude the proposal from the company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes and rules administered by the Commission, including arguments as to whether or not activities proposed to be taken would violate the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversarial procedure.

It is important to note that the staff's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly, a discretionary determination not to recommend or take Commission enforcement action does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the company's management omit the proposal from the company's proxy materials.

SANFORD J. LEWIS, ATTORNEY

April 2, 2019

Via electronic mail

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Amazon.com Request for Reconsideration regarding proposals on facial recognition

Ladies and Gentlemen:

I am writing on behalf of the Proponents, John C. Harrington and the Sisters of St. Joseph of Brentwood et al. of the 2019 shareholder proposals (the "Proposals") submitted to Amazon.com (the "Company") regarding facial recognition. We are writing in response to the March 29, 2019 request for reconsideration and appeal to the Commission ("Reconsideration Letter") submitted on behalf of Amazon.com by Ronald O. Mueller of Gibson Dunn. A copy of this reply is being submitted concurrently to Mr. Mueller.

SUMMARY

The Reconsideration Letter purports to offer four grounds for overturning the Staff's no action ruling of March 28. (Our prior February 28, 2019 reply to the no action request is attached.) In our opinion, the purported bases for exclusion of the Proposals are without foundation in the shareholder proposal rules, and would reverse decades of Staff and Commission rulings finding that proposals addressing human rights abuses are appropriate for shareholder consideration.

First, the Reconsideration Letter asserts that the topic of the Proposals is better suited to congressional deliberations than review by shareholders. There is no basis under Rule 14a-8 for reconsideration on the basis of this "leave it to the legislature" argument; in fact, such a ruling would be inconsistent with the Commission's guidance that in order to transcend ordinary business, a proposal should address a topic of widespread debate. The suggested principle for exclusion, without legal basis in the Rule, also would directly contradict the existing ordinary business rule, under which the expressed interest in the issue by lawmakers are grounds for *non-exclusion*. Further, deference for human rights protection to government legislative bodies, whether in the US, at the local level, or internationally is inconsistent with the long history of shareholder proposals addressing human rights implications of company operations.

Second, the Reconsideration Letter asserts that the subject matter of the Proposals does not fulfill the relevance requirements of Rule 14a-8(i)(5) as "otherwise significantly related" to the Company. However, the Proponents have provided ample evidence that the issues of public trust

regarding privacy and civil liberties associated with facial recognition have *already* implicated the Company's reputation – with its employees, with civil society, and with the public. These consumer trust issues are central to the Company's business model, and are vulnerable to breaches. At the same time, they are directly connected to a substantial pipeline of additional artificial intelligence products that will continue to raise the bar on sustaining consumer trust against ever greater intrusions on privacy and civil liberties.

Third, the reconsideration request asserts that the Proposals should be excludable as lacking nexus under Rule 14a-8(i)(7), mischaracterizing the Proposals as directed toward "misuse" of Rekognition. The Company's Amazon Web Services (AWS) segment is a leading cloud computing company that is integrating facial recognition software to its services, which the Proposals assert is being done at risk to civil liberties, privacy and public trust in the Company's products and services. The nexus of this issue to the Company is clear. The Proposals are not directed toward mere misuse, but toward the *capacities* and inevitable concerns raised when the software is placed in the hands of government and police entities. Prior decisions of the Staff finding nexus and rejecting Rule 14a-8(i)(7) claims where proposals addressed internet technology and services companies lack of measures to prevent surveillance or interference with freedom of expression in repressive countries are directly apropos.

In short, the Reconsideration Letter provides no new information or basis for reconsidering the Proposals, but merely is an attempt to recycle the Company's failed arguments. The reconsideration request should be denied. Further, the Reconsideration Letter provides no basis for Commission Review – it contains no substantial policy issues appropriate for Commission review under Rule 14a-8 and Paragraph 202.1(d) of Title 17 of the Code of Federal Regulations.

ANALYSIS

1. The Company's assertion that issues of facial recognition and human rights are best addressed by legislative bodies is inconsistent with the shareholder proposal rule.

Initially, the Reconsideration Letter suggests that the issues of jeopardy to civil and human rights raised by the Company's marketing of facial recognition are "more appropriately left to Congress and others charged with establishing applicable legal standards." The Letter states:

> The Company understands why people want there to be oversight and guidelines put in place to make sure facial recognition technology cannot be used to discriminate. In this regard, on February 7, 2019, after the Request Letter was submitted, the Company stated its view that the issues around how law enforcement uses facial recognition technology are appropriately addressed through a national legislative framework that protects individual civil rights and ensures that governments are transparent in their use of facial recognition technology. The Company continues to believe that the issues raised by the Proposals should be addressed by legislative processes and in this context are not appropriate for the shareholder proposal process.

Under existing Commission and Staff rulings, widespread controversy and even the interest of Congress in an issue, provides supporting evidence that a proposal addressing a significant policy issue transcends ordinary business. Furthermore, under the shareholder proposal rule, it provides a basis for *non*-exclusion, not for exclusion. The Reconsideration Letter has not even attempted to reconcile this "leave it to Congress" position with the ordinary business rule.

Consider the underlying assumption: How has this approach of leaving containment of human rights abuses to government legislative bodies worked out in authoritarian regimes? For that matter, how will this work out in the US in a world of deadlocked congressional deliberations? The Proponents believe the natural outcome of the Company's approach is clear: it would expose shareholders and society to substantial risks while legislative solutions may or may not be adopted in the various affected jurisdictions.

As we documented in our initial response, Company officers including the CEO are aware of the severe civil liberties risks associated with the technology. We quoted CEO Jeff Bezos acknowledging the risk. "…I worry that some of these technologies will be very useful for autocratic regimes to enforce their role." He asserted that society will develop an "immune response," making it the responsibility of society, rather than the Company, to prevent these harms. The American Civil Liberties Union (ACLU) has referred to this current company approach as a "break-then-fix" approach.

The Amazon VP's plea in the February blog post that the "technology should not be banned or condemned because of its potential misuse" is precisely the type of concern that was at issue in a landmark shareholder proposal ruling in *Medical Committee for Human Rights v. SEC,* 432 F.2d 659 (D.C. Cir. 1985). The case clarified that deciding whether to ban a product that is so capable of deployment by government to harm human rights is not a choice reserved to board and management, but rather is one on which shareholders have a right and duty to participate through the shareholder proposal process.

<u>The Reconsideration Letter presents no new facts or evidence regarding the "leave it to Congress" argument.</u>

We wish to note as well that the Reconsideration Letter may create the impression that the Company has found a new basis for reconsideration when it states on page 4 that "on February 7, 2019, after the Request Letter was submitted, the Company stated its view that the issues around how law enforcement uses facial recognition technology are appropriately addressed through a national legislative framework." *However, this is not a presentation of new information*. The publication of the blog, noted in footnote 4 of the Company Reconsideration Letter was discussed *at length* in our response letter submitted February 28, 2019. See Proponents' response letter, page 5.

2. Proponents provided ample demonstration of relevance for purposes of Rule 14a-8(i)(5).

Staff Legal Bulletin 14I described the Staff's new approach to considering issues of relevance under Rule 14a-8(i)(5).

> Where a proposal's significance to a company's business is not apparent on its face, a proposal may be excludable unless the proponent demonstrates that it is "otherwise significantly related to the company's business." For example, the proponent can provide information demonstrating that the proposal "may have a significant impact on other segments of the issuer's business or subject the issuer to significant contingent liabilities." The proponent could continue to raise social or ethical issues in its arguments, but it would need to tie those to a significant effect on the company's business. The mere possibility of reputational or economic harm will not preclude no-action relief. In evaluating significance, the staff will consider the proposal in light of the "total mix" of information about the issuer.

In this instance, the Proponents have met the burden of Rule 14a-8(i)(5) as well as the Staff Legal Bulletin in demonstrating that the Proposals are "otherwise significantly related" to the Company's business. The Proponents provided ample evidence that the identified issues related to Rekognition "may have a significant impact on other segments of the issuer's business."

The evidence provided goes far beyond the "mere possibility of reputational or economic harm" demonstrating that in the "total mix" of information about the issuer, the facial recognition software represents a serious threat to expectations of trust and privacy. Our reply letter documented that the facial recognition program itself implicates significant levels of sales, and that the issues of privacy expectations and trust are likely to spill over to the entirety of Amazon Web Services, as well as the Company's broader business model and product pipeline.

The Proposals implicate core intangible assets of the Company as a digital economy company whose business relies on the trust of consumers. They also have a direct and financially relevant connection to the pipeline of artificial intelligence products announced by the Company and made public through patent applications. The Company's pipeline of artificial intelligence technologies includes several interwoven technologies intended to build upon facial recognition software. This product pipeline is directly jeopardized by the violation of consumer or public expectations regarding privacy and civil liberties.[1]

Therefore, this is far from an instance of "the mere possibility of reputational or economic harm." The proof of reputational harm already raised by the technology has been demonstrated,

---

[1] A historically relevant example of application of Rule 14a-8(i)(5) in consideration of a company's future business was addressed in *American Telephone and Telegraph Company* (January 16, 1992). The proposal related to guidelines for the Company's future operations with the Soviet Union and Mainland China. The Staff noted that while the proposal related "to relatively insignificant amounts, the issues raised on the face of the proposal and the Company's current and future dealings combine to indicate that the proposal may be considered otherwise significantly related to the Company's business."

including by the unprecedented Amazon.com employee protest in opposition to the marketing of facial recognition. The negative impact on the Company's reputation also affected its quest for locating a headquarters operation in New York City, where this issue was raised by a number of speakers as among the reasons why the Company did not deserve public trust to operate in New York City.

The ACLU, along with a coalition of civil rights organizations, sent a public letter to the Company in May 2018 demanding that it stop selling its Rekognition software to government agencies.[2] That letter was followed by another open letter sent on January 15, 2019, by a coalition of more than 85 groups. These groups expressed their concern for how the Company's Rekognition technology threatens community safety, privacy, and human rights.[3]

Further, there is ample precedent at Facebook detailed in the Proponent's original reply to understand how reputation risk is as an amplifier of economic damage when things don't go as the company intended and disruptive uprisings of consumer concern interrupt the trusting relationship between a digital economy company and its consumers. As such, the related issues of investment risk should be of grave concern to "Mr. and Mrs. 401(k)." Many an investment plan, including "socially responsible" portfolios include very substantial holdings in Amazon.com. The Proponents believe that the Proposals have identified a significant financial vulnerability for the Company: the collision between marketing of artificial intelligence tools, and maintenance of the Company's relationship with the public by it preserving consumer trust, and ensuring the Company will not violate expectations of privacy, fairness and human rights protection.

Applying a Rule 14a-8(i)(5) standard that would require proof of economic harm beyond the proof provided by the Proponents in this matter would be incompatible with investor rights to utilize the shareholder proposal process to examine and address risks to digital economy companies. The request for reconsideration and exclusion under Rule 14a-8(i)(5) should be denied.

3. The Proposal addresses a significant policy issue with nexus to the Company as a cloud computing sector leader, and does not merely focus on "misuse" of a Company product.

The Company's Amazon Web Services (AWS) segment is the leading cloud computing company, and is integrating facial recognition software to its services, which the Proposals assert is being done at risk to civil liberties, privacy and public trust in the Company's products and services. The cloud computing segment, AWS, began as a side project to meet the Company's internal needs, but now it plays a dominant role in the marketplace:

> Quietly launched as a side business in 2006, AWS was a simple proposition that hit

---

[2] 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-face-surveillance-tech-cops/.
[3] *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/.

> at exactly the right time. It allows anyone, from random individuals to tech start-ups to billion-dollar companies like Slack, to offload the need to run and maintain servers. It controls a huge chunk of the cloud-server market — about 40 percent in mid-2017, per Synergy Research. (By itself, it controls more of the cloud-computer market than its three closest rivals, IBM, Google, and Microsoft, combined.)
>
> If you use Netflix, Pinterest, Airbnb, Slack, or any of Adobe's web services, you're indirectly using AWS. And, of course, you use AWS anytime you use any Amazon product, whether that's Alexa or Amazon Video. New York (and many, many other media publishers) use AWS. In general, cloud computing, as pioneered by AWS, has allowed for the tremendous shift in how the internet behaves and feels — why everything feels like a piece of software, even if very little of it is actually stored on the physical device you're using.[4]

The same cloud computing technologies that empower our digital world can also invade our privacy and violate our civil liberties — an intrinsic risk for the Company's cloud computing segment. ***As such, the nexus of the Proposals' subject matter to the Company is clear.***

The Company is in a central position of concern to civil society, as recognized by the ACLU, because the Company's cloud computing infrastructure and product pipeline is proceeding quickly to build the technological backbone for a surveillance society, and treating the related issues of civil rights and privacy as a problem for someone else to solve.

Such issues of human and civil rights have already been demonstrated in Staff decisions to have a nexus to the Company in *Amazon.com, Inc.* (March 25, 2015). While there have been few, if any, Staff decisions on artificial intelligence, directly analogous Staff decisions have recognized the nexus of issues of human rights and repression for leading internet service providers and technology companies. For instance, in *Cisco Systems, Inc.* (September 19, 2002), found not excludable under Rule 14a-8(i)(7), the proposal targeted government controls on the internet that implicated human rights in China. It requested that Cisco report to shareholders on the capabilities of its hardware and software products that allow monitoring and/or recording of internet traffic, and that act as firewalls that prevent internet traffic from reaching intended addressees or downloads from reaching selected sites outside of the country. The example is directly analogous to the present Proposals, where capabilities of software to violate human rights are at issue.[5]

---

[4] Jake Swearingen, When Amazon Web Services Goes Down, So Does a Lot of the Web, New York Magazine, March 2, 2018. http://nymag.com/intelligencer/2018/03/when-amazon-web-services-goes-down-so-does-a-lot-of-the-web.html

[5] See also *Yahoo! Inc.* (April 5, 2011) where the proposal directed the company to formally adopt human rights principles specified in the proposal to guide its business in China and other repressive countries. In *Yahoo! Inc.* (April 13, 2007) the proposal requested that management institute policies to help protect freedom of access to the internet. At issue in both cases was the potential denial of human rights in repressive countries linked to company policies that had placed inadequate constraints on the company's business relations with governments in repressive countries, and in both instances, the Staff found that the proposals were not excludable pursuant to Rule 14a-8(i)(7).

The Proposals are not addressed toward mere misuse.

The Reconsideration Letter attempts to minimize and characterize the Proposals as focused on whether "a small segment of the customer base" *might* "misuse" the "output" of the product. Substantial concerns are far from "theoretical", and have been identified by the ACLU and others, not the least of which is the lack of transparency and accountability of the Company on these technologies. While "misuse" of facial recognition may lead to violations of civil liberties, it is also the inherent capacities of the technology itself – especially with the added layers of artificial intelligence technology now in the Company's own product pipeline to provide the engine for regionalized surveillance, tracking of protesters, discrimination, etc. – that are central to the Proposals, rather than the mere possibility of misuse by some customers.

The Company's Reconsideration Letter focusing on misuse amplifies the Request Letter's legalistic posture. In the original Request Letter (page 4) the Company asserted that its acceptable use policy for AWS prohibits:

> "[a]ny activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation. This includes the violation of any laws related to privacy, discrimination, and civil rights."

Thus, by a legalistic turn of phrase, the Company might seem to make any such violations solely a matter of accountability for the end users, and not for the Company.[6]

Reviewing the language of the Proposals it is clear that the *capacities* of the facial recognition software, rather than "misuse," is the focus of the Proposals:

> "Civil liberties organizations, academics, and shareholders have demanded Amazon halt sales of Rekognition to government, concerned that our Company is enabling a surveillance system "readily available to violate rights and target communities of color." Four hundred fifty Amazon employees echoed this demand, posing a talent and retention risk.
>
> Brian Brackeen, former Chief Executive Officer of facial recognition company Kairos, said, "Any company in this space that willingly hands [facial recognition] software over to a government, be it America or another nation's, is willfully endangering people's lives."

Of particular and immediate concern is the potential that "Rekognition could facilitate immigrant surveillance and racial profiling." Other major digital technology companies are awaiting government regulation before going to market. For instance, one of the Proposals notes that:

> Microsoft has called for government regulation of facial recognition technology,

[6] As we discussed in our prior reply letter, the Company's February 7 blog post, the company acknowledged that those rights remain ill-defined.

saying, "if we move too fast, we may find that people's fundamental rights are being broken."

However, nowhere in either of the Proposals is there a limited focus on misuse. The first Proposal is not focused on misuse, but rather on prohibiting "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."

The second Proposal adds a focus on the Board of Directors which it asserts has not "rigorously assessed the magnitude of risks to our Company's financial performance associated with the privacy and human rights threat to customers and other stake holders… We believe the Board of Directors' fiduciary duty of care extends to thoroughly evaluating the impacts on reputation and shareholder value, of any surveillance technology our Company produces or markets on which significant concerns are raised regarding the danger to civil and privacy rights of customers and other stakeholders."

In contrast to the Proposals here, the decision cited by the company in *FMC Corp.* (avail. Feb. 25, 2011, *recon. denied* Mar. 16, 2011) requested moratoriums on marketing of pesticides "*where there is documented misuse of products.*" [7]

Instances of potential misuse by governments do not render a proposal excludable under Rule 14a-8(i)(7).

