MITCHELL | HAMLINE School of Law

Mitchell Hamline Law Journal of Public Policy and Practice

Volume 42 | Issue 1 Article 4

2021

The Price of Prime—Consumer Privacy in the Age of Amazon

Ariana Aboulafia

Greg Fritzius

Tessa Mears

Macy Nix

THE PRICE OF PRIME—CONSUMER PRIVACY IN THE AGE OF AMAZON

Ariana Aboulafia, Greg Fritzius, Tessa Mears & Macy Nix

TABLE OF CONTENTS

I. INTRODUCTION

It is difficult to imagine a world without Amazon. The behemoth tech corporation—which began as a humble attempt by entrepreneur Jeffery Bezos to sell books on the Internet[1]—had a market cap of $1.6 trillion as of November 2020, and its net income rose almost 200% for the third quarter of 2020, compared to the same three-month period in 2019.[2] And, far from its bookstore origins, Amazon currently sells nearly anything that one could ask for via its online website, which hosts around 300 million active accounts as of 2017.[3] Amazon Prime, which offers users free two-day shipping (among other perks) for a fee has over 150 million subscribers worldwide as of 2019.[4] And, as if that weren't enough, Amazon owns dozens of subsidiaries that span across several industries.[5] Amazon also produces consumer electronics including Kindle e-readers, Fire tablets, Fire TV sticks, and Amazon Echo devices (which are enabled with Alexa, a personal virtual assistant).

Taking all of this into account, it is clear that from the food that one eats, to the films that one watches, the books that one reads, to the incidentals that one purchases, Amazon touches—or, at the very least, has the potential to touch—nearly every aspect of a consumer's life. As such, assuming one cares about consumer privacy, Amazon's privacy policies (which apply to users of

[1] Makeda Easter & Paresh Dave, *Remember When Amazon Only Sold Books?*, L.A.TIMES (June 18, 2017), https://www.latimes.com/business/la-fi-amazon-history-20170618-htmlstory.html.
[2] Nathan Reiff, *How Amazon Makes Money*, INVESTOPEDIA (Nov 6, 2020), https://www.investopedia.com/how-amazon-makes-money-4587523.
[3] Erik Mathes, *10 Amazon Statistics That Will Shock Every Seller*, SELLERLABS (Aug. 12, 2019), https://www.sellerlabs.com/blog/10-amazon-statistics-will-shock-every-seller/.
[4] *Id.*
[5] Some of Amazon's most well-known subsidiaries include Amazon Prime Video (an instant media streaming service), Amazon Music (which streams music), Audible (an audiobook service), Amazon Publishing (which publishes books in both the print and e-book format on their website), Amazon Studios (a film production company), Twitch (a video game streaming service), Whole Foods Market (a brick and mortar grocery store), Zappos (an online shoe retailer) and Amazon Web Services (a comprehensive cloud computing platform). For a more expansive list of Amazon's subsidiaries, *see* Leticia Miranda, *These Are All the Businesses You Never Knew Were Owned by Amazon*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/leticiamiranda/these-are-all-the-businesses-you-never-knew-were-owned-by (last updated July 11, 2019).

all of Amazon's subsidiaries as well) become relevant. And, while many provisions of Amazon's privacy policies are worrisome, it may be particularly concerning both for Amazon consumers and for anyone else who cares about consumer privacy that Amazon does *not* notify users about government data requests, or promise not to "sell out" users (to governments or law enforcement, for surveillance purposes).[6] On the contrary, in fact, Amazon's privacy policies state that "[w]e release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon, our users, or others."[7] Indeed, it was these factors (along with others) that caused an international digital rights group, the Electronic Frontier Foundation, to award Amazon a paltry two out of five stars in their 2017 rating of tech companies' commitment to protecting consumer privacy.[8] In comparison, that same year other tech giants—including Adobe, Dropbox, Lyft, Pinterest, Uber, and WordPress—received five out of five stars.[9]

Clearly, Amazon could stand to improve its polices on consumer privacy. However, there are three Amazon products, partnerships and services—Alexa, Ring, and Rekognition—that are particularly concerning from the standpoint of not only protecting the privacy of consumers, but also of those who choose not to use these products and yet have their privacy rights implicated regardless. Part II of this paper will discuss these services and why their privacy implications are especially alarming. It will then propose and discuss four solutions in Part III: a new statute called the PRIME Act, a social solution consisting of increased shareholder pressure, a technological solution comprised of terms of use questionnaires, and an antitrust solution. These solutions can

[6] Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, ELEC. FRONTIER FOUND. (July 10, 2017), https://www.eff.org/who-has-your-back-2017.
[7] *Amazon Privacy Policy*, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Jan. 1, 2020).
[8] *See* Reitman, *supra* note 6.
[9] *Id.*

mitigate some of the more detrimental impacts of Amazon's consumer privacy policies as they currently stand. The final section will outline potential responses and objections to these proposed solutions and reforms, and will conclude by arguing that it is possible to allow Amazon to continue its economic growth and technological innovation while still regulating its practices, particularly those that affect consumer privacy.