The relationship between shareholder proposals and potential government uses and misuses of a company's products was addressed in *Medical Committee for Human Rights v. SEC,* 432 F.2d 659 (D.C. Cir. 1985). *Medical Committee* involved a proposal at Dow Chemical seeking an end to the production and sale of napalm during the Vietnam War. The proposal requested the Board of Directors adopt a resolution setting forth an amendment to the Composite Certificate of Incorporation of the Dow Chemical Company that napalm shall not be sold to any buyer unless that buyer gives reasonable assurance that the substance will not be used on or against human beings.[8] It is worth noting that the controversy also revolved around assertions that the government was "misusing" the technology, *by spraying it on civilians as well as on its intended target of vegetation.* An academic review[9] of the history surrounding napalm being sold by Dow

---

[7] The Reconsideration Letter also cites to cases that are inapposite here because they do not focus on a significant policy issue. *Danaher Corp.* (avail. Mar. 8, 2013, *recon. denied.* Mar. 20, 2013); and *Amazon.com, Inc.* (March 17, 2016). In *Danaher Corp.* the Staff treated the proposal on mercury pollution from dental amalgam as focused on an issue of "product development" without recognition of a significant policy issue that transcended ordinary business. In *Amazon.com, Inc.,* where the issue was whether the company had responsibility for electronic waste generated as a result of its sales to consumers, the Staff similarly granted no action relief by noting that the proposal relates to the company's products and services and *does not focus on a significant policy issue*.

[8] The SEC initially found the proposal was excludable. The appellate court in Medical Committee remanded the no-action decision to the SEC for further deliberation by the SEC consistent with the court's conclusion that the SEC should defend the rights of shareholders to file proposals directed toward significant social issues facing a company.

[9] Stephen M. Contakes and Taylor Jashinsky, Ethical Responsibilities in Military-Related Work: The Case of

Chemical to the government notes:

> In continuing as a napalm supplier… Dow was not so much adjudicating benefits and harms associated with napalm's intended use. Instead it weighted benefits associated with napalm's intended use against harms from its expected misuse, ultimately deciding in favor of the former.
>
> … Dow sought assurance that its napalm would not be misused through a strategy that combined governmental assurances with eyewitness testimony and medical reports.
>
> …Dow did not push the crucial questions about the US rules of engagement which governed how napalm could be used. These rules represented a case of moral slippage….

As we noted in our Reply, the court in *Medical Committee* concluded that shareholders nevertheless had a right to weigh in through the shareholder proposal process on whether the company should continue to market the controversial product, regardless of whether it was being misused by government. In the present matter, the Proponents view the Company's posture that society rather than the Company is responsible for the implications of its technology as a similar example of "moral slippage."

The dramatic implications for civil and human rights associated with dissemination of facial recognition technologies, are considered by many to be on par with the decision to sell napalm at issue in *Medical Committee*. On March 4, 2019, the New York Times published an article titled "Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts" that examines how the Company's advanced technologies puts it in a similar position to Dow Chemical when it was awarded a Department of Defense contract to produce napalm.[10] The napalm being sold by Dow Chemical was only one of a broad array of products being produced and marketed by Dow Chemical. The government was, in the words of the Reconsideration Letter, "one subset of its customers."

Napalm, HYLE--International Journal for Philosophy of Chemistry, Vol. 22, No. 1 (2016), pp. 31-53. http://www.hyle.org/journal/issues/22-1/contakes.htm

[10] "All told, the $5 million napalm contract most likely cost Dow Chemical billions of dollars. And it was the kind of unforced error that could have been avoided if company executives had listened to early signs of opposition, done some risk analysis and changed course.

Today's biggest tech companies are in a similar spot. Many of them, such as Amazon and Microsoft, are among the most beloved brands in the world. They employ lots of conscientious, idealistic engineers whose skills are highly valuable, giving them considerable leverage in discussions about company values. And they are operating in an era of heightened consumer sensitivity — in which one misstep can tarnish a brand for years.

…supporters of these deals argue that some of the technologies being offered to the military, such as image-recognition algorithms that can help better target drone strikes, could save civilian lives.

But the truth is that tech companies have absolutely no idea how the government will use their products in the future — and how the political landscape might shift, throwing them into an unwanted spotlight."

Kevin Roos, " Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts," *The New York*

The fact that some customers may exploit or "misuse" capacities of the company's software to violate human rights is not an issue immune from consideration through shareholder proposals where the overriding concerns address a significant policy issue, as is the case in the present Proposals. Prior Staff decisions denying ordinary business exclusion regarding guns[11] and opioids[12] could have just as easily been framed as a matter of "misuse" or "abuse" by end-users. The fact that guns, napalm, opioids, or facial recognition software might be *misused* by the end consumer, including by violating the seller's terms of sales or service, does not eliminate the nexus of accountability of the producers in the eyes of society, or under the shareholder proposal rule.

The Reconsideration Request has provided no basis for finding the Proposals excludable under Rule 14a-8(i)(7).

4. The Company has provided no new basis for reconsidering Rule 14a-8(i)(11) exclusion.

The Company Reconsideration letter includes in footnote 10 a reiteration of the Company's argument that the two Proposals are duplicative. The Company has provided no new evidence or argument in support of this claim, and therefore has not provided a basis for reconsideration on this issue.

5. The Reconsideration Request sets forth no basis for Commission Review

The issues raised by the Reconsideration Letter do not satisfy the standard for Commission review of Staff determinations under Rule 14a-8 as set forth in Paragraph 202.1(d) of Title 17 of the Code of Federal Regulations. They do not "present questions to the Commission which involve matters of substantial importance and where the issues are novel or highly complex."

The only "novel" issue raised in the reconsideration letter is the assertion that the topics of the proposal are better taken up in "national legislative determination" rather than through the

---

Times, March 4, 2019. https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html

[11] The present Proposals are also in accord with the Staff decision to deny exclusion under Rule 14a-8(i)(7) in *Sturm, Ruger & Company, Inc.* (March 5, 2001) in which the proposal requested that the Board of Directors provide a comprehensive report on company policies and procedures aimed at stemming the incidence of gun violence in the United States. In the supporting statement of that proposal, the proponents requested that the report include a description of…. [n]ames and descriptions of products that are developed or are being developed for a combination of higher caliber/maximum capacity (which would yield maximum power) and greater concealability. In essence, the proposal was directed in part toward disclosure of actions that the company was taking to prevent the most likely scenarios of misuse or abuse of the company's guns. Notably, the company had attempted to discourage the proposal by shifting focus to consumer end responsibility, noting to the proponents that: "Ownership of a firearm is a serious responsibility which requires the owner and users to take appropriate safety precautions, based upon individual circumstances beyond our control. If they are not willing to accept those serious responsibilities, then we urge them not to purchase or use any firearm." Despite the attempt to shift the onus of responsibility to end-users, the significant policy issue associated with gun sales and impacts on society caused the proposal to transcend ordinary business and not be excludable under Rule 14a-8(i)(7).

[12] *Walgreens Boots Alliance, Inc.* (November 20, 2018) urging a report to shareholders describing the corporate governance changes the Company has implemented since 2012 to more effectively monitor and manage financial and reputational risks related to the opioid crisis, nonexcludable under Rule 14a-8(i)(7).

shareholder proposal process. As documented above, Commission review on this basis has no foundation or consistency with the shareholder proposal rule.

The other assertions regarding Rules 14a-8(i)(5) and Rule 14a-8(i)(7) represent a mundane misapplication of the rules and precedents by the Company, not by the Staff, and do not merit Commission deliberation.

CONCLUSION

Based on the foregoing, we believe it is clear that the Company has provided no basis for reconsideration. As such, we respectfully request that the Staff inform the Company that it is denying the reconsideration request. Furthermore, the Proposals and Reconsideration Letter present no issue meriting Commission consideration under Paragraph 202.1(d) of Title 17 of the Code of Federal Regulations.

If you have any questions, please contact me at (413) 549-7333 or sanfordlewis@strategiccounsel.net.

Sincerely,

Sanford Lewis

cc: Jay Clayton, Chairman
Robert J. Jackson, Jr., Commissioner
Hester M. Peirce, Commissioner
Elad L. Roisman, Commissioner
William Hinman, Director, Division of Corporation Finance
Mark Hoffman, Amazon.com, Inc.
John C. Harrington
Mary Beth Gallagher, Tri-State Coalition for Responsible Investment

SANFORD J. LEWIS, ATTORNEY

February 28, 2019
Via electronic mail

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Shareholder Proposal to Amazon.com, Inc. Regarding Facial Recognition on Behalf of John C. Harrington and the Sisters of St. Joseph of Brentwood, et al.

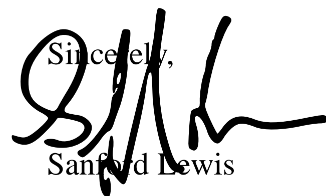
Ladies and Gentlemen:

John C. Harrington and the Tri-State Coalition for Responsible Investment, the Sisters of St. Joseph of Brentwood, the Sisters of St. Francis of Philadelphia, the Sisters of St. Francis Charitable Trust, Assad Asset Management, and the Maryknoll Sisters of St. Dominic, Inc. (the "Proponents") are beneficial owners of common stock of Amazon.com, Inc. (the "Company") and have submitted shareholder proposals to the Company. I have been asked by the Proponents to respond to the letter dated January 23, 2019 ("Company Letter") sent to the Division of Corporation Finance of the Securities and Exchange Commission by Ronald Mueller of Gibson Dunn. In that letter, the Company contends that the proposals may be excluded from the Company's 2019 proxy statement. A copy of this letter is being emailed concurrently to Ronald Mueller of Gibson Dunn.

Our response includes a Summary indexed with page references to the detailed Analysis and Response that follows. Based on these materials, we believe it is clear that the Company has provided no basis for the conclusion that the Proposals are excludable from the 2019 proxy statement pursuant to Rule 14a-8.

We respectfully request that the Staff inform the Company that it is denying the no-action letter request. If you have any questions, please contact me at 413 549-7333 or sanfordlewis@strategiccounsel.net.

Sincerely,



Sanford Lewis

cc: Ronald Mueller

PO Box 231 Amherst, MA 01004-0231 • sanfordlewis@strategiccounsel.net • (413) 549-7333

SUMMARY
Response to No Action Request
2019 Proxy Season

Amazon, Inc.
Proxy Proposals regarding
Facial Recognition Technologies

References in this Summary are to pages of
attached ANALYSIS AND RESPONSE

Amazon, Inc. is at the center of a controversy regarding the sale of facial recognition services raising significant civil rights and privacy protection concerns. Two proposals regarding this facial recognition technology were submitted to the Company.

The first submitted proposal (the "Prohibition Proposal") requests that the Board of Directors prohibit sales of any 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. In its supporting statement the Proposal recommends 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, as well as how Amazon would mitigate these risks and 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.

The second submitted proposal ("the Disclosure Proposal") requests the Board of Directors commission an independent study of Rekognition (the Company's facial recognition technology) and report to shareholders. The requested report would examine: the extent to which such technology may endanger, threaten, or violate privacy and or civil rights, and unfairly or disproportionately target or surveil people of color, immigrants and activists in the United States; the extent to which such technologies may be marketed and sold to authoritarian or repressive foreign governments, identified by the United States Department of State Country Reports on Human Rights Practice; and the financial or operational risks associated with these human rights issues. The full text of the proposals is included as Appendix A to this document.

The Company Letter claims that both proposals (hereafter, "the Proposals") are either excludable under Rule 14a-8(i)(7) as relating to the Company's ordinary business, or Rule 14a-8(i)(5) as relating to operations that are not economically significant or otherwise "significantly related to the Company's business".

Rule 14a-8(i)(7)

The Board of Directors did not provide an opinion or evidence pursuant to Staff Legal Bulletin 14I to support the claim that the issues raised by the Proposals are an insignificant public policy issue for the Company. While the submission of such an opinion is not obligatory, in this instance the subject of the Proposals has been in the center of a highly visible debate and controversy, implicating privacy, discrimination and civil liberties concerns, making a compelling case for its significance as a public policy issue. In fact, after submission of the Company Letter, another spokesman for the Company has called for government regulation of the Company's facial recognition technology, an acknowledgment that existing laws and regulations are inadequate to effectively control the controversial impacts of the technology. Pages 3-4.

The Company's approach of bringing this technology to market despite threats posed to public welfare and consumer trust has been called a "break-then-fix" approach. This has led to an enormous public backlash – with extensive media coverage of NGO activity including the ACLU, opposition to the technology by the Company's own employees, US congressional calls for further analysis of the technology, and corrosion of public trust, including in the context of the Company's efforts to build a second headquarters in New York City. Pages 5-6, 15-20, 31.

Staff precedents demonstrate that when a management issue such as a decision to sell a product or market a particular technology rises to the level of controversy present with regard to facial recognition technology, the subject matter transcends ordinary business and a proposal addressing it is not excludable under Rule 14a-8(i)(7). Pages 6-9.

Despite the Company Letter's attempt to remove nexus by portraying the significant impacts of this technology as occurring only *after* consumers or governments acquire it, or claiming that significant impacts would occur only as a result of end user customers' (i.e., not the Company's) actions, a strong nexus to the Company exists, and is demonstrated by Staff precedent, the ongoing global controversy regarding facial recognition technology, growing opposition from the Company's employees, US congressional interest, and debate on the technology's use by domestic and foreign governments. Pages 10-20.

Rule 14a-8(i)(5)

The Company Letter claims that the Proposals relate to operations that are not economically significant or otherwise "significantly related to the Company's business."

However, the subject matter of the Proposals is "otherwise significantly related to the company" and the Proposals are not excludable under Rule 14a-8(i)(5). The facial recognition software is a high visibility offering of an estimated $23 billion revenue segment of the Company, Amazon Web Services. The controversy surrounding the technology threatens the relationship of trust between the Company and its consumers, employees, and the public at large. The company's products include a number of other products – Alexa, Ring, and Eero — that will face a spillover effect if Amazon's status as a trusted company 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 is on a collision course with just such concerns. Pages 20-25.

Rule 14a-8(i)(11)

The Company Letter further asserts that if the Rule 14a-8(i)(7) and Rule 14a-8(i)(5) objections are found inapplicable, that the later submitted proposal (the Disclosure Proposal) may be excluded under Rule 14a-8(i)(11) because it substantially duplicates the previously submitted Prohibition Proposal.

In this instance, the Proponents believe that there would be significant value to investors in voting on both Proposals, each containing a distinct request.

The thrust of the first submitted proposal is for shareholders to vote on whether the Company should halt sales of facial recognition software to the government; the later submitted proposal simply invites a vote on conducting a study on the societal issues concerning facial recognition software.

Therefore, the proponents believe that the shareholders, board and management would benefit, and the functioning of corporate democracy would be best served, through the additional information that will be provided by allowing both Proposals to proceed to a vote. Further, the clear distinction between the questions presented by the Proposals would be evident to shareholders. Pages 32-33.

ANALYSIS AND RESPONSE
TO EXCLUSION CLAIMS

Response to No Action Request
2019 Proxy Season

Amazon, Inc.
Proxy Proposals regarding
Facial Recognition Technologies

BACKGROUND

Facial recognition technology is an artificial intelligence tool. The technology has become possible as a result of recent advances in computer-driven "machine learning". An Amazon technology that is part of Amazon Web Services (AWS), Rekognition is being deployed for facial recognition and recognition of other imagery in photographic and video recordings. The Company Letter notes:

> Since being introduced in 2016, Amazon Rekognition has been applied extensively for various commercial uses, such as to identify public figures who are speaking at large events or live on-air, search through large volumes of media assets, authenticate attendees at live events to shorten lines, build educational apps for children, power social media apps that allow users to see which celebrities they most closely resemble, enhance security through multi-factor authentication, prevent package theft, and identify for removal third-party-generated website content for suggestive or explicit content, among numerous other examples. Amazon Rekognition has also proven useful to aid government and private groups in law enforcement, such as to prevent human trafficking, inhibit child exploitation, and reunite missing children with their families.

AWS is by far the largest provider of Internet "cloud" services in the world, with 2018 revenue of about $23 billion.[1] As promoted on the AWS web site, Rekognition is marketed as one app 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.

While Rekognition's uses are often beneficial, the negative impacts on privacy, civil liberties and discrimination threaten to overshadow the benefits. The Proposals urge the Company to take a more deliberative approach to stewardship of this technology, by assessing and disclosing risks, and by halting sale of the technology to government agencies until an evaluation is conducted demonstrating that technology does not contribute to actual or potential violations of civil and human rights.

---

[1] https://www.zdnet.com/article/in-2018-aws-delivered-most-of-amazons-operating-income/.
[2] https://aws.amazon.com/rekognition/pricing/.

The rapid and largely unregulated deployment of Rekognition has made it one of the most controversial technologies in the world today. Facial recognition raises multiple concerns involving civil and human rights and government surveillance.

The trajectory of usage suggests that facial recognition technology can hyper-charge government surveillance of citizens. Amazon's Rekognition technology, especially in combination with related innovations and development by the Company for which it seeks to secure patents, could provide the backbone for a "surveillance society" in which citizens are surveilled on a 24/7 basis. At stake in the US are fundamental human rights — including the First and Fourth amendment rights of free speech, freedom of association, privacy, and due process. In other countries, where those rights are not even established, the potential for abuse is even greater.

The Company's goodwill and brand are highly dependent on consumer and public trust. The deployment of this technology in the hands of government agencies like the FBI and police departments poses a potent threat of disrupting that trust relationship. Yet Rekognition has already been marketed to and deployed by governments and government agencies. Reported consideration of the technology by Immigrations and Customs Enforcement (ICE) has amplified these issues of trust.