II. THE TROUBLESOME TRIFECTA

A. Amazon Alexa

As previously mentioned, Amazon Alexa is a digital voice assistant software created by Amazon that responds to users' voice commands.[10] While Alexa is not a standalone product, the Alexa software was first introduced in November 2014 as a feature embedded in Amazon Echo devices, a portable smart speaker meant for homes,[11] which was advertised as a family-friendly product designed to help with tasks such as creating to-do lists, setting alarms, answering questions and providing real-time information such as the news or the current weather.[12] Between its release in November 2014 and January 2019—less than five years—over 100 million Alexa-enabled devices have been sold by Amazon.[13]

However, Alexa's emergence in the marketplace has not been without controversy, most of which stem from two issues. First, there have been several incidents of Alexa listening to conversations without consumers' knowledge or without their full consent. For example, while

[10] Michael Bizzaco et al., *What Is Alexa? Where Does She Come from? How Does She Work?*, DIGIT. TRENDS (Nov. 25, 2020), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/.
[11] Laura Lorenzetti, *Forget Siri, Amazon Now Brings You Alexa*, FORTUNE (Nov. 6, 2014), https://fortune.com/2014/11/06/forget-siri-amazon-now-brings-you-alexa/.
[12] *See* Top Tech, *Introduction of Amazon Echo*, YOUTUBE (Sept. 20, 2015), https://www.youtube.com/watch?v=6V5I8HHFTNQ.
[13] Dieter Bohn, *Amazon Says 100 Million Alexa Devices Have Been Sold—What's Next?*, VERGE (Jan. 4, 2019, 4:00 PM), https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp.

Alexa is only supposed to record when a consumer uses a programmed "wake word" and asks it to do so, consumers have reported that Alexa has sent recordings of their private conversations without the users being aware that they had given Alexa any instructions to do so.[14] Alexa has also been awakened by sounds of sex—which it mistakes for signs of distress—and recorded (and stored) that audio.[15] And, to make matters worse, Amazon has recently considered doing away with the "wake word" entirely, which would allow Alexa to listen in on conversations indiscriminately.[16] Regarding consent, various organizations have accused Amazon of violating the Children's Online Privacy Protection Act because Alexa records minors under the age of 13 without their consent.[17] Amazon appears unfazed by these claims, as it currently sells Alexa products designed and marketed specifically for children.[18]

The second area of controversy surrounding Alexa and Alexa-enabled devices concerns questions as to how the data collected by Alexa is ultimately used. For example, a team consisting of over a thousand Amazon employees manually reads transcripts of Alexa recordings and/or listens to its audio.[19] This, of course, means that anything that is recorded by Alexa—even if

[14] Leia Klingel, *Amazon Devices Recording, Sending Your Conversations?*, FOX BUS. (May 25, 2018), https://www.foxbusiness.com/markets/amazon-devices-recording-sending-your-conversations. It is worth noting that Amazon claims that this incident was caused by the users unintentionally "waking" Alexa and prompting it to record conversations, yet the users maintain that they never heard Alexa audibly respond to any of its supposed triggers prior to it recording and sending the message in question.
[15] Nick Parker, *Alexa, Stop Being a Perv*, SUN, https://www.thesun.co.uk/tech/9611689/outrage-as-amazons-alexa-listens-to-brits-having-sex-rowing-swearing-and-sharing-medical-news/ (last updated Aug. 2, 2019).
[16] A.J. Dellinger, *Amazon Considered Letting Alexa Listen to You Without a Wake Word*, ENGADGET (May 23, 2019), https://www.engadget.com/2019/05/23/amazon-alexa-recording-before-wake-word-patent/.
[17] Mark Harris, *Virtual Assistants Such as Amazon's Echo Break US Child Privacy Law, Experts Say*, GUARDIAN (May 26, 2016, 7:00 AM), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.
[18] *See* Press Release, Amazon, Amazon Announces New Kindle Kids Edition, Fire HD 10 Kids Edition, and FreeTime on Fire TV, Providing Access to Kid-Friendly Content—Now in Even More Places (Oct. 7, 2019, 9:04 AM), https://press.aboutamazon.com/news-releases/news-release-details/amazon-announces-new-kindle-kids-edition-fire-hd-10-kids-edition.
[19] Matt Day et al., *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019, 5:34 PM), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

accidentally recorded—can and will potentially be examined by a real person, who can then forward those conversations to authorities if deemed necessary as per Amazon's aforementioned privacy policies. Indeed, as to this latter point, recordings from Alexa have been used by police in at least one criminal investigation at the time of writing, and privacy advocates believe that this may become more commonplace as time goes on, and Alexa-enabled devices become more popular.[20]

These controversies—and the several legal issues which are implicated by these controversies—have not escaped attention from both legal scholars[21] and lawmakers.[22] These advocates seem to be particularly worried by the Fourth Amendment implications of the utilization of Alexa recordings in criminal investigations, considering it may be used as precedent to diminish the reasonable expectation of privacy within the home, a long-held tenet of the Fourth Amendment jurisprudence.[23] This issue also implicates our understanding of the third-party search doctrine, and whether or not it is a constitutional issue for Amazon to share user data for use in criminal investigations when one considers that users allow their data to be shared with Amazon (a third-party) in the first place, and in doing so perhaps lose their right to protest the further sharing of that data to law enforcement.[24] Given these questions and the implications of their answers, not only for those who purposely purchase, install and utilize Alexa-enabled devices in their own homes but also for potential visitors, advocates have also argued that there may be a duty for the

[20] Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, ABA (July 20, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman/.
[21] *Id.*
[22] *See* Letter from Christopher A. Coons, U.S. Sen., to Jeff Bezos, Chief Exec. Officer, Amazon, Inc. (May 23, 2019). In this letter, Coons requested information on the types of data Amazon collects, stores, and preserves from Alexa, as well as the degree to which consumers control their personal information.
[23] *See* Boughman, *supra* note 20.
[24] *Id.*

owners of Alexa-enabled devices to warn guests within their home that those devices are present, and that they may be recorded at any time.[25] Amazon's plans to roll out a new line of Alexa-enabled devices meant to exist outside of the home (including headphones, rings, and other "wearable tech" devices)[26] will only compound this particular problem, since these devices will likely record non-consenting and unknowing members of the public in proximity to such devices.