The American Civil Liberties Union (ACLU)[3] has noted that "[f]ace surveillance also 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." The FBI is currently petitioning for face recognition systems to be exempt from the prohibitions on tracking people during the exercise of their right to free speech. 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. The Georgetown Law Center on Privacy and Technology, a leading academic analyst of privacy issues, explains[4]:

> Despite the fact that leading law enforcement agencies—including the FBI and the Department of Homeland Security (DHS)—have explicitly recognized the potential chilling effect of face recognition on free speech, we found that almost none of the agencies using face recognition have adopted express prohibitions against using the technology to track political or other First Amendment activity.
>
> The federal Privacy Act generally prohibits the government from keeping records "describing how any individual exercises rights guaranteed by the First Amendment."[5] But the FBI is now petitioning for its face recognition system to be exempt from the enforcement of this provision.

If the technology is deployed in countries outside the US, where there are fewer safeguards of

---

[3] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

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

[5] The Administrative Procedure Act, 5 U.S.C. § 552a(e)(7) (2014).

civil and human rights, the threats may be magnified further. For instance, in China, the government is already using a pervasive system of cameras and facial recognition technology.

"Companies can't continue to pretend that the 'break-then-fix' approach works," Nicole Ozer, technology and civil liberties director for the ACLU of California, said in a statement to Fortune magazine.[6] "We are at a crossroads with face surveillance, and the choices made by these companies now will determine whether the next generation will have to fear being tracked by the government for attending a protest, going to their place of worship, or simply living their lives."

The issues surrounding the facial recognition controversy are attracting enormous public attention. A Google search for the term "Facial Recognition" yields approximately 347 million results. A Google search combining the terms "Facial Recognition" and "Inaccurate" yields approximately 18.7 million results; the combination of "Facial Recognition" and "Controversy" yields approximately 17.6 million results.

In a sense, the Proposals may be seen as an application of 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. The Company'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 report on these impacts and risks, is therefore necessary here to ensure sound stewardship at the Company.

The Proposals suggest that the Company can and should undertake more high-level oversight of these issues before unleashing 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.

I. Rule 14a-8(i)(7)

The Company Letter asserts that the Proposals are excludable under Rule 14a-8(i)(7) because the Proposal merely addresses ordinary business (the sale of a technology) without addressing a transcendent policy issue.

The legal framework for Rule 14a-8(i)(7) developed by the Commission, Staff and the courts, including under Staff Legal Bulletin 14I, begins with the question of whether the subject matter of the proposal is one of "ordinary business." That is, is it a topic that is integral to the day-to-day management and operations of the company?[7] These "nitty-gritty" operational considerations might

---

[6] http://fortune.com/2019/01/15/coalition-pressures-amazon-microsoft-google-facial-recognition-surveillance-government/.

[7] Staff Legal Bulletin 14H published in 2015 described ordinary business in terms of the "nitty gritty" of

include, for instance, decisions regarding whether to sell a particular product or service, use a particular technology, hire a particular individual or group, or to decide where to invest or expand capital. In general, such ordinary business questions are reserved to the board and management. The exception is where the subject matter addresses a significant policy issue.

If the proposal's underlying subject matter transcends the day-to-day business matters of the company and raises significant policy issues it may be appropriate for a shareholder vote. Staff determinations have made it clear that "transcendent" issues that constitute significant policy relate to whether the proposal addresses an issue of widespread public debate. Examples recognized by the Commission and the Staff include such topics as human rights, discrimination, environmental impact, and climate change. Numerous other categories of public controversy have been recognized.

In the event that the proposal relates to a significant policy issue, the proposal generally will not be excludable under Rule 14a-8(i)(7) as long as a sufficient nexus exists between the subject of the proposal and the company.[8] Does the subject matter relate significantly to the company's business or strategy? The Staff has extended an invitation to the board of directors of each company, under Staff Legal Bulletins 14I and 14J, to provide evidence and findings to assert and demonstrate that an issue is insignificant for the company. Proponents are also expected to continue to provide their own evidence regarding these questions of significance to the company. If there is a reasonable basis for concluding that a proposal's subject matter represents a significant policy issue with a connection to the company, it transcends ordinary business and is not excludable.[9]

In the present instance, the Company Letter argues that that the Proposals are excludable under Rule 14a-8(i)(7) because they address an ordinary business matter — the sale of a particular technology — without addressing a transcendent policy issue. The following discussion will demonstrate that, to the contrary, the Proposals address a transcendent policy issue with a very clear nexus to the Company.

The Board of Directors would be hard-pressed to demonstrate that this is an insignificant policy issue for the company.

While the Company Letter includes an extended discourse on Staff precedents where Staff found no transcendent policy issue to elevate the proposal from a focus on ordinary business, this discourse does not make up for the notable absence of a board of directors opinion asserting that the Proposals do not address a significant policy issue for the Company. While the inclusion of such an opinion and evidence considered by the board is not obligatory under Staff Legal Bulletin 14I, it also is clear that the absence of such an expression of opinion by the Board may speak loudly on its own. Here, it appears that the Board of Directors would be hard-pressed to claim that the raging public controversy surrounding the Company's high visibility product is insignificant to the Company's ability to earn the continued trust of consumers and the public, had such an attempt been made. Meanwhile, in the wake of this silence, the Company has felt

corporate management: "a proposal may transcend a company's ordinary business operations even if the significant policy issue relates to the "nitty-gritty of its core business." This makes the distinction between and ordinary business determination and a significant policy determination clear.

[8] Staff Legal Bulletin No. 14E (October 27, 2009).

[9] A further basis for possible exclusion under Rule 14a-8(i)(7) is micromanagement, which is not at issue in the current request.

compelled to repeatedly respond to the emerging controversy in defense of the product. The Company's response level to this controversy further evidences the significance its technology has for the Company.

In an attempt to minimize the concerns regarding abuse, the Company Letter references the existing Acceptable Use Policy, which prohibits usage for *illegal* purposes or to *violate rights*. However, these 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 ineffectual.

Significantly, after the Company Letter was submitted, other communications from a Company representative undermine this policy's reassurance and acknowledge public concerns. In February 2019, Amazon Web Service's Global Public Policy VP, Michael Punke, published a blog post that outlined several 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.[10] The blog post[11] notes a series of issues that must be addressed in public policy:

1. Facial recognition should always be used in accordance with the law, including laws that protect civil rights.

2. When facial recognition technology is used in law enforcement, human review is a necessary component to ensure that the use of a prediction to make a decision does not violate civil rights.

3. When facial recognition technology is used by law enforcement for identification, or in a way that could threaten civil liberties, a 99% confidence score threshold is recommended.

4. Law enforcement agencies should be transparent in how they use facial recognition technology.

5. There should be notice when video surveillance and facial recognition technology are used together in public or commercial settings.

This unusual call for regulation by the Company of its technologies that have already been brought to market and made available to government agencies amplifies what a significant policy issue this is. The 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 the continued lack of regulation further threaten the Company and its technology. Notably, the recent blog post by the AWS VP concluded with a plea against banning the technology:

> New technology should not be banned or condemned because of its potential

[10] Reported in https://futurism.com/amazon-regulation-facial-recognition-tech.
[11] https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

> misuse. Instead, there should be open, honest, and earnest dialogue among all parties involved to ensure that the technology is applied appropriately and is continuously enhanced.

In light of these risks and uncertainties, as well as the plea for dialogue with stakeholders direct from a Company executive, it is frankly difficult to understand why the Company is opposing the current Proposals. The Proposals themselves seem 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.[12]

Moreover, 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 Filing on Form 10-K:

> 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.[13]

The Company's communications regarding the need for regulation is powerful evidence that the Proposal addresses a significant policy issue.

Most telling and strong evidence of the validity of the Proposals is provided by the plea by VP Punke that "New technology should not be banned or condemned because of its potential misuse."

Jeff Bezos, the Company's CEO , spoke to CNN:[14]

> He compared current technology to the invention of books, which have been used for good and bad, including creating "fascist empires."
>
> "The last thing we'd ever want to do is stop the progress of new technologies," said Bezos.
> Eventually, society will develop an "immune response" to bad uses of technology, according to Bezos.

---

[12] While the Proponents hope their proposals will inspire just such a dialogue with their fellow shareholders and with the management and board, the Proponents are also aware that some may question whether the Company's quest for government regulation is disingenuous. For instance, the Company belongs to the Internet Association in California, along with Twitter and Uber, which has spent about $200,000 on lobbying since the state adopted the California Consumer Privacy act last year. "There's going to be a fight here to weaken it," said Mary Stone Ross an advocate of the law https://www.washingtonpost.com/technology/2019/02/08/theres-going-be-fight-here-weaken-it-inside-lobbying-war-over-californias-landmark-privacy-law/?u.

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

[14] https://www.cnn.com/2018/10/15/tech/jeff-bezos-wired/index.html.

> "…I worry that some of these technologies will be very useful for autocratic regimes to enforce their role ... But that's not new, that's always been the case. And we will figure it out."

The Company's technological artificial intelligence (AI) "flywheel" is rapidly moving AI technologies from development to market, including into rights-jeopardizing uses by government.[15]

The CEO's assumption that *society* will eventually place limits and develop an "immune response" to abuses – while the company abstains from placing effective limits on its own – has been referred to as a "break-then-fix" approach. Nongovernmental organizations and academics are demanding the Company cease selling Rekognition technology to government agencies[16]. The American Civil Liberties Union (ACLU), along with a coalition of civil rights organizations, sent a public letter to the Company in May 2018 demanding that it stop selling its Rekognition software to government agencies[17]. That letter was followed by another open letter sent on January 15, 2019, this time by a coalition of more than 85 activist groups, including the ACLU, the National Lawyers Guild chapters, and Freedom of the Press Foundation. These groups expressed their concern for how the Company's Rekognition technology threatens community safety, privacy, and human rights.[18]

If the Company's technology may dramatically undermine civil rights and fuel tyrannical and autocratic regimes, is the release of that technology still a choice that is reserved to management? The legal history of the shareholder proposal process provides a compelling indication that this is not the type of issue that is reserved to board and management, but rather one that goes to the core of shareholders' rights and duties to exercise the instruments of corporate democracy.

The shareholder right and duty to weigh in on a company's impacts on society was addressed in *Medical Committee for Human Rights v. SEC,* 432 F.2d 659 (D.C. Cir. 1985), in which the U.S. Court of Appeals for the D.C. Circuit found that shareholder proposals do not concern ordinary business when they raise issues of corporate social responsibility or question the "political and moral predilections" of board or management. The takeaway from this decision is that board and management have no monopoly on expertise over investors when it comes to guiding company strategy on issues with broad and significant social consequence. Investors are entitled to weigh in through the shareholder proposal process.

Medical Committee involved a proposal at Dow Chemical seeking an end to the production and sale of napalm during the Vietnam War. The proposal requested the Board of Directors adopt a resolution setting forth an amendment to the Composite Certificate of Incorporation of the Dow

---

[15] https://www.wired.com/story/amazon-artificial-intelligence-flywheel/.
[16] Danielle Abril, *Coalition Pressures Amazon, Microsoft, and Google to Keep Facial Recognition Surveillance Away From Government*, Fortune (Jan 16, 2019), http://fortune.com/2019/01/15/coalition-pressures-amazon-microsoft-google-facial-recognition-surveillance-government/.
[17] 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-face-surveillance-tech-cops/.
[18] *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/.

Chemical Company that napalm shall not be sold to any buyer unless that buyer gives reasonable assurance that the substance will not be used on or against human beings.[19]
In deciding *Medical Committee*, the court noted that it would be appropriate for shareholders to use the mechanism of shareholder democracy to pose "to their co-owners, in accord with applicable state law, the question of whether they wish to have their assets used in a manner which they believe to be more socially responsible." The court further noted such a choice was not appropriately reserved to the board or management.

The dramatic impacts associated with dissemination of facial recognition technologies are on par with the decision to sell napalm at issue in *Medical Committee*. As stated in *Medical Committee:*

> [T]he clear import of the language, legislative history, and record of administration of section 14(a) is that its overriding purpose is to assure to corporate shareholders the ability to exercise their right — some would say their duty — to control the important decisions which affect them in their capacity as stockholders and owners of the corporation. (SEC v. Transamerica Corp., 163 F.2d 511, 517 (3d Cir. 1947), cert. denied, 332 U.S. 847, 68 S. Ct. 351, 92 L. Ed. 418 (1948)).
>
> * * *
>
> What is of immediate concern…is the question of whether the corporate proxy rules can be employed as a shield to isolate such managerial decisions from shareholder control. After all, it must be remembered that "[t]he control of great corporations by a very few persons was the abuse at which Congress struck in enacting Section 14(a)." SEC v. Transamerica Corp., supra, 163 F.2d at 518. We think that there is a clear and compelling distinction between management's legitimate need for freedom to apply its expertise in matters of day-to-day business judgment, and management's patently illegitimate claim of power to treat modern corporations with their vast resources as personal satrapies implementing personal political or moral predilections. It could scarcely be argued that management is more qualified or more entitled to make these kinds of decisions than the shareholders who are the true beneficial owners of the corporation; and it seems equally implausible that an application of the proxy rules which permitted such a result could be harmonized with the philosophy of corporate democracy which Congress embodied in section 14(a) of the Securities Exchange Act of 1934.

Strategic business choices regarding whether to produce and sell products with large impacts on society have been baked into the shareholder proposal process since the *Medical Committee* decision, with the right of shareholders to file proposals on an array of strategic choices regarding issues such as human rights, discrimination, environmental impact, and climate change.

---

[19] The SEC initially found the proposal was excludable. The appellate court in Medical Committee remanded the no-action decision to the SEC for further deliberation by the SEC consistent with the court's conclusion that the SEC should defend the rights of shareholders to file proposals directed toward significant social issues facing a company.

Here, the Proposals would have shareholders vote on whether the Company should halt sales of facial recognition technology to government agencies until these issues are resolved – representing exactly the type of shareholder determination that has long been considered protected and appropriate under the shareholder rule. The Company's statement that a "technology should not be banned or condemned because of its potential misuse" is precisely the type of concern that was at issue in *Medical Committee.* This is a choice that is not reserved to board and management, but on which shareholders have a right and duty to participate through the shareholder proposal process.

Staff determinations support recognition of major company controversies as a significant policy issue.

While the Company Letter cites a series of Staff rulings in which exclusion was allowed in relation to product selection criteria and other ordinary business matters, the common thread in those cases is the lack of an overriding, significant policy issue. Viewing the larger body of Staff rulings, however, it is apparent that when the magnitude of a controversy relating to a company rises to the level of the one in the current Proposals, it will lead the Staff to find a significant policy issue transcends ordinary business.

The prohibition on proposals that focus on products necessarily gives way if the evidence presented by the Proponent documents a significant point of conflict and controversy facing the company. Relevant to the present matter is *Quaker Oats Company* (March 28, 2000), in which the proposal requested that the board (1) adopt a policy of removing genetically engineered crops, organisms, or products thereof from all products sold or manufactured by Quaker, where feasible, until long-term testing has shown that they are not harmful to humans, animals, and the environment, with the interim step of labeling and identifying these products, and (2) report to shareholders by August 2000. The Staff was unable to concur that the company was entitled to exclude the proposal in reliance on Rule 14a-8(i)(7), due to the presence of significant policy issues. The context – a lack of proven safety – is apropos in the present instance as well. In *Quaker Oats*, the proponent argued:

> We believe that it is clear beyond cavil that the manufacture of food products which utilize crops which have been genetically altered, and whose safety has not yet been proven, is a significant policy issue for a registrant….

Even a registrant which is one of the largest producers of genetically altered seed agrees that the safety of crops produced by such seed is not proven. Thus, a recent article in Business Week (December 20, 1999) quoted DuPont's CEO as follows:

> Even staunch bio-tech food backers agree [that we just don't know for certain about the safety of genetically altered materials]. "**We don't have all the answers and to pretend that we do, or to brush off concern as unfounded, is to be arrogant and reckless,"** said DuPont Chief Executive Charles O. Holliday, Jr. in a recent speech. [Emphasis added]

Amazon is in a parallel situation with its Rekognition technology to that of Quaker in the

deployment of GMO's. As discussed above, Amazon's own representatives have implicitly acknowledged, by their call for government regulation of their own technology, that the technology is currently being applied without adequate safeguards in place. The consequences of untested GMO's were placing public health at risk; in this instance, the severe risks to privacy, democracy and civil liberties identified by critics are every bit as substantial in regard to their societal impacts.

Another instance of how "sale of a particular product" can be transcended by a significant policy issue is exemplified by *Exxon Mobil Corporation* (March 23, 2000). There, the proposal requested that Exxon Mobil adopt a policy to promote renewable energy sources, develop plans to help bring bioenergy and other renewable energy sources into Exxon's energy mix and advise shareholders regularly on these efforts. The company argued that this was directing the company to undertake the sale of a specific product – renewable energy. The proponent argued that the proposal was focused on the transcendent policy issue of climate change, and the Staff declined to allow exclusion under Rule 14a-8(i)(7).

A high visibility conflict that places a company or sector in the public spotlight, has played a role in how a significant policy override functions in relation to proposals attempting to dictate company advertising. There is a broad expectation and generally, a record of Staff exclusions preventing a proposal from dictating the content of a company's advertising. Yet in *UST Inc.* (February 22, 1999), the Staff declined to allow exclusion of a proposal requesting that the board of a tobacco company implement a policy of submitting advertising campaigns to independent testing to ensure that they are not more appealing to children than to adults. The evidence presented by the proponents principally focused on a single *New York Times* article that described certain tobacco documents demonstrating that at least one of the nation's largest cigarette companies had been, for decades, courting young smokers as young as 14, and regarding them as the future of their business. They described concrete strategies being deployed, such as the placement of advertising, and internal memoranda discussing that the "brand must increase its share penetration among the 14- 24 age group." In light of the degree to which the tobacco companies were directly in the crosshairs of public attention over these revelations, the content of advertising, so frequently treated as excludable, was in this instance found to transcend ordinary business.[20] The present company finds itself in a similar precarious spotlight on the issue of facial recognition, with extensive media coverage and congressional scrutiny.[21]

The current proposal, because it is focused on a set of high visibility controversies and concerns

---

[20] *See also, Loews Corporation* (February 22, 1999).

[21] Another example of significant policy issues leading to an allowance for proposals directed toward products sold by companies involves past decisions regarding the prevention of animal cruelty allowed proposals directed toward products sold by companies when they were connected to a significant policy issue facing restaurant chains. *Outback Steakhouse, Inc.* (March 6, 2006)(poultry slaughter methods); *Wendy's Int'l, Inc.* (Feb. 8, 2005)(involving food safety and inhumane slaughter of animals purchased by fast food chains); *Denny's* (March 17, 2009)(commit to selling at least 10% cage-free eggs by volume), *Wendy's International, Inc.* (February 19, 2008)(report on the economic feasibility of committing to purchase a percentage of its eggs from cage-free hens), and *Bob Evans Farms, Inc*. (June 6, 2011)(phase-in the use of cage-free eggs in Bob Evans restaurants). A common theme in these past decisions based on the successful arguments of the proponents was that the item in question represented a significant part of the ingredients featured in restaurant products, and was relevant to the restaurant chain's reputation. The same is true in regard to the present Company.

raised by recent reported events, is nonexcludable under Rule 14a-8(i)(7). Although proposal addressing choice of technologies *without* a significant policy issue would be excludable, the explosion of concern regarding the company's facial recognition software – widespread debate – represents a crisis in management of privacy and civil liberties issues by the Company that calls for elevated response through the proposal process.

The record of decisions by the Staff where consumer rights and interests were at stake across a broad population elevates many issues from ordinary business to significant policy issue. For instance, for a time the Staff allowed exclusion of proposals relating to subprime lending and predatory lending – issues that related to the treatment of individual consumers. After the financial crisis, however, proposals addressing the details of lending practices became fair game as a subject of proposals. In each of the following determinations, no-action relief was denied under Rule 14a-8(i)(7): *Wells Fargo & Company* (March 11, 2013) (proposal requested that the board conduct an independent review of internal controls to ensure that its mortgaging and foreclosure practices do not violate fair housing and fair lending laws to report to shareholders); *JPMorgan Chase & Co.* (March 4, 2009) (proposal recommended that the company issue a report related to its credit card marketing, lending, collection practices, and the impacts the practices have on borrowers).[22]

Nexus

The Company Letter claims that there is no nexus for the focus on the Company's sale of these products, because the abuses and the rights violations would be committed by the Company's customers and therefore be out of the Company's control. For instance, the Company Letter notes:

> any unlawful use of Amazon Rekognition by the Company's customers would violate the contractual terms on which the Company has made its product available. As such, the Proposals do not transcend the Company's ordinary business operations, and instead address the Company's relationships with its customers. The products and services that the Company

---

[22] Similarly, proposals on diversity and gender were once excludable as employment related issues. However, in 1998 the Commission issued the "Final Rule: Amendments to Rules on Shareholder Proposals," 17 CRF Part 240, Release No. 34-40018, which reversed the Cracker Barrel no-action letter concerning the Division's approach to employment-related shareholder proposals raising social policy issues. The Commission stated:

> "Since 1992, the relative importance of certain social issues relating to employment matters has reemerged as a consistent topic of widespread public debate. In addition, as a result of the extensive policy discussions that the Cracker Barrel position engendered, and through the rulemaking notice and comment process, we have gained a better understanding of the depth of interest among, shareholders in having an opportunity to express their views to company management on employment-related proposals that raise sufficiently significant social policy issues."

In the Final Rule the Commission recognized that shareholders should have the right to express themselves on significant policy issues related to employment, whether they be matters of social policy or such significant issues as plant closings, executive compensation, or golden parachutes. This has been applied in numerous Staff decisions. For example, in *Citigroup Inc.* (February 2, 2016), the proposal directly asked the company to prepare a report demonstrating that the company does not have a gender pay gap. The Company attempted to assert that this related to employee relations and wages therefore would be excludable as ordinary business. Following the precept established in the 1998 release, the Staff stated that it was unable to concur that Citigroup may exclude the proposal under rule 14a-8(i)(7).

> decides to offer through its AWS business, including Amazon Rekognition, constitute ordinary business matters for the Company.…The Proposals relate instead to what certain of the Company's customers may do with the output that is generated based on data that its customers provide and process through, and the confidence level they establish for, their data runs using Amazon Rekognition.

Similarly, the Company Letter states:

> The Proposals further focus not on the Company's use of Amazon Rekognition, but instead its potential problematic use by one subset of its customers — specifically, governments and law enforcement. The vast majority of customers who use Amazon Rekognition do not fall within this category.

The Company position that abuses of a technology that it releases to the market are the responsibility of the end users, including those end users that may abuse the technology, such as governments, is a dangerous and flawed position, that also would have justified exclusion of the Dow Chemical *Medical Committee* proposal on napalm – after all, the atrocities were being committed in the hands of government, not the company.

The Company Letter's logic would also have led to exclusion of *Yahoo! Inc.* (April 5, 2011), in which Yahoo! requested permission to omit a shareholder proposal asking the company to formally adopt human rights principles to guide its business in China and other repressive countries. Yahoo! Sought exclusion by arguing that the human rights abuses were not under its control, but the Staff did not concur, reasoning that the proposal focused on the significant policy issue of human rights.

Issues of human and civil rights, such as those raised by facial recognition technology, have already been demonstrated in Staff decisions to have a nexus to Amazon. In *Amazon.com, Inc.*(March 25, 2015), the proposal urged the Board of Directors to report to shareholders on Amazon's process for comprehensively identifying and analyzing potential and actual human rights risks of Amazon's entire operations and supply chain (a "human rights risk assessment") including human rights principles used to frame the assessment; methodology used to track and measure performance; nature and extent of consultation with relevant stakeholders in connection with the assessment; and Actual and/or potential human rights risks identified in the course of the human rights risk assessment related to (a) Amazon's use of labor contractors/subcontractors, temporary staffing agencies or similar employment arrangements (or a statement that no such risks have been identified). In that instance, despite focus of the proposal on day-to-day issues like the use of laborers and temporary staffing agencies, the Staff denied an exclusion under Rule 14a-8(i)(7).

The Company Letter also attempts to make a legalistic argument regarding nexus, that any end-users that are violating rights are violating the "Acceptable Use Policy" and therefore this is not an issue with a nexus to the company. The practical reality expressed by the Company's own 10-K risk factors statement that the law currently is ambiguous regarding such technologies, and expressed by the VP that regulation is needed, deflates this attempt to portray an arm's length

relationship to the abuses that will inevitably follow the sale of its largely unregulated technology.

As demonstrated below, the barrage of negative media focused on Amazon, congressional interest in Amazon's role in this issue, NGO pressure campaigns, and urgent pleas from employees and experts, demonstrate a clear nexus to the Company.

Global debate and controversy demonstrate nexus between the Proposals' subject matter and the Company.

Amazon's Rekognition has become a flashpoint of controversy involving a subject that implicates a significant social policy issue and presents real and critical risks to the Company's reputation, including the willingness of consumers to trust the company to defend their privacy and civil and human rights. 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. Proponents believe Rekognition threatens civil and human rights and the Company's relationship of trust with customers and the public, and as a consequence also threatens Amazon's long-term prospects.

The Company Letter attempts to characterize facial recognition technology as a narrow issue with little social significance, the importance of which hinges entirely on the accuracy of the technology. While the accuracy of facial recognition systems is a concern, for billions of people around the globe whose human rights are neglected by autocratic government regimes, there are additional and more fundamental issues, including whether facial recognition should be deployed at all because of the role the technology plays in enabling ubiquitous government surveillance.

Human rights organizations, for example, 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."[23] And in India, a country where Amazon has said it seeks to dramatically grow the Company's presence, the government is in the process of face scanning more than 1.3 billion people.[24] In the United Kingdom, a man was recently fined after refusing to be scanned by controversial facial recognition cameras being trialled by London's Metropolitan Police.[25]

Scholars Woodrow Hartzog and Evan Selinger have written:[26]

> We believe facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It's the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits

[23] 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.
[24] https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html.
[25] https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.htmlc.
[26] https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

> both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering.

Clare Garvie, of Georgetown Law's Center on Privacy & Technology, has written:[27]

> A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn't commit. 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.

In December 2018, the highly-regarded AI Now Institute at New York University warned:

> The events of this year have strongly underscored the urgent need for stricter regulation of both facial and affect recognition technologies. Such regulations should severely restrict use by both the public and the private sector, and ensure that communities affected by these technologies are the final arbiters of whether they are used at all. This is especially important in situations where basic rights and liberties are at risk, requiring stringent oversight, audits, and transparency. Linkages should not be permitted between private and government databases. At this point, given the evidence in hand, policymakers should not be funding or furthering the deployment of these systems in public spaces.[28]

According to Todd Pastorini, executive vice president and general manager of DataWorks Plus, a facial recognition technology company that sells to numerous U.S. local police departments: "I estimate that less than 5 percent of all law enforcement agencies in the United States use facial recognition, but five years from now it maybe closer to 10 percent. ...in the Northeast, and the states of Michigan and Pennsylvania, they have a statewide deployment of facial recognition."[29]

In the United States, legislation that would ban government use of facial recognition technology has been recently introduced in the states of Massachusetts[30] and Washington[31] and in the city of San Francisco.[32] 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.

---

[27] https://www.washingtonpost.com/opinions/facial-recognition-threatens-our-fundamental-rights/2018/07/19/a102703a-8b64-11e8-8b20-60521f27434e_story.html?utm_term=.2a5a34faf3e0.
[28] *AI Now Report 2018*, AI Now Institute at New York University (December 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf.
[29] http://www.govtech.com/public-safety/Orlando-Police-to-Launch-Round-Two-of-Facial-Recognition-Testing.html.
[30] https://malegislature.gov/Bills/191/SD671.
[31] https://app.leg.wa.gov/billsummary?BillNumber=5528&Year=2019&Initiative=false.
[32] https://www.theverge.com/2019/1/29/18202602/san-francisco-facial-recognition-ban-proposal.

Facial recognition technology has stirred protest in the U.S. In July 2018, more than 150,000 people signed a petition protesting Amazon's sale of Rekognition to government agencies. Amazon also received a coalition letter signed by nearly 70 organizations representing communities nationwide, as well as a letter from Amazon shareholders.[33] In January 2019, a coalition of more than 85 activist groups sent letters to Microsoft, Amazon, and Google pressing them not to sell their facial recognition technology to the government for surveillance.[34]

Amazon competitors in the technology field, Microsoft and Alphabet, have also spoken out publicly. Alphabet, parent of Google, in December 2018 said it has opted to not yet offer facial recognition technology, writing:[35]

> [L]ike many technologies with multiple uses, facial recognition merits careful consideration to ensure its use is aligned with our principles and values, and avoids abuse and harmful outcomes. We continue to work with many organizations to identify and address these challenges, and unlike some other companies, **Google Cloud has chosen not to offer general-purpose facial recognition APIs before working through important technology and policy questions**. [Emphasis added]

Brad Smith, president of Microsoft, called in June 2018 for government regulation of facial recognition technology, writing:[36]

> Facial recognition technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression. These issues heighten responsibility for tech companies that create these products. In our view, they also call for thoughtful government regulation and for the development of norms around acceptable uses. In a democratic republic, there is no substitute for decision making by our elected representatives regarding the issues that require the balancing of public safety with the essence of our democratic freedoms. Facial recognition will require the public and private sectors alike to step up – and to act.

Although the Company Letter might be read to imply that the Company's Acceptable Use Policy provides adequate protection against these concerns, other communications from the Company clearly contradict this position. For example, in the face of the groundswell of concern by NGOs and civil liberties experts, a leading company spokesman, as discussed above, has tempered the Company's position, calling for government regulation and "dialogue" among stakeholders, including shareholders.

---

[33] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/over-150000-people-tell-amazon-stop-selling-facial.
[34] http://fortune.com/2019/01/15/coalition-pressures-amazon-microsoft-google-facial-recognition-surveillance-government/.
[35] https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/.
[36] https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

Facial recognition has been, and continues to be, a topic of widespread public attention and global media coverage. It is discussed and debated on a daily basis by technology experts, members of the U.S Congress, state and local government officials, and civil and human rights advocates. Members of Congress have written multiple letters to CEO Jeff Bezos expressing concerns about Amazon's Rekognition product.[37] Amazon employees have also expressed deep concern as well as outrage at the Company's policies and practices regarding Rekognition.[38] Civil and human rights organizations are leading high-profile campaigns relating to Rekognition questioning the Company's commitment to ethics and corporate responsibility.[39]

The Washington Post, in an editorial echoing the opinions of many experts, stated:[40]

> [W]idespread real-time recognition, unchecked, could allow government to scan the face of any American at any time, enabling a low-cost comprehensive tracking system of every civilian. China's surveillance state gives some idea of how the technology may be abused...We carry our faces with us everywhere we go. Society might be safer if we simply tolerated the intrusion. It might also be less free.

The Company's response to criticism so far has lacked transparency. MIT's Joy Buolamwini, one of the world's leading experts on facial recognition technology, has identified concerns regarding whether Rekognition may be significantly biased in having less accuracy in recognizing faces of people of color and also making false identifications of people of color. Her critique of the Company, the Company's rebuttal, and her reply to that are viewable online.[41] However, she

---

[37] 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.

[38] https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac.

[39] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/over-150000-people-tell-amazon-stop-selling-facial.

[40] https://www.washingtonpost.com/opinions/facial-recognition-could-make-us-safer--and-less-free/2018/12/25/391ccd00-f994-11e8-8c9a-860ce2a8148f_story.html?utm_term=.977e1127b791.

[41] There are ongoing concerns regarding race and gender bias in facial recognition technology. An M.I.T. study by Joy Buolamwini, a seasoned researcher of bias in algorithms and machine learning, found that Amazon had an error rate of 31% when identifying the gender of women with dark skin (notably finding that Oprah Winfrey was 76.5% likely to have a male gender label), but was 100% successful at identifying the images of light-skinned men. Joy Buolamwini, *Response: Racial and Gender bias in Amazon Rekognition—Commercial AI System for Analyzing Faces* (Jan. 25, 2019), https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

However, the Company's general manager of artificial intelligence, Dr. Matt Wood, said the Company's own internal study found no major difference in gender classification across all ethnicities, while noting the M.I.T. study did not reflect Amazon's internal research, and did not use the latest version of Rekognition. Zoe Kleinman, *Amazon: Facial Recognition Bias Claims are 'Misleading'*, BBC News (Feb. 4, 2019), https://www.bbc.com/news/technology-47117299.

Buolamwini has addressed Dr. Wood's criticism by stating the M.I.T. study used "profile images of people looking straight into a camera", rather than using more difficult real-world conditions, thus making it easier for Rekognition to have accurate results despite their low accuracy rate. She also argued that although Amazon's benchmark of over 1 million faces may have performed well internally, the skin types used in the benchmarks is not known and

reports that despite her attempt to engage with the company on these issues, her experience in true engagement has been most disappointing: "Amazon's approach thus far has been one of denial, deflection, and delay. We cannot rely on Amazon to police itself or provide unregulated and unproven technology to police or government agencies."[42]

Employee opposition to selling Rekognition to government and law enforcement agencies demonstrates nexus.

In October 2018, more than 450 employees signed a letter opposing such sales, with one of them writing on the website Medium: "Amazon's website brags of the system's ability to store and search tens of millions of faces at a time. Law enforcement has already started using facial recognition with virtually no public oversight or debate or restrictions on use from Amazon."[43]

In their public letter to CEO Jeff Bezos, the hundreds of employees compared Amazon's choice to equip government agencies with surveillance technology to the role of IBM equipping Nazis during the Holocaust, saying: "we refuse to contribute to tools that violate human rights. As ethically concerned Amazonians, we demand a choice in what we build, and a say in how it is used. 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."[44]

The issue was raised by employees one month later, in November 2018, at what's been described as a company-wide meeting attended by CEO Bezos and AWS CEO Andy Jassy. Mr. Jassy reportedly said, "We feel really great and really strongly about the value that Amazon Rekognition is providing our customers of all sizes and all types of industries in law enforcement."[45]

Speaking publicly to Vanity Fair, one Amazon employee said: "Amazon is actually very good about protecting customers' security—it's probably the safest Web site to shop on. They clearly understand people value their personal information, **so them pushing technology that's such a clear violation of people's privacy and personal information is insane and hypocritical, and they know exactly why it's wrong."[46]** [Emphasis added]

U.S. Congressional interest underscores nexus.