In short, the privacy implications of Alexa are vast, and the protections of our current laws appear inadequate to assure individuals that their privacy rights will not be easily exploited. And there is little solace that the solutions will come from Amazon itself. Despite Amazon's claims that it takes user privacy seriously, some tech advocates describe these proclamations as inherently disingenuous when compared to Amazon's current practices and future plans.[27] Ideally, the systematic and widespread application of the solutions advocated for within this paper will curb the invasive practices of Amazon pertaining to not only Alexa-enabled devices, but all of Amazon's technologies, including Amazon Rekognition and Ring.

B. Amazon Rekognition

Like Amazon Alexa, Rekognition is not a standalone device; rather, it is an Application Programming Interface (API) that supposedly provides "highly accurate facial analysis and facial search capabilities" and can be integrated into any other web, mobile, or connected device

[25] *See* Susie Coen, *Alexa, Warn Our Guests that You're Eavesdropping on Them: Google Chief Says People Should Warn Visitors of Smart Speakers in Their Homes*, DAILY MAIL, https://www.dailymail.co.uk/news/article-7577251/Google-chief-says-people-warn-visitors-smart-speakers-homes.html (last updated Oct. 16, 2019).
[26] Ben Fox Rubin, *Amazon's Alexa Dives into Mobile World with Echo Earbuds, Glasses and Ring*, CNET (Sept. 26, 2019, 5:00 AM), https://www.cnet.com/news/amazons-alexa-dives-into-mobile-world-with-echo-earbuds-glasses-and-ring/.
[27] Russell Brandom, *To Use Alexa, You Have to Trust Amazon*, VERGE (Sept. 26, 2019, 1:24 PM), https://www.theverge.com/2019/9/26/20885512/amazon-alexa-voice-assistant-privacy-features-trust ("This is what Amazon does . . . . They make empty statements to sell their products and then continue to build a for-profit, surveillance dragnet without oversight and accountability[,]" quoting Evan Greer, a deputy director at Fight for the Future, a nonprofit advocacy group.).

applications, including those operated by third-parties for personal or professional use.[28] Some key features of Amazon Rekognition include object, scene, and activity detection; facial recognition; facial analysis; pathing; unsafe content detection; celebrity recognition; and identifying text in pictures.[29] Pinterest and C-SPAN have used Rekognition for object recognition and analytics[30]—it has even been used to identify guests at the royal wedding.[31] However, there are other, far more nefarious uses for this technology.

There are several problems that arise from Amazon's facial recognition software—including significant issues with racial bias.[32] While these issues are concerning, the problem with Rekognition that most directly impacts consumer privacy is the partnership between law enforcement agencies and Rekognition. On the federal level, Immigration Customs Enforcement (ICE) has utilized Rekognition to scan state driver's license databases for undocumented individuals, without the consent or knowledge of these individuals.[33] On a more local level, the Washington County Sheriff currently partners with Rekognition, paying between $6 and $12 per

[28] *Amazon Rekognition: Automate Your Image and Video Analysis with Machine Learning*, AMAZON WEB SERVICES, (last visited Nov. 1, 2019).
[29] *Id.*
[30] James Vincent, *Sky News Will Use Facial Recognition to Identify Celebs and Nobility at the Upcoming Royal Wedding*, VERGE (May 4, 2018, 9:17 AM), https://www.theverge.com/2018/5/4/17318354/royal-wedding-uk-facial-recognition-sky-news-date.
[31] *Id.*
[32] In 2018, the ACLU conducted a study using Rekognition on members of Congress. Through this study, the ACLU built a face database and search tool using 25,000 publicly available arrest photos, and then searched that database against public photos of every current member of the House and Senate using the default match settings that Amazon sets for Rekognition. The software incorrectly matched twenty-eight members of Congress, identifying them as other people who have been arrested for a crime. Nearly forty percent of Rekognition's false matches in our test were of people of color, even though they make up only twenty percent of Congress. For additional information on this study, *see* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[33] Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

month for access to Rekognition to scan mugshot photos against real-time footage.[34] While certain civilians may be comforted by the thought of their local police department going the extra mile to solve serious crimes, this partnership has thus far almost exclusively been used to solve petty crimes. For example, the Washington County Sheriff's office took surveillance footage from a store and then used Rekognition to run the screenshots from the footage against a mugshot database to solve one crime in which a woman stole a pair of shoes. They did the same thing in another case where a woman stole a $12 worth of gas from a hardware store.[35]

Even outside of the traditional crime-stopping context, the partnership between cities and Rekognition gives privacy advocates a pause—and for good reason. The city of Orlando, Florida has attempted to partner with Rekognition in order to create a singular system of surveillance throughout the entire city. Orlando's Rekognition pilot program was pulled twice due to insufficient resources;[36] however, if fully operable, this program would allow for real-time facial recognition of any civilian via the integration of Rekognition into a network of cameras throughout the city.[37] The director of this project, an employee of Amazon, attempted to minimize the Orwellian appearance of the partnership by stating that it could be used innocuously, for city officials to find out ". . . if the mayor of the city is in a place, or [if] there are persons of interest they want to track."[38] Regardless of these feeble attempts by Amazon to justify this partnership,