---

therefore the performance of that benchmark cannot be adequately evaluated. Furthermore, while the Company may have an updated version of Rekognition, Buolamwini points out that older versions are still in use.

[42] https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac.
[43] https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac.
[44] https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509.
[45] https://gizmodo.com/amazon-breaks-silence-on-aiding-law-enforcement-followi-1830321057.
[46] https://www.vanityfair.com/news/2018/10/theyre-playing-both-sides-bezoss-flirtation-with-ice-appalls-amazon-employees.

The issue of facial recognition and its impact on privacy and civil liberties has been a focus of Congressional attention since at least 2012. The US Senate Subcommittee on Privacy Technology and the Law of the Committee on the Judiciary, held a hearing in 2012 entitled, *What Facial Recognition Technology Means for Privacy and Civil Liberties:*[47]

> Unlike what we have in place for wiretaps and other surveillance devices, there is no law regulating law enforcement use of facial recognition technology. And current Fourth Amendment case law generally says that we have no reasonable expectation of privacy in what we voluntarily expose to the public; yet we can hardly leave our houses in the morning without exposing our faces to the public. So law enforcement does not need a warrant to use this technology on someone. It might not even need to have a reasonable suspicion that the subject has been involved in a crime.
> -Senator Al Franken
>
> Though face recognition implicates important First and Fourth Amendment values, it is unclear whether the Constitution would protect against the challenges it presents. Without legal protections in place, it could be relatively easy for the government or private companies to amass a data base of images on all Americans. This presents opportunities for Congress to develop legislation to protect Americans. The Constitution creates a baseline, but Congress can and has legislated significant additional privacy protections. As I discuss in more detail in my written testimony, Congress could use statutes like the Wiretap Act or the Video Privacy Protection Act as models for this legislation. Given that facial recognition and the accompanying privacy concerns are not going away, it is imperative that Congress and the rest of the United States act now to limit unnecessary biometrics collection, to instill proper protections on data collection, transfer, and search, to ensure accountability, to mandate independent oversight, to require appropriate legal process before government collection, and define clear rules for data sharing at all levels.
>
> -Jennifer Lynch, Staff Attorney
> Electronic Frontier Foundation

Congressional attention turned to Amazon in 2018, as a global media firestorm was spurred by tests of Amazon's Rekognition highlighted by the ACLU. As the *New York Times* reported:[48]

> Representative John Lewis of Georgia and Representative Bobby L. Rush of Illinois are both Democrats, members of the Congressional Black Caucus and civil rights leaders.
>
> But facial recognition technology made by Amazon, which is being used by

[47] Hearing Record of the US Senate Subcommittee on Privacy, Technology and the Law, of the Committee on the Judiciary, *What Facial Recognition Technology Means for Privacy and Civil Liberties*, July 18, 2012.
[48] https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.

> some police departments and other organizations, incorrectly matched the lawmakers with people who had been charged with a crime, the American Civil Liberties Union reported on Thursday morning.
>
> The errors emerged as part of a larger test in which the civil liberties group used Amazon's facial software to compare the photos of all federal lawmakers against a database of 25,000 publicly available mug shots. In the test, the Amazon technology incorrectly matched 28 members of Congress with people who had been arrested, amounting to a 5 percent error rate among legislators.
>
> The test disproportionally misidentified African-American and Latino members of Congress as the people in mug shots.

Amazon challenged the methodology and what it called "misinterpreted results" of this test, arguing in a statement that the testers used an improper "default confidence threshold."[49]

Nonetheless, in July 2018, U.S. Senators Ron Wyden, Chris Coons, Ed Markey, and Corey Booker, and Rep. Jerrold Nadler, then the ranking Democrat on the House Judiciary Committee, called on the federal government's General Accounting Office to investigate the commercial and government use, and potential abuse, of facial recognition technology:[50]

> Given the recent advances in commercial facial recognition technology — and its expanded use by state, local, and federal law enforcement, particularly the FBI and Immigration and Customs and Enforcement — we ask that you investigate and evaluate the facial recognition industry and its government use.

Separately, Senators Edward J. Markey and Representatives Luis Gutiérrez and Mark DeSaulnier wrote to Amazon CEO Jeff Bezos:[51]

> While facial recognition services might provide a valuable law enforcement tool, the efficacy and impact of the technology are not yet fully understood. In particular, serious concerns have been raised about the dangers facial recognition can pose to privacy and civil rights, especially when it is used as a tool of government surveillance, as well as the accuracy of the technology and its disproportionate impact on communities of color.

In November 2018, Senator Markey and a group of Congressmen wrote again to Mr. Bezos:[52]

> Regrettably, despite asking you a series of questions on this subject and

---

[49] https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/.

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

[51] 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.

[52] https://www.markey.senate.gov/imo/media/doc/Bicameral%20Amazon%20Recognition.pdf.

requesting specific information in letters sent to you on July 26, 2018 and July 27, 2018, your company has failed to provide sufficient answers.

Debate on government deployment of Rekognition amplifies the need for investors and the board to know more and, therefore supports nexus.

While Amazon publicly identifies only a small handful of its Rekognition subscribers, the product could be of critical import to many current and potential AWS government customers. Amazon's AWS for Government unit currently provides cloud services to more than 2,000 government agencies.[53] AWS provides cloud services for: the U.S. intelligence community;[54] the Department of Defense;[55] the U.S. Navy,[56] Air Force[57] and Army;[58] and the Department of Homeland Security.[59]

In January 2019, the ACLU filed a Freedom of Information Act request to the Dept. of Justice "seeking records about the use of facial recognition and other biometric systems from the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA." In the request, the ACLU wrote: "Amazon Web Services (AWS) provides cloud services for all 17 United States intelligence agencies, including the DOJ and its component agencies the FBI and DEA. According to recent media reporting, the FBI is testing Amazon's Rekognition face recognition product, which is part of the suite of software products available on AWS, in a pilot program."[60]

The Company has also reportedly attempted to sell facial recognition technology to the US Immigration and Customs Enforcement (ICE). According to media reports[61] and a public records request that uncovered email exchanges between Amazon and ICE officials, in the summer of 2018, Amazon representatives met with officials from ICE and "pitched the government agency on its controversial technology that can identify people in real time by scanning faces in a video feed, documents obtained by the Project on Government Oversight show." In December 2018, an Amazon spokesperson confirmed that the company had met with ICE.[62]

Alonzo Peña, a former deputy director of ICE, said of the potential use of facial recognition by ICE that possible abuse "should be an area of concern, given this new technology—there's potential for its use to be very widespread." He also stated that the technology risks being used in ways that could disincentivize undocumented immigrants from accessing important services they

---

[53] https://aws.amazon.com/government-education/government/.
[54] https://aws.amazon.com/federal/us-intelligence-community/.
[55] https://aws.amazon.com/government-education/defense/.
[56] https://aws.amazon.com/blogs/publicsector/the-navy-turns-to-aws-govcloud-us-for-standardization-and-security/.
[57] https://aws.amazon.com/blogs/publicsector/air-force-saves-costs-and-increases-reliability-by-moving-portal-to-the-cloud/.
[58] https://www.datacenterdynamics.com/news/pentagon-cuts-950m-cloud-computing-contract-with-aws-reseller-to-65m/.
[59] https://www.fedscoop.com/dhs-moved-network-cloud/.
[60] https://www.aclu.org/sites/default/files/field_document/doj_face_recognition_foia_final_1.18.19.pdf
[61] https://www.thedailybeast.com/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech.
[62] https://www.geekwire.com/2018/amazon-selling-facial-recognition-software-ice-exec-fields-tough-questions-ny-hearing/.

might otherwise receive.[63]

Rekognition is also being marketed to state and municipal law enforcement agencies. According to the *Washington Post*, "Amazon has been essentially giving away facial recognition tools to law enforcement agencies in Oregon and Orlando...paving the way for a rollout of technology that is causing concern among civil rights groups."[64] According to documents obtained by the ACLU of Northern California, Amazon asked the sheriff's office in Washington County, Oregon to tout its experience with Rekognition to other public sector customers.

Florida's Orlando Police Department (OPD) and the city of Orlando, in July 2018, said they were "planning to launch a second round of testing of Amazon's Rekognition software." The announcement came despite a firestorm of protests earlier this year when the first pilot was conducted over several months, according to a media report.[65] "We don't know if the technology will prove to be successful, efficient and cost effective model that would enhance our public safety efforts," said the press secretary for the mayor of Orlando.[66]

In Oregon, Rekognition is being deployed by the Washington County Sheriff's Office where, according to news reports, officials have acknowledged that they are not using the product as directed by AWS. WIRED magazine recently (2 February 2019) reported:[67]

> Amazon says that its law enforcement clients use these optimal settings. But sources at the Washington County Sheriff's Office in Oregon, the only law enforcement agency that Amazon publicly cites as using Rekognition, told Gizmodo this week that the department doesn't follow Amazon's guidelines and didn't receive training to implement them. This doesn't necessarily mean that the Washington County Sheriff's Office is doing anything wrong, but it does undermine Amazon's position that the problems researchers have found in Rekognition wouldn't apply to law enforcement usage.

The ACLU's documents revealed that Washington County police have used Rekognition to identify "unconscious or deceased individuals," and "possible witnesses and accomplishes in images."[68] In a separate media report regarding the Washington County Sheriff's Office, Amazon declined to state whether it tracks the "confidence thresholds" employed by its clients.[69]

To summarize – the Proposals address a topic of widespread public debate as reflected in press coverage, congressional interest, and NGO and employee actions. The subject matter has a clear nexus to the Company. Indeed, the Company seems to be the principal public focus of concern

---

[63] https://www.thedailybeast.com/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech.
[64] https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/?utm_term=.f066ea721a67.
[65] http://www.govtech.com/public-safety/Orlando-Police-to-Launch-Round-Two-of-Facial-Recognition-Testing.html.
[66] http://www.govtech.com/public-safety/Orlando-Police-to-Launch-Round-Two-of-Facial-Recognition-Testing.html.
[67] https://www.wired.com/story/facebook-takes-down-hundreds-of-fake-pages-from-iran-security-roundup/.
[68] https://gizmodo.com/amazons-plan-to-scan-your-face-even-has-police-worried-1826231267.
[69] https://gizmodo.com/defense-of-amazons-face-recognition-tool-undermined-by-1832238149.

about the civil liberties and privacy implications of facial recognition technology and especially its deployment by government and police, particularly because some tech peers are withholding such technologies until the serious concerns and controversies can be addressed.

II. Rule 14a-8(i)(5)

The Company Letter also requests exclusion of the Proposals as lacking relevance to the Company under Rule 14a-8(i)(5). The Company Letter asserts that the subject matter of the Proposals is not financially significant to the Company's AWS business, and that the Proposals merely address potential problematic use by one subset of its customers — specifically, governments and law enforcement.

Rule 14a-8(i)(5) provides that a proposal is excludable "if the proposal relates to operations which account for less than 5 percent of the company's total assets at the end of its most recent fiscal year, and for less than 5 percent of its net earnings and gross sales for its most recent fiscal year, and is not otherwise significantly related to the company's business"

Staff Legal Bulletin 14I described the evolution of the Staff of process for considering Rule 14a-8(i)(5) claims, noting:

> Where a proposal's significance to a company's business is not apparent on its face, a proposal may be excludable unless the proponent demonstrates that it is "otherwise significantly related to the company's business." For example, the proponent can provide information demonstrating that the proposal "may have a significant impact on other segments of the issuer's business or subject the issuer to significant contingent liabilities." The proponent could continue to raise social or ethical issues in its arguments, but it would need to tie those to a significant effect on the company's business. The mere possibility of reputational or economic harm will not preclude no-action relief. In evaluating significance, the staff will consider the proposal in light of the "total mix" of information about the issuer.
>
> As with the "ordinary business" exception in Rule 14a-8(i)(7), determining whether a proposal is "otherwise significantly related to the company's business" can raise difficult judgment calls. Similarly, we believe that the board of directors is generally in a better position to determine these matters in the first instance. A board acting with the knowledge of the company's business and the implications for a particular proposal on that company's business is better situated than the staff to determine whether a particular proposal is "otherwise significantly related to the company's business." Accordingly, we would expect a company's Rule 14a-8(i)(5) no-action request to include a discussion that reflects the board's analysis of the proposal's significance to the company. That explanation would be most helpful if it detailed the specific processes employed by the board to ensure that its conclusions are well-informed and well-reasoned.

As noted earlier in this reply, the Amazon Board of Directors has declined to weigh-in with an opinion either on the significance of the issue to the Company (Rule 14a-8(i)(7)), or on relevance under Rule 14a-8(i)(5). While the absence of such an opinion is not dispositive, we believe that the absence here speaks volumes. As the Bulletin noted "A board of directors, acting as steward with fiduciary duties to a company's shareholders, generally has significant duties of loyalty and care in overseeing management and the strategic direction of the company." Here the Staff has not been provided with the Board's findings or evidence that the Proposal is *not* "sufficiently significant …. to be appropriate for a shareholder vote." The evidence from management communications, and other evidence presented in this letter, suggests that it is actually *quite* significant to the Company.

As recommended in Staff Legal Bulletin 14I, we provide here concrete evidence regarding the formidable and concrete risks to the Company's business segments and to its goodwill posed by the subject matter of the Proposal, which make the subject matter of the Proposal "otherwise significantly related" to Amazon's business.

The subject matter of the proposals is relevant to the Company's financial prospects including its most important intangible asset of consumer trust.

When a Company that is in a brand-sensitive business engages in activities that jeopardize its reputation by associating the company with human rights abuses, the Staff has long held that such a proposal is "otherwise significantly related" to the company's business. For instance, in *Marriott International Inc.* (March 18, 2002) the proposal urged the board of directors to create a committee of independent directors to prepare a report describing the risks to shareholders of operating and/or franchising hotels in Burma, including possible risks to Marriott's brand name resulting from association with human rights abuses in Burma. The Staff noted that they were unable to concur in the view that Marriott could exclude the proposal under Rule 14a-8(i)(5) since they were of the view that the proposal was otherwise significantly related to Marriott's business. Similarly, a request for a report on the economic and public relations cost relating to the company's operations in Burma, despite those operations accounting for less than 5% of the registrant's total assets, was deemed otherwise significantly related to the company in *Unocal Corporation* (April 3, 1998).

Rekognition is a significant element of the Company's AWS Segment, which generated an estimated $23 billion in revenue in 2018.

As one of the highest visibility controversies associated with Amazon Web Services, the reputation of the services, and their alignment with concerns about privacy and surveillance, provide a significant financial connection.

According to The Wall Street Journal, "AWS generated $23.3 billion in revenue for the company during the 12-month period ended Sept. 30 [2018], up 46% year over year."[70] According to CNBC, "Amazon Web Services, has actually generated the majority of Amazon's operating

[70] https://www.wsj.com/articles/amazons-cloud-hasnt-obscured-microsoft-1544184000?mod=searchresults&page=1&pos=13.

income since 2016."[71] A tech industry publication observed in February 2019 that AWS "is on pace to be a $30 billion business this year. Although still a relatively small part of the $200+ billion retail giant, AWS is the company's most profitable division, and by some distance. The importance of AWS to the company is evidenced by the fact that fully half of the bulleted highlights in Amazon's earnings release were devoted to new or enhanced AWS services."[72] "Amazon Web Services remains the key driver of Amazon profits. Although AWS is only about 11 percent of overall revenues, it continues to account for more operating profit than the rest of the company combined. Revenue growth was down less than a single percentage point from the third quarter on an annual run rate of about $30 billion."[73]

Investment analysts – including some who recommend buying Amazon shares – have noted the promising financial prospects for the Rekognition product and the Company's AWS division. Writing in Forbes magazine in July 2018 ("Be On The Lookout: Amazon Turns Its Gaze To Surveillance"), John Markman, president of Markman Capital Insight, said Amazon's shares "are cheap, given the potential size of the business opportunity."[74] The business opportunity Mr. Markman described:

> In 2016, Amazon.com leveraged its Amazon Web Services cloud … the work its engineers were doing with artificial intelligence … and its massive database of anonymized stored pictures from Amazon Prime members. And it built a new image and video analysis program called Rekognition…Surveillance is a big AI business most investors have not recognized. And it's only one application.

Jeopardizing trust regarding privacy and consumer rights: one of Amazon's most important assets

While Amazon moves objects in the material world, the core of its infrastructure is its information technologies, and its ability to gather, analyze and deploy information regarding its customers. All of this activity is grounded in the intangible asset of goodwill and trust.

Currently, the Company is reported to be the second most trusted institution in the United States[75], following the military, and consumers willingly entrust the company with information, and even acquire technological offerings like Alexa and Echo despite the growing understanding of a surveillance/privacy concern associated with the devices. Amazon has even implemented a program in which its deliveries will be brought into people's homes. All of this is built on an extraordinary relationship of trust. Key to that relationship is respect for privacy. As Amazon's Chief Executive Officer, Jeffrey Bezos has stated "Privacy is the one aspect of Alexa that Amazon can't afford to screw up."[76]

---

[71] https://www.cnbc.com/2019/02/12/how-amazon-makes-money.html.
[72] https://diginomica.com/insights-on-cloud-growth-from-aws-and-microsoft-latest-earnings/.
[73] https://siliconangle.com/2019/01/31/amazons-cloud-boosts-profits-sales-guidance-disappoints/.
[74] https://www.forbes.com/sites/jonmarkman/2018/07/24/be-on-the-lookout-amazon-turns-its-gaze-to-surveillance/#1a395ed0638d.
[75] Kaitlyn Tiffany, *In Amazon We Trust — But Why?,* Vox, (Oct. 25, 2018), https://www.vox.com/the-goods/2018/10/25/18022956/amazon-trust-survey-american-institutions-ranked-georgetown.
[76] Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Us*, The Washington

Experience at other information technology companies, notably Facebook, shows that a reputation of trust is a fragile element that can be undermined by particular incidents and applications, especially when there is an underlying consumer ambivalence regarding the information sharing aspect of the relationship. The reputation of trust can be shattered if the company's trustworthiness is betrayed by its actions.