[34] Elizabeth Dwoskin, *Amazon is Selling Facial Recognition to Law Enforcement—For a Fistful of Dollars*, WASH. POST (May 22, 2018, 11:53 AM), https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/.
[35] Ben Fox Rubin, *Facial Recognition Overkill: How Deputies Cracked a $12 Shoplifting Case*, CNET (Mar. 19, 2019, 9:15 AM), https://www.cnet.com/news/facial-recognition-overkill-how-deputies-solved-a-12-shoplifting-case/.
[36] *Facial Recognition Pilot Program*, CITY OF ORLANDO, (last visited Nov. 1, 2019).
[37] Russel Brandom, *Amazon is Selling Police Departments a Real-Time Facial Recognition System*, VERGE (May 22, 2018, 11:06 AM), https://www.theverge.com/2018/5/22/17379968/amazon-rekognition-facial-recognition-surveillance-aclu.
[38] *Id.*

the privacy implications of a singular system of surveillance which allows the government to keep a constant eye on all of its citizens and to utilize facial recognition software to know exactly who they are watching at all times are clearly concerning to put it lightly. These privacy implications are only compounded when one considers the potential for Rekognition to be integrated in personal (rather than government-run) surveillance and home security systems—some of which, like Ring,[39] are also owned by Amazon.

C. Ring

Ring is a smart security device company that was acquired by Amazon in 2018 for $839 million.[40] Ring's product line includes floodlight video cameras and in-home security cameras,[41] but it is best known for its video doorbell which allows users to see, talk to, and record anyone and anything that comes to their door.[42] Ring devices are integrated with a complementing mobile application, Neighbors, where users can post videos directly from their Ring device as well as view posts from other "neighbors" within a five-mile radius.[43] Notably, police also have a presence on Neighbors—this is just one aspect of the troubling relationships between Ring and law

[39] Amazon does not currently use facial recognition technology in Ring devices and has stated that it does not collaborate with Amazon Rekognition. However, it has filed a facial recognition related patent application that could identify "suspicious" people and then alert law enforcement, which illustrates the potential for the integration of Rekognition with Ring devices and the privacy implications thereof. *See* Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 6:53PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.
[40] Rani Molla, *How Amazon's Ring is Creating a Surveillance Network With Video Doorbells*, VOX (Sep. 24, 2019, 3:56 PM), https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell.
[41] RING, https://ring.com (last visited Nov. 1, 2019).
[42] *Ring Video Doorbells*, RING, https://shop.ring.com/pages/doorbell-cameras (last visited Nov. 1, 2019).
[43] *Neighbors by Ring*, RING, https://shop.ring.com/pages/neighbors (last visited Nov. 1, 2019).

enforcement, relationships which are so concerning that they have caused both Congress[44] and numerous civil rights organizations to speak out.[45]

Of the roughly eighteen thousand law enforcement agencies in the United States, Ring has contracts with more than four hundred police departments across five hundred cities.[46] Ring's CEO has stated that the company's goal is to "have every law enforcement agency on the police portal."[47] These partnerships grant police access to a direct portal on the Neighbors app where they can access data related to consumers' use of Ring and submit video footage requests.[48] Police primarily use Neighbors by interacting with users, commenting on posts and asking users to file police reports.[49] Through this use, Neighbors essentially provides a tool for police to seek out petty crimes and ensure that they are formally reported, even if the victims of those crimes originally had no intention of doing so. But, the partnership between Ring and police departments goes further than a guaranteed presence on the Neighbors app. Indeed, when police want to acquire video footage captured on a Ring camera that may not have been posted on the Neighbors app, Ring will send a request to users located within a certain radius of the address of the crime (provided by law enforcement), on behalf of the police, asking for assistance with an investigation.

---

[44] Office of Ed Markey, *Senator Markey Calls for Answers About Amazon Camera Doorbell Company's Partnerships with Police Departments* (Sept. 5, 2019), https://www.markey.senate.gov/news/press-releases/senator-markey-calls-for-answers-about-amazon-camera-doorbell-companys-partnerships-with-police-departments.
[45] *Open Letter Calling on Elected Officials to Stop Amazon's Doorbell Surveillance Partnerships with Police*, FIGHT FOR THE FUTURE (Oct. 7, 2019, 2:18 PM), https://www.fightforthefuture.org/news/2019-10-07-open-letter-calling-on-elected-officials-to-stop/.
[46] Dell Cameron, *Ring Gave Police Stats About Users Who Said 'No' to Law Enforcement Requests*, GIZMODO (Aug. 30, 2019, 1:45 PM), https://gizmodo.com/ring-gave-police-stats-about-users-who-said-no-to-law-e-1837713840.
[47] *Ring Security System Program With Law Enforcement Raises Privacy Concerns*, CBS NEWS (Aug. 29, 2019, 8:46 AM), https://www.cbsnews.com/news/ring-security-system-program-with-law-enforcement-raises-privacy-concerns/.
[48] Caroline Haskins, *Amazon is Coaching Cops on How to Obtain Surveillance Footage Without a Warrant*, VICE (Aug. 5, 2019, 12:08 PM), https://www.vice.com/en_us/article/43kga3/amazon-is-coaching-cops-on-how-to-obtain-surveillance-footage-without-a-warrant.
[49] Alfred Ng, *Amazon's Ring Wants Police to Keep These Surveillance Details from You*, CNET (Aug. 21, 2019), https://www.cnet.com/news/amazon-ring-wants-police-to-keep-these-surveillance-details-from-you/.

According to Ring, users are not required to give video to police.[50] However, Amazon does guide police on how to more successfully obtain footage from users through these requests, by providing scripts to law enforcement, and giving them tips on how to adjust their tactics if they are unsuccessful obtaining footage.[51] If users decline to share their video footage, police may contact Amazon to obtain the footage regardless.[52] Notably, Ring's privacy policy states that it may provide a user's footage to law enforcement based on a "good faith belief" that it is necessary to comply with a "reasonable government request."[53] In short, like its parent company, Ring retains the right to give away its users' footage and police may get the video footage requested either way.

As if implicating the privacy of both users and non-user passerby alike in the crime-solving context were not bad enough, Ring also has a history of using customers' doorbell footage for its own advertising purposes. In a recent incident that garnered national media attention, Ring published a Facebook advertisement that included footage of a woman looking around a car, without obscuring her face.[54] The now-deleted advertisement asked users to identify and call the police on the woman, describing her as a suspected thief.[55] Following backlash, the company has now taken to blurring facial features in their advertisements. However, Ring's privacy policy does grant Ring and its licensees an "unlimited, irrevocable . . . right to use, distribute, store, delete, translate, copy, modify, display, sell, create derivative works from and otherwise exploit" any videos shared on Neighbors.[56] This clause essentially states that any footage captured by Ring, and

[50] *See* Cameron, *supra* note 46.
[51] *See* Haskins, *supra* note 48.
[52] *See* Ng, *supra* note 49.
[53] *Ring Terms of Service*, RING, https://shop.ring.com/pages/terms (last visited Nov. 2, 2019).
[54] Davey Alba & Ryan Mac, *Ring is Using Its Customers' Doorbell Camera Video for Ads. It Says It's Allowed To*, BUZZFEED NEWS (June 7, 2019, 3:00 PM), https://www.buzzfeednews.com/article/daveyalba/amazon-ring-doorbell-company-using-security-footage-for-ads.
[55] *Id.*
[56] *See Ring Terms of Service*, *supra* note 53.

shared on Neighbors, can be used by Amazon for nearly any purpose and, again, the privacy concerns illuminated by this incredibly permissive policy are clear. Through the proposed solutions below, we aim to better equip users in understanding and defending themselves against the privacy concerns that are implicated not only by these partnerships, but also by the aforementioned issues related to Rekognition and Alexa as well.

III. PROPOSED SOLUTIONS

A. Policy—The Prime Act

In developing a legal solution to alleviate the privacy concerns associated with Amazon products and services—specifically, Alexa, Rekognition, and Ring—the authors created a model statute. This statute aims to strike a balance between allowing Amazon to continue innovating without so gravely impacting consumer and non-consumer privacy. To this end, this bill—the Privacy Rights of Individuals Management and Enforcement (PRIME) Act—prohibits certain entities from using technology to identify or track an end user without obtaining the affirmative consent of the end user. In drafting this bill, the authors took inspiration from the European Union's General Data Protection Regulation (GDPR) and the United States' proposed federal bill entitled the Commercial Facial Recognition Privacy Act (CFRPA).[57] The remainder of this section will break down the statute; the statute is also attached to this paper as a supplementary material.

Definitions. There are four definitions included in the PRIME Act: affirmative consent, controller, personal data, and end user (which appears within the definition of personal data). These definitions are modeled based on those found in the GDPR and CFRPA.[58]

[57] *See generally* Commission Regulation 2016/679, of European Parliament and of the Council of April 2016 on the General Data Protection Regulation O.J. (L 199); Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).
[58] Commission Regulation 2016/679, of European Parliament and of the Council of April 2016 on the General Data Protection Regulation O.J. (L 199) Ch. I, art. 4; Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 2 (2019).

Prohibited Conduct. The PRIME Act makes it unlawful for Amazon and other tech companies to collect personal data from users without affirmative consent; use personal data to discriminate in violation of federal or state law; repurpose personal data; and share personal data with an unaffiliated third party without affirmative consent. The vast majority of inspiration for this portion of the Act was from the CFRPA.

Affirmative Consent. The PRIME Act also provides that Amazon and other tech companies must not only obtain the affirmative consent of the user, but it must also be able to demonstrate that the affirmative consent was obtained in clear, plain language. The language for the portion of the Act concerning affirmative consent derives from the CFRPA, while the requirement for clear and plain language is derived from the GDPR.

Transparency and the Right to Erasure. In a similar vein, the Transparency requirement aims to ensure that tech companies like Amazon must make it clear to users what it intends on doing with user data. The Right to Erasure provision gives users the right to have their data erased in certain circumstances. Taking inspiration from the GDPR's Right to Erasure provision, the PRIME Act carves out three situations in which an end user has the right to have their data erased: if the data is no longer necessary, if the data was unlawfully processed, or if the data must be erased in compliance with a legal obligation to which the controller is subject.

Exceptions. This Act carves out two exceptions for the release of personal data. The first exception allows the disclosure of data related to criminal convictions, offenses, investigations, or related security measure as long as warrants or subpoenas that are required by law are obtained. In requiring a warrant or subpoena, the goal is to circumvent current practices illustrated by Ring and Alexa particularly that have allowed police departments to obtain footage or audio with only a request rather than a subpoena or warrant. The second exception would allow for the disclosure of

data related to an emergency involving imminent danger, which essentially codifies the exigency exception which is prevalent in American Fourth Amendment jurisprudence.