Technology companies' vulnerability to issues of trust among their consumers is being tallied in consumer polls. Morning Consult reported on a recent poll: "Compared with a similar survey in June, consumer trust in Apple is down 7 percentage points, and trust in Google has fallen 5 points, to 60 percent. Amazon fell 6 points, to 63 percent".[77]

According to a PricewaterhouseCoopers 2018 survey, consumers "want benefits, not surveillance" and value "trust in the brand":

> PwC's Global Consumer Insights Survey reached out to more than 22,000 consumers in 27 territories across the globe during the late summer and fall 2017. We asked these consumers which factors, other than price, influence their decision to shop at a particular retailer. More than one in three (35%) ranked 'trust in the brand' as among their top three reasons[78]...
>
> Consumers want benefits, not surveillance... In the age of increasing surveillance, the biggest concerns for consumers are around being tracked.[79]

Cornerstone Capital issued a report to investors arguing that consumers' concerns regarding privacy reveal the underlying skepticism and ambivalence of consumers regarding whether provision of their personal data is an appropriate exchange for goods and services:

> A 2016 survey on data privacy by the Pew Center found that:
>
> 74% of respondents regarded it as very important that they control who can get information about them…
>
> 92% of adults agreed or strongly agreed that consumers have lost control of how personal information is collected and used by companies;

Post (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.cce0fc008398.

[77] The survey was conducted after security flaws were revealed in chips used in computers and smartphones, thereby demonstrating how security is tied with customer trust. Anna Gronewold, *Poll Shows Falling Trust in Tech Companies' Security Amid Disclosure of Chip Flaws*, Morning Consult (Jan. 10, 2018), https://morningconsult.com/2018/01/10/poll-shows-falling-trust-in-tech-companies-security-amid-disclosure-of-chip-flaws/.

[78] PwC, *Global Consumer Insights Survey 2018: Whom do Consumers Really Trust?*, at p. 2, https://www.pwc.com/gx/en/retail-consumer/assets/consumer-trust-global-consumer-insights-survey.pdf.

[79] PwC, *Global Consumer Insights Survey 2018: Whom do Consumers Really Trust?*, at p. 7, https://www.pwc.com/gx/en/retail-consumer/assets/consumer-trust-global-consumer-insights-survey.pdf.

> 68% of internet users believed current laws are not good enough at protecting people's privacy online[80]
>
> [A] 2015 Annenberg study concludes instead that many consumers allow data collection because they feel that they have no other choice — that they are resigned to sharing their data because they perceive a lack of power and agency in the marketplace. They would prefer not to share data but believe that refusing to do so would result in unacceptable costs — paying higher prices, missing contact with friends on social media, and losing access to services that feel necessary in modern society.
>
> * * *
>
> The risk for companies is that resignation evolves into active opposition or that new corporate entrants design products and services which tap into that latent discomfort and either actively block such data or figure out how to pay consumers for providing it, thereby intermediating what has, to this point, been the widespread provision of "free" data[81].
>
> At present, dissatisfaction among consumers in the US has not led to practical efforts to curtail this trend because consumers as individuals feel powerless to prevent it. But this should not be considered a stable set of circumstances. If the public perceives the rising tide of data to be unacceptably invasive of individual privacy rights, consumer resignation could eventually turn to active opposition in the form of mass, collective action resulting in stringent regulation, or widespread action by individual consumers to block the gathering of their personal data. Companies would be at heightened risk if consumer trust continues to fall[82].

<u>Precarious consumer trust jeopardized at Amazon.com.</u>

The highly visible vulnerabilities of Rekognition in highlighting the role of company technologies in privacy breaches and surveillance can easily spill over to the trust relationship that lies at the heart of Amazon's brand.

Much of Amazon's current branding is being built around so-called smart devices or speakers, including, the Echo, Dot, and Alexa smart speakers which use a voice-control system. The voice-control system activates the smart device with a trigger word (e.g., "Alexa", "Echo", "Amazon", or "Computer") and follows commands, like turning on music, or responds to basic inquiries. Alexa is able to respond because of a natural-language processing system, whose "success is

---

[80] John Wilson and Heidi Bush, *The Data Privacy Puzzle Companies gather enormous – and growing – amounts of personal data every day. What happens if consumer attitudes or regulations change?*, Corner Capital Group (Aug. 2018), at p. 13.
[81] *Id.* at p. 14.
[82] *Id.* at p. 20.

dependent on the several very sensitive microphones built into all Echo devices." As a result, "Alexa is always listening…," and once activated by a trigger word, streams users' voice to the cloud for analysis[83].

However, user experience with Alexa and Echo has begun to expose privacy and surveillance concerns, generating potential public outrage. With Alexa, the devices are capable of picking up and transmitting a consumer's private conversations to the cloud and even transmitting those conversations to others. According to Politifact[84]:

> In one highly publicized incident, a Portland family's Alexa captured a private conversation after the voice-controlled device misheard what it thought was the wake word. It later sent the audio recording to someone in Seattle whose number was stored in the family's contact list.

Amazon described the chain of events as "an extremely rare occurrence," and issued the following statement:

> "Echo woke up due to a word in background conversation sounding like 'Alexa.' Then, the subsequent conversation was heard as a 'send message' request. At which point, Alexa said out loud 'To whom?' At which point, the background conversation was interpreted as a name in the customer's contact list. Alexa then asked out loud, '[contact name], right?' Alexa then interpreted background conversation as 'right.' As unlikely as this string of events is, we are evaluating options to make this case even less likely."

Though Amazon states that such an occurrence is rare, the Echo device remains unpredictable in its functionality with an unknown frequency[85]. Washington Post's Geoffrey Fowler, who has an Echo, Google Home and Apple HomePod, explained that Amazon may have marketed Echo to consumers by ensuring them that the Company only records conversations when given a "wake word", but that this is a "misnomer" because "[t]hese devices are always awake", passively listening, and imperfectly receiving information ("false positives"). Fowler said his devices go rogue on a regular basis[86].

---

[83] Grant Clauser, *What Is Alexa? What Is the Amazon Echo, and Should You Get One?*, wirecutter (Jan. 29, 2019), https://thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one/#how-does-alexa-work.

[84] John Kruzel, *Is Your Amazon Alexa Spying on You?*, Politifact (May 31, 2018), https://www.politifact.com/truth-o-meter/statements/2018/may/31/ro-khanna/your-amazon-alexa-spying-you/.

[85] "But how often do these devices go rogue and record more than we'd like them to? Neither Google nor Amazon immediately responded to my questions about false positives for their "wake words." But anyone who lives with one of these devices knows it happens." Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Us*, The Washington Post (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.cce0fc008398.

[86] Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Us*, The Washington Post (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-

> "At least one of them starts recording, randomly, at least once per week," he wrote. "It happens when they pick up a sound from the TV, or a stray bit of conversation that sounds enough like one of their wake words." "Separating a command out from surrounding home noise — especially loud music — is no easy task. Amazon's Echo uses seven microphones and noise-canceling tech to listen out for its wake word. Doing so, it records about a second of ambient sound on the device, which it constantly discards and replaces. But once it thinks it hears its wake word, the Echo's blue light ring activates and it begins sending a recording of what it hears to Amazon's computers."

While the smart devices have limited "wake words", the Company filed a patent application that would let future versions identify statements that would allow monitoring based on interests and help the Company target consumers with related advertising.

Despite the value consumers place on trust in a company, uncertainty surrounding the frequency of such "false positives" and the unknown degree to which consumers are under surveillance make the Company vulnerable to losing customers' goodwill, along with losing a competitive market position when launching new products. The Harvard Business Review reports:

> [O]ur research shows that consumers are aware that they're under surveillance—even though they may be poorly informed about the specific types of data collected about them—and are deeply anxious about how their personal information may be used.
>
> In a future in which customer data will be a growing source of competitive advantage, gaining consumers' confidence will be key. Companies that are transparent about the information they gather, give customers control of their personal data, and offer fair value in return for it will be trusted and will earn ongoing and even expanded access. Those that conceal how they use personal data and fail to provide value for it stand to lose customers' goodwill—and their business.
>
> A firm that is considered untrustworthy will find it difficult or impossible to collect certain types of data, regardless of the value offered in exchange. Highly trusted firms, on the other hand, may be able to collect it simply by asking, because customers are satisfied with past benefits received and confident the company will guard their data. In practical terms, this means that if two firms offer the same value in exchange for certain data, the firm with the higher trust will find customers more willing to share. For example, if Amazon and Facebook both wanted to launch a mobile wallet service, Amazon, which received good ratings in our survey, would meet with more customer acceptance than Facebook, which had low ratings. In this equation,

---

about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.cce0fc008398.

trust could be an important competitive differentiator for Amazon.[87]

Characterizing reputation risk for Amazon.

Staff Legal Bulletin 14I requested that shareholders document a risk, such as reputation risk, is more than hypothetical – providing evidence. We believe we have provided sufficient evidence to demonstrate that the Rekognition technology endangers the Company's trust relationship with the public and consumers, and that it is "otherwise significantly related" under Rule 14a-8(i)(5).

Reputation analysts consider how reputation risk flows from specific events that happen at a company. For instance, a breach of privacy of a group of customers would be an event. Although the direct costs to a company (e.g. from liability suits) may be shrouded in uncertainty, from for instance, a discovery that the company is accidentally or intentionally violating customers' privacy, the magnitude of the real costs of many incidents lies in the fact that reputation "risk is a multiplier that amplifies the direct impact of an event through the loss of future revenue due to the reputational impact of the event."[88]

One measure of the cost of such events is how the market reacts. A Wharton study evaluated sudden stock price drops, defined as a drop in the company stock price that is greater than 20%, within a 10-day period relative to changes in the industry average. Stock price drops from reputational damage (related to reputation, image, pricing, and presence in the market) emerged as ***the largest category*** in the study.[89] In addition, it took an average of 80 weeks for a company stock price to recover after a sudden price drop.

Special vulnerability of the technology sector to breaches in trust.

The experience of Facebook provides ample evidence that the prominent tech sector companies, especially those that are entrusted with key consumer data, are highly vulnerable to experiencing a reputational crisis. In 2018, multiple scandals involving user privacy resulted in "a tumultuous year," for Facebook, according to a CNBC analysis, with the company's two top executives forced to testify before the U.S. Congress.

Reputational crises can turn a company around in one day, as was the case on one day in March 2018, when news that Cambridge Analytica had exploited Facebook to collect the data of more than 50 million users without their permission caused the company's stock to fall nearly 7 percent, losing more than $36 billion in value. The stock absorbed several later hits to its value, such as when COO Sheryl Sandberg testified before the Senate Intelligence Committee and had to face tough questioning regarding the failure of the company to do more to prevent Russian meddling.[90] After peaking in July, Facebook shares were down in November 2018 almost 40 percent for the year. While Facebook's share price rebounded somewhat in January 2019, it

[87] Timothy Morey, Theodore Forbath and Allison Schoop, *Customer Data: Designing for Transparency and Trust*, Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.
[88] Oliver Wyman, *The Hidden Cost of Reputation Risk*, 2017, page 4.
[89] Wharton, *Corporate Strategies for Managing Catastrophic Risks in the S&P 500* (preliminary study), 2013. Cited in Oliver Wyman, *Reputation Risk: a Rising Sea Suite Imperative*, 2014.
[90] https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html.

remains about 19% below its 2018 high.

The scandals at Facebook have "fundamentally changed how we run this company. We've changed how we build services to focus more on preventing harm. We've invested billions of dollars in security, which has affected our profitability," CEO Mark Zuckerberg told analysts in a January 2019 conference call.[91] One analyst cautioned the risk to Facebook's stock may continue to manifest in the future, when European regulators get more deeply involved in their privacy probes. Several different bodies are investigating Facebook, including the Irish Data Protection Commissioner. The consequences may not come this year, but they will eventually, said Brian Wieser, an analyst for Pivotal Research. "Unfortunately, Wall Street can be very short-sighted," he said.[92]

Such consequences can be accelerated by controversial technologies, like facial recognition features in products. Indeed, one of Facebook's regulatory problems in 2018 involved facial recognition. In April, a coalition of consumer groups filed a complaint with the Federal Trade Commission that focused on a Facebook feature that helps users identify people in uploaded photos by suggesting the names of people it recognizes. The "Tag Suggestions" feature relies on sophisticated facial-recognition software that compares faces in photos with a massive database of face templates.[93]

<u>Impact of eroding trust on featured company products and product pipeline</u>

The privacy and surveillance controversy regarding Rekognition mirrors and amplifies similar controversies regarding an array of other company offerings and activities – there is Ring, Echo and Alexa each of which is raising the bar on the level of trust and the level of potential vulnerability regarding privacy breaches. Controversies regarding Rekognition as a prematurely released surveillance technology that grossly violates people's expectations for privacy threaten to spill over to its broad platform of technologies with similar elements of surveillance and privacy violations, undermining consumer trust.

Ring, acquired last February[94] is a smart video-doorbell company that has facial and object recognition software, in addition to video recording, live video feeds, and notification capabilities. It can be mounted anywhere in or around a home, allowing consumers to keep tabs on their home while they are away. According to its founder, Ring was created with the mission of reducing neighborhood crime; however, privacy concerns exist regarding the data's accessibility, the extent of which was made known when in 2016, customers' unencrypted video feeds from every video created by every Ring camera worldwide, were reportedly made accessible to a Ukraine-based research and development team. They could easily download and share customer video files, and had access to a corresponding database linking each video file

---

[91] https://seekingalpha.com/article/4236897-facebook-inc-fb-ceo-mark-zuckerberg-q4-2018-results-earnings-call-transcript.
[92] https://www.bloomberg.com/news/articles/2019-01-30/facebook-sales-profit-beat-wall-street-estimates-shares-surge.
[93] https://www.wsj.com/articles/consumer-groups-file-ftc-complaint-against-facebook-1523025141.
[94] Laura Stevens and Douglas MacMillan, *Amazon Acquires Ring, Maker of Video Doorbells*, The Wall Street Journal (Feb. 27, 2018), https://www.wsj.com/articles/amazon-acquires-ring-maker-of-video-doorbells-1519768639/.

with specific Ring customers. Meanwhile, Ring provided executives and engineers with access to its technical support video portal, allowing unfiltered round-the-clock access to live feeds of customers' cameras.[95]

Echo is a smart speaker activated by a voice command feature of Alexa software, but a report by the advocacy group Consumer Watchdog found that the device is always listening — even when it is not activated —and charts its consumers patterns[96]. The Company has already been collecting data on when Echo is used to turn on a device, but it is now seeking to partner with smart-home gadget makers to send continuous "status reporting"— information regarding the on/off status of smart features such as lights, locks, and televisions, including the television channel[97]. Researchers have called this data collection a "Trojan horse" because the Company is presenting status reporting as a helpful feature for consumers, but in reality that information could be misused by infringing on privacy rights without permission, as a means to obtain a greater market position[98]. Privacy concerns are now heightened by the Company's filing of a patent application for an algorithm that would allow the Echo to identify statements related to hobbies, thus allowing it to target related advertising.[99]

The Company's trajectory on multiple planned product lines is vulnerable to public perception on issues of consumer privacy.

The relationship of trust the Company has built with its consumers will be tested as the Company's product pipeline, including recent acquisitions and technologies for which the Company is pursuing patents, seeks to intrude much more deeply into people's private lives.

In February 2019, the Company announced its acquisition of Eero, a technology that creates a mesh network with wireless routers and extenders that provide better coverage for home Wi-Fi networks.[100] According to the Company, it kept Eero's pre-existing privacy policy and does not currently collect personal information such as websites visited, or information about when consumers are home or away, but because Eero can link several smart devices together over a broadband network, it houses valuable marketing data regarding the types and models of smart devices owned by a particular consumer. Moreover, while there is currently a privacy policy in place for Eero consumers, worry exists surrounding the ease with which new management could update future terms of service to lessen privacy restrictions.[101]

---

[95] Sam Biddle, *For Owners of Amazon's Ring Security Cameras, Strangers May have Been Watching Too*, The Intercept (Jan. 10, 2019), https://theintercept.com/2019/01/10/amazon-ring-security-camera/.

[96] *How Google and Amazon are 'Spying' on You*, Consumer Watchdog, https://www.consumerwatchdog.org/privacy-technology/how-google-and-amazon-are-spying-you.

[97] Matt Day, *Your Smart Light Can Tell Amazon and Google When You go to Bed*, Bloomberg (Feb. 12, 2019), https://www.bloomberg.com/technology.

[98] Matt Day, *Your Smart Light Can Tell Amazon and Google When You go to Bed*, Bloomberg (Feb. 12, 2019), https://www.bloomberg.com/technology.

[99] *How Google and Amazon are 'Spying' on You*, Consumer Watchdog, https://www.consumerwatchdog.org/privacy-technology/how-google-and-amazon-are-spying-you.