Enforcement and Penalties. As with the CFRPA, The Federal Trade Commission would be responsible for enforcement of the PRIME Act.[59] In the case of lack of compliance with the provisions of this Act, entities whose total worldwide annual turnover exceeded $1 billion would be subject a fine of the greater of $10 million or two percent of the total worldwide annual turnover of the preceding financial year of the controller. Entities whose total worldwide annual turnover is less than $1 billion would be subject to a fine of two percent of the total worldwide annual turnover of the preceding financial year of the controller. These numbers are taken from the GDPR's penalty provision,[60] and ensure that a powerhouse tech company like Amazon would be subject to the larger of the two fines, while smaller tech companies would be subject to a significantly reduced fine, in an effort to encourage the growth of these potential competitors while still ensuring that they are abiding by basic privacy provisions.

B. Social—Shareholder Pressures & Watchdog Partners

In addition to the above policy solution, this paper proposes a social solution to Amazon's invasive practices by arguing that it is the role of Amazon's shareholders, in cooperation with watchdog organizations, to attempt to lead initiatives for better privacy practices at the company. Such shareholder initiatives can fill the void left by lawmakers and hold Amazon accountable. While it is oftentimes difficult for shareholder resolutions to make direct changes to company policies of large tech companies due to the structure of voting rights, measures voted on by shareholders can result in negative press for large tech companies, which can then result in changes

[59] Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 4 (2019).
[60] Commission Regulation 2016/679, of European Parliament and of the Council of April 2016 on the General Data Protection Regulation O.J. (L 199) Ch. III, art. 84.

in policies, if indirectly.[61] For example, shareholders have already pressured Amazon to avoid using facial recognition technology by putting forth two measures asking Amazon to stop selling Rekognition to government agencies and to do an audit of the privacy implications of the technology.[62] While these measures have not yet tangibly changed Amazon's policies, they have at the very least forced Amazon to publicly explain the use of this technology, thus bringing negative media attention onto the company and causing them to perhaps consider foregoing the usage of Rekognition altogether. Similar economic pressure from shareholders, with the backing of watchdog groups, can force Amazon to change other invasive practices across the company. Indeed, privacy advocate groups have already worked with shareholder activists to drive change at other large tech corporations.[63] These watchdog groups should make direct efforts to reach out to the shareholders of Amazon so that they can work together in order to encourage changes the company's practices, particularly those that negatively impact user and non-user privacy.

There are many groups that would make ideal partners for such shareholder initiatives, many of which have already been discussed in this paper. These include, but are not limited to, the ACLU,[64] the Electronic Frontier Foundation,[65] Open MIC (an organization that already works with activist shareholders to improve corporate governance at some of America's biggest

[61] *See* Salvador Rodriguez, *Zuckerberg Dodges Shareholder's Question About Whether He'd Give Up His Power at Facebook*, CNBC, https://www.cnbc.com/2019/05/30/facebook-ceo-mark-zuckerberg-dodges-shareholder-question-about-power.html (last updated May 30, 2019, 7:14 PM). Mark Zuckerberg, Facebook's CEO, recently faced a firestorm of criticism from shareholders demanding a reduction of his power and, despite Facebook rejecting multiple shareholder proposals critical of Zuckerberg, these proposals nonetheless received extensive press attention.

[62] Colin Lecher, *Amazon Shareholders Vote Down Proposals on Facial Recognition and Climate Change*, VERGE (May 22, 2019, 1:44 PM), https://www.theverge.com/2019/5/22/18635632/amazon-shareholders-vote-facial-recognition-climate-change-investors-employees.

[63] *See Our Work*, OPEN MIC, https://www.openmic.org/what-we-do (last visited Nov. 19, 2020) ("We provide education, tools and networks to support shareholder advocacy campaigns to change corporate practices across the media and tech sectors.").

[64] *See* Snow, *supra* note 32.

[65] *See* Reitman, *supra* note 6.

companies),[66] and Fight for the Future (a nonprofit that has already criticized Amazon Alexa products[67] and which currently tracks the implementation of facial recognition technology across the country).[68] If watchdog groups like these work alongside Amazon shareholders, their ability to generate negative press surrounding Amazon products' privacy implications would be compounded, thus enhancing their impact and potential to effect real change within the corporation.

C. Technological—Terms of Use Questionnaires

One of the most important goals of both of the above solutions is to ensure that Amazon users understand the potential privacy implications of using Amazon devices. In the spirit of enhancing consumer knowledge, this paper proposes a technological solution (ideally used in conjunction with the other solutions discussed in this paper) wherein users of Amazon products and services would have to correctly answer three multiple-choice questions[69] regarding the product's new terms of service (compliant with the PRIME Act) before use. Examples of questions that companies could use in these questionnaires are found in Appendix B. Importantly, these quizzes would not prevent anyone who has purchased an Amazon device from being able to use it, as users will be able to retake the questionnaire as many times as necessary. Instead, these questions would represent an added layer of friction, giving consumers a chance to pause and

[66] *See Our Work*, *supra* note 63.
[67] *See* Brandom, *supra* note 27.
[68] Ban Facial Recognition, FIGHT FOR THE FUTURE, https://www.banfacialrecognition.com/map/ (interactive map shows where facial recognition surveillance ishappening, where it's spreading to next, and where there are local and state efforts to rein it in) (last visited Nov. 8, 2019).
[69] Inspiration for this solution came from a tool implemented by NRKbeta (the tech arm of the Norwegian public broadcaster NRK), which created a tool that required users to answer three multiple-choice questions about the article before they were allowed to comment on that article. The company's stated goal was to "ensure that the commenters have actually read the story before they discuss it." For more information, see Joseph Lichterman, *This Site is "Taking the Edge Off Rant Mode" by Making Readers Pass a Quiz Before Commenting*, NIEMAN LAB (Mar. 1, 2017, 7:00 AM), https://www.niemanlab.org/2017/03/this-site-is-taking-the-edge-off-rant-mode-by-making-readers-pass-a-quiz-before-commenting/.

consider the implications of Amazon's privacy practices before making an active choice whether or not to use their newly purchased Amazon products. Ideally, terms of use questionnaires would create a more highly educated user base regarding tech products' privacy implications beyond products produced by Amazon.