[100] Therese Poletti, *Opinion: Amazon Wants to Control Your Entire House After Eero Acquisition*, MarketWatch (Feb. 12, 2019), https://www.marketwatch.com/story/amazon-wants-to-control-your-entire-house-after-eero-acquisition-2019-02-11.

[101] Dieter Bohn, *Why Amazon Buying Eero Feels so Disappointing*, The Verge (Feb. 12, 2019), https://www.theverge.com/2019/2/12/18221441/amazon-buying-eero-disappointing.

Similarly, there are patent applications underway to expand the applicability of Rekognition data — to provide a regional surveillance and tracking capacity through the technology, and to apply the facial recognition technologies to home security cameras such as Ring. At the CES tech show, Ring announced an internet-connected video doorbell small enough to fit into peepholes.[102] While it does not currently use facial recognition technology, Ring filed a patent application so that its home security cameras could use a facial-recognition system.[103]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.[104]

Two facial recognition-related patent applications[105] 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. The ACLU has strongly come out against these patent applications, arguing that such technology creates a dangerous future where the public would be subject to a widespread decentralized surveillance network.[106]

The Company also reportedly filed a patent application for an algorithm that would allow ongoing listening and detection by the Echo device to identify statements related to interests (e.g. "I like skiing"), thus allowing it to collect massive information and target related advertising.[107]

<u>The trust of the Company's employees is also being undermined by the Company's internal management and potential sale of surveillance technologies, including facial recognition.</u>

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. The patents state the aim of this technology is to improve inventory management efficiency — a pulse alert on workers' wristbands signals to a worker when their hands are in close proximity to a target bin, thereby allowing for faster retrieval of the bin's contents. However, by tracking detailed hand movements, the Company can also obtain and record highly private information, such as when an employee takes a bathroom break. This degree of monitoring and directing employees by the

---

[102] Rachel Lehrman and Joseph Pisani, *Smart but Nosy: Latest Gadgets Want to Peer Into Our Lives*, AP News (Jan 11, 2019), https://www.apnews.com/8035020f41d24847b16276b5627195c5.
[103] Rachel Lehrman and Joseph Pisani, *Smart but Nosy: Latest Gadgets Want to Peer Into Our Lives*, AP News (Jan 11, 2019), https://www.apnews.com/8035020f41d24847b16276b5627195c5.
[104] Emiliano Falcon, *Amazon Doubles Down on Face Surveillance, Files Patent for Scary New Tech*, Privacy SOS (Dec. 5, 2018), https://privacysos.org/blog/amazon-doubles-face-surveillance-files-patent-scary-new-tech/.
[105] Peter Holly, " This patent shows Amazon may seek to create a 'database of suspicious persons' using facial-recognition technology," Washington Post, December 18, 2018.
[106] Ibid.
[107] Consumer Watchdog, *Google and Amazon Really DO Want to Spy on You: Patent Reveals Future Versions of Their Voice Assistants Will Record Your Conversations to Sell You Products*, https://www.consumerwatchdog.org/privacy-technology/google-and-amazon-really-do-want-spy-you-patent-reveals-future-versions-their.

Company adds Fourth Amendment privacy intrusion concerns[108] to the mix of a work culture already criticized for pressuring employees to work long hours and perform above all else.[109]

The Company's attempt this past June to sell Rekognition to Immigration and Customs Enforcement (ICE) officials as a means for targeting or identifying immigrants in homeland security investigations[110] fueled a backlash[111] among Amazon employees, who wrote an open letter to the Company in protest, demanding the Company reject contracts that could be used for government surveillance[112]. They expressed their fear that the powerful surveillance capabilities of Rekognition would harm the most marginalized, and further stated that they refuse to contribute to tools that violate human rights by building platforms that power ICE[113]. More than 450 anonymous employees are now reported to have signed the letter[114]. Drew Harwell of the Washington Post described how the June meeting has more broadly fueled a Silicon Valley "culture clash" between executives in pursuit of government contracts and outraged rank-and-file workers[115].

Spillover impact: the Company's public license to operate in New York City.

A part of the cost of a degraded reputation is whether and where the company has a public license to operate. The New York City deal for a major new HQ2 facility recently fell through. While there were a variety of issues raised by the community, and Rekognition was not the main issue raised, it was raised by a number of key community leaders, and could well have further

---

[108] Dariush Adli, *Do Amazon's Movement-Tracking Wristbands Violate Workers' Privacy Rights?*, Entrepreneur (June 14, 2018), https://www.entrepreneur.com/article/314696.
[109] Mathew Ingram, *Amazon: Dystopian nightmare, or just another successful*, Fortune (Aug. 17, 2015), http://fortune.com/2015/08/17/amazon-dystopian-nightmare-or-just-another-successful-tech-company/.
[110] Drew Harwell, *Amazon Met with ICE Officials Over Facial-Recognition System That Could Identify Immigrants*, The Washington Post (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/?noredirect=on&utm_term=.a1f6a0bde678.
[111] Andrea Peterson and Jake Laperruque, *Amazon Pushes ICE to Buy Its Face Recognition Surveillance Tech*, POGO (Oct. 24, 2018), https://www.pogo.org/investigation/2018/10/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech/.
[112] Drew Harwell, *Amazon Met with ICE Officials Over Facial-Recognition System That Could Identify Immigrants*, The Washington Post (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/?noredirect=on&utm_term=.a1f6a0bde678.
[113] Hamza Shaban, *Amazon Employees Demand Company Cut Ties With ICE*, The Seattle Times (June 22, 2018), https://www.seattletimes.com/business/amazon-employees-demand-company-cut-ties-with-ice/.
[114] Andrea Peterson and Jake Laperruque, *Amazon Pushes ICE to Buy Its Face Recognition Surveillance Tech*, POGO (Oct. 24, 2018), https://www.pogo.org/investigation/2018/10/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech/. Sen. Ron Wyden (D-Ore.) also issued as statement regarding the meeting between ICE officials and the Company, in which he discussed the potential for dangerous misuse by the government without clear protections in place. Drew Harwell, *Amazon Met with ICE Officials Over Facial-Recognition System That Could Identify Immigrants*, The Washington Post (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/?noredirect=on&utm_term=.a1f6a0bde678.
[115] Drew Harwell, *Amazon Met with ICE Officials Over Facial-Recognition System That Could Identify Immigrants*, The Washington Post (Oct. 23, 2018), https://www.washingtonpost.com/technology/2018/10/23/amazon-met-with-ice-officials-over-facial-recognition-system-that-could-identify-immigrants/?noredirect=on&utm_term=.a1f6a0bde678.

undermined the community's willingness to trust the company.

A variety of issues were raised in the course of hearings held by the New York City Council in December 2018, including the Company's potential support of surveillance by the government. Brian Huseman, Amazon's vice president for public policy, testified. According to a media report:[116]

> Corey Johnson, the city council speaker, asked specifically about Amazon's dealings with US Immigration and Customs Enforcement.
>
> "We believe the government should have the best available technology," said Brian Huseman, Amazon's vice president of public policy.
>
> Huseman's answer was met with a chorus of boo's from protestors, who filled the council meeting and often interrupted proceedings with chants and feedback....
>
> ...Huseman was also pressed Wednesday about an experiment from the American Civil Liberties Union that found that Amazon's Rekognition software incorrectly ID'd members of Congress as people who had been arrested in the past.
>
> "We have not been able to replicate the findings of that," Huseman said.
>
> "...I think that will come as cold comfort to people who are picked up as a result of your facial recognition," NYC council member Brad Lander responded.

In addition, other local community leaders picked up this issue on Twitter. For instance, after Amazon announced that it was pulling out of the deal, U.S. Rep. Alexandria Ocasio-Cortez suggested in a tweet that it was hard to understand how "a technology giant of big-brother-esque potential was selling (notoriously flawed & racially biased) facial recognition technology to ICE while trying to move into 1 of the most immigrant-dense areas of the world." [117]

The way that concern about the surveillance issues, including potential sale of Rekognition to the government, proved to be an *underlying* vulnerability of the Company is highlighted in the discussion surrounding the Company's interest in New York City. *New York Times* reporter J. David Goodman on Twitter described the Company's decision to pull out of the deal: "One factor that concerned Amazon executives was how activists in New York City broadened their attacks from the specifics of the deal to the company's practices far beyond the five boroughs, on unions and working with ICE, per two people familiar with Amazon's decision."[118]

---

[116] https://www.businessinsider.com/amazon-ice-government-provides-facial-recognition-tech-2018-12.
[117] https://twitter.com/AOC/status/1098000445912559619.
[118] https://twitter.com/jdavidgoodman/status/1096144088234119169.

III. Rule 14a-8(i)(11)

The Company Letter further asserts that if the Rule 14a-8(i)(7) and Rule 14a-8(i)(5) objections are found inapplicable, that the Disclosure Proposal may be excluded under Rule 14a-8(i)(11) because it substantially duplicates the Prohibition Proposal. In this instance, the Proponents believe that there would be significant value to investors in voting on both Proposals.

The principal thrust of the Prohibition Proposal is for a shareholder vote on whether they believe the company should halt sales to the government. The principal thrust of the Disclosure Proposal is for disclosure and the commissioning of an independent study. Though the discussions in the background sections overlap to some degree, the actions requested are significantly different.

Longstanding staff precedent holds that proposals addressing a broad overarching topic (e.g., climate change) are not necessarily duplicative so long as they have a distinct "principal thrust." This holds even when the subject matter has some overlap in two proposals, as *in ExxonMobil Corp.* (March 17, 2014) where a proposal seeking a report on carbon asset risk was not substantially duplicative of a proposal seeking GHG reduction goals despite the fact both proposals dealt broadly with climate change. Similarly, in *Pharma-Bio Serv, Inc.* (January 17, 2014) two proposals related to the issuance of dividends were allowed by the Staff to appear on the proxy even though the subject matter of dividends underlay both proposals. Proposals that relate to aspects of board elections are also not considered duplicative under the rule. For instance, in *Baxter Inc.* (January 31, 2012), one proposal calling for a simple majority vote, and another calling for directors to be elected on an annual basis were not found duplicative for purposes of Rule 14a-8(i)(11). *See also AT&T Inc.* (February 3, 2012) (indicating that a proposal seeking a report on lobbying contributions and expenditures is distinct from a proposal seeking a report on political disclosure, whereas AT&T argued they were both "political").

Notably, Staff denied relief in several cases where there were two proposals on one subject matter, and where one proposal dealt with halting an activity, while the second related to a company's assessment or related disclosures. This framework exactly parallels the Proposal here.

For example, in *Bank of America Corp.* (January 7, 2013) a proposal seeking to explore an end to political spending on elections and referenda was found distinct from a proposal asking the company to disclose its political spending in a variety of categories, where both related to political spending. Similarly, in *Chevron Corp.* (March 24, 2009), Staff denied relief under the (i)(11) exclusion when the company was confronted with competing proposals. One sought "information on the policies and procedures that guide Chevron's assessment of host countries laws and regulations with respect to their adequacy to protect human health, the environment and our company's reputation," and the other proposal a report on "Chevron's criteria for (i) investment in; (ii) continued operations in; and, (iii) withdrawal from specific countries." Despite Chevron's argument that both proposals dealt with decisions about foreign investment, the Division determined that the two proposals were sufficiently different to make the (i)(11) exclusion inapplicable.

The Proponents believe that the process of corporate democracy would be best served, and the shareholders, board and management would receive more information, by allowing both Proposals to proceed to a vote. The clear distinction between these two approaches would be apparent to the shareholders and would not be confusing.

APPENDIX A

The “Prohibition Proposal”
of the Tri-State Coalition for Responsible Investment and others
(First-submitted Proposal)

Risks of Sales of Facial Recognition Software
Amazon.com, Inc. - 2019

Whereas, shareholders are concerned Amazon's facial recognition technology ("Rekognition") poses risk to civil and human rights and shareholder value.

Civil liberties organizations, academics, and shareholders have demanded Amazon halt sales of Rekognition to government, concerned that our Company is enabling a surveillance system "readily available to violate rights and target communities of color." Four hundred fifty Amazon employees echoed this demand, posing a talent and retention risk.

Brian Brackeen, former Chief Executive Officer of facial recognition company Kairos, said, "Any company in this space that willingly hands [facial recognition] software over to a government, be it America or another nation's, is willfully endangering people's lives."

In Florida and Oregon, police have piloted Rekognition.

Amazon Web Services already provides cloud computing services to Immigration and Customs Enforcement (ICE) and is reportedly marketing Rekognition to ICE, despite concerns Rekognition could facilitate immigrant surveillance and racial profiling.

Rekognition contradicts Amazon's opposition to facilitating surveillance. In 2016, Amazon supported a lawsuit against government "gag orders," stating: "the fear of secret surveillance could limit the adoption and use of cloud services ... Users should not be put to a choice between reaping the benefits of technological innovation and maintaining the privacy rights guaranteed by the Constitution."

Shareholders have little evidence our Company is effectively restricting the use of Rekognition to protect privacy and civil rights. In July 2018, a reporter asked Amazon executive Teresa Carlson whether Amazon has "drawn any red lines, any standards, guidelines, on what you will and you will not do in terms of defense work." Carlson responded: "We have not drawn any lines there...We are unwaveringly in support of our law enforcement, defense, and intelligence community."

In July 2018, lawmakers asked the Government Accountability Office to study whether "commercial entities selling facial recognition adequately audit use of their technology to ensure that use is not unlawful, inconsistent with terms of service, or otherwise raise privacy, civil rights, and civil liberties concerns."

Microsoft has called for government regulation of facial recognition technology, saying, "if we move too fast, we may find that people's fundamental rights are being broken."

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.

The “Disclosure Proposal”
of John C. Harrington

(Second Submitted Proposal)

Whereas, our Company, through Amazon Web Services (AWS), developed and is marketing to government and law enforcement agencies, a facial recognition system (Rekognition), that we believe may pose significant financial risks due to its privacy and human rights implications;

Whereas, human and civil rights organizations are concerned that facial surveillance technology may ultimately violate civil rights by unfairly and disproportionally targeting and surveilling people of color, immigrants and civil society organizations;

Whereas, hundreds of Amazon's employees have petitioned our Company Chief Executive Officer to stop providing Rekognition to government agencies, a practice detrimental to internal cohesion, morale, and which undermines Amazon employees' commitment to its retail customers by placing those customers at risk of warrantless, discriminatory surveillance;

Whereas, in the past our Company has publicly opposed secret government surveillance and our Chief Executive Officer has personally expressed his support for First Amendment freedoms and openly opposed the discriminatory Muslim Ban;

Whereas, the marketing of this technology could also be expanded to foreign authoritarian regimes, resulting in our Company's surveillance technologies being used to identify and detain democracy advocates;

Whereas, over seventy civil and human rights groups, joined by academics, employees, and other stakeholders have called upon our Company's Chief Executive Officer to stop selling Rekognition enabling a "government surveillance infrastructure,";

Whereas, the American Civil Liberties Union (ACLU) found that Amazon's Rekognition falsely matched 28 members of Congress with people who have been arrested for a crime, in a test that relied on the software's default settings;

Whereas, there is little evidence to suggest that our Board of Directors, as part of its fiduciary oversight, has rigorously assessed the magnitude of risks to our Company's financial performance associated with the privacy and human rights threat to customers and other stake holders;

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

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

The report should be produced at reasonable expense, exclude proprietary or legally privileged information, and be published no later than September 1, 2019.

Supporting Statement

We believe the Board of Directors' fiduciary duty of care extends to thoroughly evaluating the impacts on reputation and shareholder value, of any surveillance technology our Company produces or markets on which significant concerns are raised regarding the danger to civil and privacy rights of customers and other stakeholders. The recent failures of Facebook to engage in sufficient content and privacy management, and the resulting economic impacts to that company should be taken as sufficient warning: it could happen to Amazon.

GIBSON DUNN

Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

Ronald O. Mueller
Direct: +1 202.955.8671
Fax: +1 202.530.9631
RMueller@gibsondunn.com

March 29, 2019

VIA E-MAIL

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: *Amazon.com, Inc.*
Reconsideration Request/Commission Appeal
Shareholder Proposals of John C. Harrington and the Sisters of St. Joseph of Brentwood et al.
Securities Exchange Act of 1934—Rule 14a-8

Ladies and Gentlemen:

On behalf of our client, Amazon.com, Inc. (the "Company"), we respectfully request review and reconsideration by the staff of the Division of Corporation Finance (the "Staff") and the Securities and Exchange Commission (the "Commission") of the Staff's March 28, 2019 response (the "Staff Response Letter") to our no-action request dated January 22, 2019 (the "Request Letter") regarding two proposals (the "Proposals") addressing use of the Company's facial recognition technology by U.S. government and law enforcement agencies. We are requesting review for the following reasons:

> The Proposals seek to utilize the shareholder proposal process to interject the Company and its shareholders into the public policy debate regarding law enforcement's appropriate use of facial recognition technology. The Company requests reconsideration or Commission review of the Staff's response because it believes that the Proposals address a topic more appropriately left to Congress and others charged with establishing applicable legal standards, and because it believes that the Staff misapplied the applicable standards under Rules 14a-8(i)(5) and (i)(7).