D. Antitrust

Another potentially viable solution to address the concerns over Amazon's lack of protection for consumer privacy would focus not precisely on Amazon's privacy policies, but rather on their anti-competitive behavior more generally. Recently, the Federal Trade Commission launched an antitrust probe into Amazon, which could result in a major restructuring of the way that Amazon does business and could eventually impact the corporation's growth by reducing its power within the larger e-commerce market.[70] But, how do antitrust probes help Amazon's privacy problem? The short answer is that they do not, exactly; however, one of the reasons why Amazon's privacy protections are so abysmal may be because they have no real market competition. That is, given the choice between two corporations—Amazon, for example, and another e-commerce giant which we will call "Congo,"[71] wherein Congo offered nearly everything that Amazon offered, but with enhanced privacy protections—it is likely that consumers would choose the company with greater privacy protections. Unfortunately, nothing like Congo has been able to break through the market that is so dominated by Amazon. As such, it is at the very least worth watching the current antitrust probe, to see if it creates space in the market for other competitors—some of whom may very well be more devoted to consumer privacy protections than Amazon—to gain traction.

[70] Spencer Soper & Ben Brody, *Amazon Probed by U.S. Antitrust Officials Over Marketplace*, BLOOMBERG (Sept. 11, 2019, 4:00 AM), https://www.bloomberg.com/news/articles/2019-09-11/amazon-antitrust-probe-ftc-investigators-interview-merchants.

[71] The Congo Rainforest is the second largest rainforest in the world, with the first (of course), being the Amazon Rainforest. *See* Chrissy Sexton, *The 10 Largest Rainforests in the World*, EARTH.COM (Jan. 3, 2018), https://www.earth.com/news/10-largest-rainforests/.

IV. POTENTIAL OBJECTIONS, AUTHOR RESPONSES, AND CONCLUSION

At this point, it is necessary to address the significant objections that these proposed solutions would face by various groups, and how the authors, as proponents of the solutions, would respond to those objections. Amazon and other tech companies are the most obvious entities that would object to the proposed solutions. These companies would likely argue that enhanced regulations would curtail their ability to continue producing innovative products. Furthermore, Amazon may also argue that there will be detrimental economic effects (perhaps, in terms of reduced numbers of jobs)[72] to any reform that would force Amazon to focus on protecting consumers rather than on constant growth.[73] While it is undeniable that these corporations have significant resources to fund lobbying efforts, there would be sufficient counter-efforts to fund lobbyist groups that would favor protecting consumer privacy, particularly in the wake of the Facebook and Cambridge Analytica crisis. Furthermore, the proposed reforms outlined in the PRIME Act would require little time, energy, and resources to implement. The GDPR, after all, already provides residents of the European Union the right to transparency, right to erasure, and affirmative consent. Because companies like Amazon already do business within the European Union, they already have the infrastructure in place to abide by the GDPR, and would simply have to apply those same policies to their customers in the United States to comport with the PRIME Act. There is no reason why they cannot do so.

[72] Between June 2016 and June 2017, Amazon added more jobs than 46 out of 50 U.S. states—keeping this in mind, Amazon's objections to job reduction policies may be persuasive to consumers and politicians. *See* Ian Salisbury, *Amazon Created More Jobs Last Year Than 46 States*, MONEY (Sept. 25, 2017), http://money.com/money/4932593/amazon-job-creation/.

[73] "Growth obsession" has caused many tech companies—particularly Facebook—to focus only on adding users, active accounts, and amount of time spent using service as opposed to investing time, energy and resources into preserving the quality of the experience of users. *See* Fred Vogelstein, *Zuckerberg Finds It's Not Easy to Tame Facebook's Growth Obsession*, WIRED (Mar. 30, 2018), https://www.wired.com/story/zuckerberg-finds-its-not-easy-to-tame-facebooks-growth-obsession/ (discussing Facebook's redirection of growth obsession).

Politicians and police departments would also likely object to our proposed reforms, on the grounds that it is important to allow police to continue utilizing Amazon's technologies to solve crimes and enhance the safety of communities. These parties may argue that the privacy implications dwarf in comparison to the importance of these goals. Our response to this rhetoric would focus on the fact that these partnerships and technologies are most often used by police to solve petty crimes (when they are utilized at all),[74] and that this use merely represents a continuation of broken windows policing.[75] This policing style is problematic not only because it disproportionately targets minorities, but also because it does not actually work.[76] Rather than utilizing these technologies to continue to invest time and resources into this type of ineffective policing, the authors would encourage police departments to explore new methods of policing and crime solving that are more effective, and do not have such detrimental impacts on civilian privacy rights.