As described by the Staff, the first of the Proposals (the "First Proposal," attached hereto as Exhibit A)[1] requests that the board prohibit sales of facial recognition technology to government agencies unless the board concludes, after an evaluation using independent

[1] The First Proposal was submitted by the Sisters of St. Joseph of Brentwood, The Sisters of St. Francis of Philadelphia, the Sisters of St. Francis Charitable Trust, Azzad Asset Management, and the Maryknoll Sisters of St. Dominic, Inc.

evidence, that the technology does not cause or contribute to actual or potential violations of civil and human rights. The second of the Proposals (the "Second Proposal," attached hereto as Exhibit B)[2] requests that the board commission an independent study of Rekognition, the Company's image and video analysis service that allows customers to help identify objects, people, text, scenes, and activities, and issue a report addressing, among other things, the extent to which such technology may endanger, threaten, or violate privacy and or civil rights, the extent to which such technologies may be marketed and sold to certain foreign governments, and the financial or operational risks associated with these issues.

In the Staff Response Letter, which is available at https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2019/johnharringtonetal032819-14a8.pdf, the Staff stated that it was unable to concur:

- that the Proposals could be excluded under rule 14a-8(i)(5) "because we are unable to conclude that the Proposals are not otherwise significantly related to the Company's business";
- that the Proposals could be excluded under rule 14a-8(i)(7) because, in the Staff's view, "the Proposals transcend ordinary business matters"; and
- that the Second Proposal could be excluded under rule 14a-8(i)(11) because, in the Staff's view, "the Second Proposal does not substantially duplicate the First Proposal."

Commission Review Is Warranted

The issues raised by the Proposals satisfy the standard for Commission review of Staff determinations under Rule 14a-8 as set forth in Paragraph 202.1(d) of Title 17 of the Code of Federal Regulations. Under that regulation, "the [S]taff . . . will generally present questions to the Commission which involve matters of substantial importance and where the issues are novel or highly complex."

As discussed below, review is warranted under this standard because:

- The principal focus of the Proposals – the appropriate framework to protect individual civil rights and ensure transparency in use of a specific technology by government and law enforcement – is more appropriately a topic for national legislative determination, rather than a matter to be addressed through the shareholder proposal process;
- The Staff's response misapplies the standard applicable under Rule 14a-8(i)(5) as set forth in Staff Legal Bulletin No. 14I (Nov. 1, 2017) ("SLB 14I"); and
- The Staff's response misapplies the standard under Rule 14a-8(i)(7) and is inconsistent with well-established precedent regarding the nexus requirement under Rule 14a-8(i)(7).

---

[2] The second proposal was submitted by John C. Harrington (together with the Sisters of St. Joseph of Brentwood, The Sisters of St. Francis of Philadelphia, the Sisters of St. Francis Charitable Trust, Azzad Asset Management, and the Maryknoll Sisters of St. Dominic, Inc., the "Proponents").

Analysis

Background Regarding Amazon Rekognition

The Request Letter contains an extensive discussion about what Amazon Rekognition is, how customers may use it, and the nature of the Company's role in offering the service. For purposes of this letter, the following points are most relevant:

- Amazon Rekognition is a service offered by Amazon Web Services ("AWS") that customers can access via the cloud, allowing customers to analyze the customers' images or videos to help identify objects, people, text, scenes, and activities, as well as to detect inappropriate content.[3] Amazon Rekognition is just one of more than 165 services offered by AWS.
- To use Amazon Rekognition, customers provide the images and videos that they wish to have analyzed, and Amazon Rekognition returns an output based on the customer's data, including a confidence score in the accuracy level of the output. Customers determine their own use for the output returned by Amazon Rekognition.
- Customers provide the images to be analyzed by Amazon Rekognition, including the database that images are to be matched against. Amazon does not record or generate the input that its customers use to run pictorial or video comparisons on Amazon Rekognition; customers decide whether to access the application, select the input used, and directly receive the output generated.
- Since AWS introduced Rekognition in 2016, there has not been a single documented case of the service being misused by law enforcement. Instead, Amazon Rekognition has been used to aid government and private groups in law enforcement, such as to prevent human trafficking, inhibit child exploitation, and reunite missing children with their families.
- The revenue, income, and assets related to Amazon Rekognition were less than 5% of AWS's 2018 revenue, net income, and assets, were a significantly lower percentage of the Company's revenue, net income, and assets, and are expected to remain insignificant for 2019.

The Proposals

The principal focus of the Proposals is whether law enforcement agencies may misuse Amazon Rekognition or its output in a way that violates individuals' civil rights. This focus is clear from the text of the Proposals, and from the Proposals' supporting statements. For example, the First Proposal requests that the Company not provide its facial recognition service to government agencies unless the Board conducts an independent evaluation and determines "that the technology does not cause or contribute to actual or potential violations

---

[3] *See* Amazon Rekognition, *available at* https://aws.amazon.com/rekognition/ (the "Rekognition Homepage").

of civil and human rights." It is clear from the explicit reference to government agencies and the Proposal's "cause or contribute to" language that the focus of this resolution is on how customers use the output generated by Amazon Rekognition. The supporting statements to the First Proposal make that point abundantly clear: each paragraph focuses on how government customers use Amazon Rekognition, and Amazon itself is addressed only in the context of whether it makes the service available to its government customers.

Similarly, the Second Proposal requests that the Board conduct an independent evaluation regarding how customers may use or misuse Amazon Rekognition, such as by "target[ing] or surveil[ling]" immigrants, activists, or others. Although worded in a manner that does not explicitly refer to the Company's law enforcement customers, the resolution and its supporting statement as a whole make clear that the reason for the Second Proposal is concern over whether customers will misuse Amazon Rekognition or the output it generates. The first paragraph of the supporting statements in the Second Proposal leaves no doubt about this focus, beginning with the statement, "Whereas, our Company . . . developed and is marketing to government and law enforcement agencies, a facial recognition system . . . ." As discussed above, because AWS only offers the Amazon Rekognition service for others to use, it is clear that the focus of concern of the Proposals is how customers might use the service.

The Company understands why people want there to be oversight and guidelines put in place to make sure facial recognition technology cannot be used to discriminate. In this regard, on February 7, 2019, after the Request Letter was submitted, the Company stated its view that the issues around how law enforcement uses facial recognition technology are appropriately addressed through a national legislative framework that protects individual civil rights and ensures that governments are transparent in their use of facial recognition technology.[4] The Company continues to believe that the issues raised by the Proposals should be addressed by legislative processes and in this context are not appropriate for the shareholder proposal process.

Rule 14a-8(i)(5)

As noted above, Amazon Rekognition accounts for significantly less than 5% of the Company's revenue, income, and assets. Accordingly, the Proposals are excludable unless they are "otherwise significantly related to the company." Prior to issuing SLB 14I, in assessing this standard, the Staff "simply considered whether a company conducted any amount of business related to the issue in the proposal and whether that issue was of broad social or ethical concern." Under SLB 14I, however, proposals that raise issues of social or ethical significance may be excluded notwithstanding their significance in the abstract,

---

[4] *See* Some Thoughts on Facial Recognition Legislation, *available at* https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

unless it is clear that the issue is significant to the Company's business. SLB 14I states that a proponent can "continue to raise social or ethical issues in its arguments, but it would need to tie those to a significant effect on the Company's business."

Here, the Proponents have failed to demonstrate any significant effect of the concerns underlying these Proposals on the Company's business.[5] The supporting statements to the Proposals are full of conjecture over what "could" happen, but they fail to point to a single quantifiable or demonstrable impact on the Company's business.[6] In this regard, SLB 14I states, "The mere possibility of reputational or economic harm will not preclude no-action relief." The Proponents have not demonstrated any actual impact on the Company resulting from their speculative concerns, and accordingly, the Proposals are properly excludable under Rule 14a-8(i)(5).

In this regard, we respectfully believe that the Staff applied the wrong standard under Rule 14a-8(i)(5). The Staff's response states that they do not concur in exclusion "because we are unable to conclude that the Proposals are not otherwise significantly related to the Company's business." That standard is equivalent to "simply consider[ing] whether a company conducted any amount of business related to the issue in the proposal and whether that issue was of broad social or ethical concern." Under SLB 14I, a proposal that does not satisfy the economic thresholds is excludable unless the Staff affirmatively determines that the proposal is "otherwise significantly related to the Company's business." The Staff did not make that determination with respect to the Proposals, and we do not believe that there is a basis for doing so. Accordingly, the Proposals are properly excludable under Rule 14a-8(i)(5).

Rule 14a-8(i)(7)

Exchange Act Release No. 40018 (May 21, 1998) states that proposals involving "significant social policy issues" are not excludable under Rule 14a-8(i)(7) because they "transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote." Id. (citing Exchange Act Release No. 12999 (Nov. 22, 1976)). Note 4 of Staff Legal Bulletin 14E (Oct. 27, 2009) states that "[i]n those cases in which a

---

[5] The fact that the Company is participating in the legislative policy debate regarding regulation of facial recognition technology does not distinguish this issue from dozens of other issues that bear on the Company's business.

[6] Similarly, a letter dated February 28, 2019, submitted on behalf of the Proponents ("Proponents' Response Letter"), fails to identify any significant impact or relevance: it has no support for (and is inaccurate in) its assertion that Amazon Rekognition is significant to AWS as Amazon Rekognition is only one of over 165 services offered by AWS and is far from being one of the most utilized services; additionally, its assertions regarding privacy and consumer rights issues relating to other companies and to an entirely different Company product (Alexa) have no relation to the Company's facial recognition service.

proposal's underlying subject matter transcends the day-to-day business matters of the company and raises policy issues so significant that it would be appropriate for a shareholder vote, the proposal generally will not be excludable under Rule 14a-8(i)(7) as long as a sufficient nexus exists between the nature of the proposal and the company" (emphasis added). The Staff reaffirmed this position in Note 32 of Staff Legal Bulletin 14H (Oct. 22, 2015), explaining "[w]hether the significant policy exception applies depends, in part, on the connection between the significant policy issue and the company's business operations."[7]

As discussed above, the focus of the Proposals is on whether certain of Amazon's customers might misuse the output generated by Amazon Rekognition. AWS's law enforcement customers are only one small segment of the customer base that uses Amazon Rekognition.[8] The Request Letter does not dispute whether the Proposals touch upon a significant social policy issue. Instead, the Request Letter cites well established precedent that when the focus of a proposal is on potential customer misuse of a company's product, in a manner where such misuse can implicate a significant policy issue, there is not a sufficient nexus to avoid exclusion under Rule 14a-8(i)(7).[9] We respectfully believe that there is no basis for a determination that the potential misuse of a product by a customer establishes a sufficient nexus such as to transcend ordinary business matters. Here, where the focus of a proposal is on the potential actions of customers (and we reiterate that the Proponents are only addressing conjecture and that the Company is not aware of a single report of misuse of Amazon Rekognition by law enforcement), the Staff's determination is a radical departure from the precedent cited in the Request Letter and is not consistent with any precedent of which we are aware. Accordingly, we continue to believe that the Proposals are appropriately excludable under Rule 14a-8(i)(7).

---

[7] In this regard, when assessing proposals under Rule 14a-8(i)(7), the Staff considers the terms of the resolution and its supporting statement as a whole. See Staff Legal Bulletin No. 14C, part D.2 (June 28, 2005) ("In determining whether the focus of these proposals is a significant social policy issue, we consider both the proposal and the supporting statement as a whole.").

[8] As noted in the Initial Request, Amazon Rekognition has been applied extensively for various commercial uses, such as to identify public figures who are speaking at large events or live on-air, search through large volumes of media assets, authenticate attendees at live events to shorten lines, build educational apps for children, power social media apps, enhance security through multi-factor authentication, prevent package theft, and identify for removal third-party-generated website content for suggestive or explicit content, among numerous other examples.

[9] See in particular, *FMC Corp.* (avail. Feb. 25, 2011, *recon. denied* Mar. 16, 2011), as well as *Danaher Corp.* (avail. Mar. 8, 2013, *recon. denied.* Mar. 20, 2013) and *Amazon.com, Inc.* (avail. Mar. 17, 2016). The Proponents' Response Letter does not cite a single precedent to support its claims that public debate, Congressional inquiry, or other matters support "nexus." Moreover, much of the public debate cited in the Proponents' Response Letter is addressed to the users of facial recognition technology, or to companies engaged in surveillance or similar activities, and thus are not relevant to the Company.

Conclusion

Based on the foregoing analysis, the Company believes that review and reconsideration by the Commission of the Proposals and the Staff Response Letter is warranted.[10]

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to shareholderproposals@gibsondunn.com. If we can be of any further assistance in this matter, please do not hesitate to call me at (202) 955-8671, or Mark Hoffman, the Company's Vice President & Associate General Counsel and Assistant Secretary, at (206) 266-2132.

Sincerely,

Ronald O. Mueller

Enclosures

cc: Jay Clayton, Chairman
Robert J. Jackson, Jr., Commissioner
Hester M. Peirce, Commissioner
Elad L. Roisman, Commissioner
William Hinman, Director, Division of Corporation Finance
Mark Hoffman, Amazon.com, Inc.
John C. Harrington
Mary Beth Gallagher, Tri-State Coalition for Responsible Investment

1032354181.1

[10] We also continue to believe that because both Proposals request a report on how Amazon Rekognition might be misused by government and law enforcement customers, the Second Proposal is excludable under Rule 14a-8(i)(11) as addressing substantially the same subject as the First Proposal.

EXHIBIT A

Risks of Sales of Facial Recognition Software
Amazon.com, Inc. - 2019

Whereas, shareholders are concerned Amazon's facial recognition technology ("Rekognition") poses risk to civil and human rights and shareholder value.

Civil liberties organizations, academics, and shareholders have demanded Amazon halt sales of Rekognition to government, concerned that our Company is enabling a surveillance system "readily available to violate rights and target communities of color." Four hundred fifty Amazon employees echoed this demand, posing a talent and retention risk.

Brian Brackeen, former Chief Executive Officer of facial recognition company Kairos, said, "Any company in this space that willingly hands [facial recognition] software over to a government, be it America or another nation's, is willfully endangering people's lives."

In Florida and Oregon, police have piloted Rekognition.

Amazon Web Services already provides cloud computing services to Immigration and Customs Enforcement (ICE) and is reportedly marketing Rekognition to ICE, despite concerns Rekognition could facilitate immigrant surveillance and racial profiling.

Rekognition contradicts Amazon's opposition to facilitating surveillance. In 2016, Amazon supported a lawsuit against government "gag orders," stating: "the fear of secret surveillance could limit the adoption and use of cloud services ... Users should not be put to a choice between reaping the benefits of technological innovation and maintaining the privacy rights guaranteed by the Constitution."

Shareholders have little evidence our Company is effectively restricting the use of Rekognition to protect privacy and civil rights. In July 2018, a reporter asked Amazon executive Teresa Carlson whether Amazon has "drawn any red lines, any standards, guidelines, on what you will and you will not do in terms of defense work." Carlson responded: "We have not drawn any lines there...We are unwaveringly in support of our law enforcement, defense, and intelligence community."

In July 2018, lawmakers asked the Government Accountability Office to study whether "commercial entities selling facial recognition adequately audit use of their technology to ensure that use is not unlawful, inconsistent with terms of service, or otherwise raise privacy, civil rights, and civil liberties concerns."

Microsoft has called for government regulation of facial recognition technology, saying, "if we move too fast, we may find that people's fundamental rights are being broken."

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.*

EXHIBIT B

Whereas, our Company, through Amazon Web Services (AWS), developed and is marketing to government and law enforcement agencies, a facial recognition system (Rekognition), that we believe may pose significant financial risks due to its privacy and human rights implications;

Whereas, human and civil rights organizations are concerned that facial surveillance technology may ultimately violate civil rights by unfairly and disproportionally targeting and surveilling people of color, immigrants and civil society organizations;

Whereas, hundreds of Amazon's employees have petitioned our Company Chief Executive Officer to stop providing Rekognition to government agencies, a practice detrimental to internal cohesion, morale, and which undermines Amazon employees' commitment to its retail customers by placing those customers at risk of warrantless, discriminatory surveillance;

Whereas, in the past our Company has publicly opposed secret government surveillance and our Chief Executive Officer has personally expressed his support for First Amendment freedoms and openly opposed the discriminatory Muslim Ban;

Whereas, the marketing of this technology could also be expanded to foreign authoritarian regimes, resulting in our Company's surveillance technologies being used to identify and detain democracy advocates;

Whereas, over seventy civil and human rights groups, joined by academics, employees, and other stakeholders have called upon our Company's Chief Executive Officer to stop selling Rekognition enabling a "government surveillance infrastructure,";

Whereas, the American Civil Liberties Union (ACLU) found that Amazon's Rekognition falsely matched 28 members of Congress with people who have been arrested for a crime, in a test that relied on the software's default settings;

Whereas, there is little evidence to suggest that our Board of Directors, as part of its fiduciary oversight, has rigorously assessed the magnitude of risks to our Company's financial performance associated with the privacy and human rights threat to customers and other stake holders;

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

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

The report should be produced at reasonable expense, exclude proprietary or legally privileged information, and be published no later than September 1, 2019.

Supporting Statement

We believe the Board of Directors' fiduciary duty of care extends to thoroughly evaluating the impacts on reputation and shareholder value, of ***any*** surveillance technology our Company produces or markets on which significant concerns are raised regarding the danger to civil and privacy rights of customers and other stakeholders. The recent failures of Facebook to engage in sufficient content and privacy management, and the resulting economic impacts to that company should be taken as sufficient warning: **it could happen to Amazon.**