Finally, and most ironically, consumers themselves may also protest the proposed regulations, for several reasons. First and foremost, the average consumer is likely uneducated as

[74] When asked to comment on the County Sheriff's partnership with Rekognition, Jeff Talbot (the public information officer for Washington County) even admitted that the technology is rarely used but attempted to justify its use anyway. *See* Rubin, *supra* at note 35. Jeff Talbot stated, "[a]re we solving 500 crimes a year using this technology? Absolutely not . . . . But do we think this is an important piece of technology that we should be utilizing while doing it responsibly? Absolutely." *Id.*

[75] "Broken windows" generally refers to the theory that maintaining social order by policing low-level offenses can prevent more serious crimes. Sarah Childress, *The Problem with "Broken Windows" Policing*, PBS (June 28, 2016), https://www.pbs.org/wgbh/frontline/article/the-problem-with-broken-windows-policing/. For additional information on this style of policing, and the devastating impact that it has had on low-income communities of color, see *id.*

[76] Bernard Harcourt has written rather extensively on the failures of the broken windows theory. In 2005, he and Jens Ludwig published results from a five-city social experiment which provided housing vouchers to 4,600 low-income families living in high-crime communities characterized by high rates of social disorder. *See* Bernard E. Harcourt & Jens Ludwig, *Broken Windows: New Evidence from New York City and a Five-City Social Experiment*, 73 U. CHI. L. REV. 271 (2006). The vouchers allowed these families to move to less disorderly communities. *Id.* at 271, 276. The results of the experiment (arguably the first rigorous test of the broken windows theory), provided no support for a relationship between social disorder and crime as hypothesized by the original authors of broken windows theory. *Id.* at 277.

to just how extreme the privacy implications are of using services like Alexa, Rekognition, and Ring. Lack of public knowledge likely led to a corresponding lack of public concern over the protection of consumer privacy in this context—concern that would be necessary to justify, for example, the friction that would now be built into Amazon products through the terms of use questionnaires. The authors' response to these objections would be to ensure that watchdog groups and community partners properly educate consumers as to the myriad of ways that their lives can be negatively impacted by the current lack of privacy protections, and how the proposed reforms ameliorate those issues. While some may argue that consumers live in a post-privacy world,[77] the importance of privacy as a closely-held American value and legal concept reflects that the desire for at least *some* level of privacy is an aspect of human nature.[78] The advent of technology has not yet completely obliterated this innate, uniquely human need for privacy—a need, and a right, that these proposed reforms aim to protect, to the ultimate benefit of even the most reluctant consumer.

Amazon is truly a technological giant, with an empire that spans across various industries online and off. Particularly in light of Amazon's forthcoming expansion of Alexa-enabled devices, as well as its partnerships with police through Ring products and Rekognition services, it is clearer now than ever that Amazon's privacy problem goes far beyond consumers and has the potential to impact each and every person in the United States, if not the world. Through a multidisciplinary approach focusing on law, policy, and technology, there are solutions to these problems. However,

[77] Nova Spivack, *The Post-Privacy World*, WIRED, https://www.wired.com/insights/2013/07/the-post-privacy-world/ (last visited Nov. 8, 2019) ("Privacy is dead. In fact, it has been dying a rather operatic death for over a decade. . . . In the post-privacy world, privacy is no longer guaranteed or expected. . . . [W]e can't stop this shift from happening[.]").

[78] *What Is Privacy?*, PRIV. INT'L (Oct. 23, 2017), https://privacyinternational.org/explainer/56/what-privacy ("Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. . . . Privacy is essential to who we are as human beings . . . .").

lawmakers and advocates must rapidly address the grave privacy concerns outlined in this paper before their full, detrimental impact is realized.

SUPPLEMENTAL MATERIALS

V. APPENDIX A: THE PRIME ACT

Privacy Rights and Information Management Enforcement Act (PRIME Act)

A BILL to prohibit certain entities from using various technologies to identify or track an end user without obtaining the affirmative consent of the end user.

This Bill lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

This Bill protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The free movement of personal data within the United States shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

1. DEFINITIONS.

In this Act:

(a) Affirmative Consent. The term ‘affirmative consent’ means the consent of an end user that involves an individual, voluntary, and explicit agreement to the collection and data use policies of a controller.

(b) Controller. The term ‘controller’ means a covered entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

(c) Personal Data. The term ‘personal data’ means any information relating to an identified or identifiable natural person (‘end user’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. PROHIBITED CONDUCT.

(a) In General. Except as provided in Section 6, it shall be unlawful for a controller to knowingly—

(1) use various technologies, including, but not limited to, virtual assistants, voice recognition software, facial recognition software, video cameras, and/or microphones to collect personal data, unless the controller obtains from an end user affirmative consent in accordance with Section 3;

(2) use personal data to discriminate against an end user in violation of applicable Federal or State law;

(3) repurpose personal data for a purpose that is different from those presented to the end user under Section 2(a)(1); or

(4) share the personal data with an unaffiliated third party without affirmative consent that is separate from the affirmative consent required under Section 2(a)(1).

3. AFFIRMATIVE CONSENT.

(a) Where processing is based on consent, the controller must be able to demonstrate that the end user has consented to processing of his or her personal data.

(b) The controller must present the terms of consent in an intelligible and easily accessible form, using clear and plain language.

4. TRANSPARENT INFORMATION REGARDING PROCESSING OF PERSONAL DATA.

(a) The controller shall provide information related to the processing of personal data to the end user in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or where appropriate, by electronic means.

(b) The end user shall have the right to obtain from the controller access to the personal data and following information:

(1) the purposes of processing;

(2) the personal data collected and the length of retention by the controller of such personal data; and

(3) the existence of the right to request from the controller erasure of personal data or restriction of processing of personal data concerning the end user.

5. WITHDRAWING CONSENT AND ERASURE OF PERSONAL DATA.

(a) The end user retains the right to withdraw his or her consent to the processing of his or her personal data at any time, subject to the exceptions set forth in Section 6 herein. It shall be as easy to withdraw as to give consent.

(b) The end user shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(2) the personal data have been unlawfully processed; or

(3) the personal data have to be erased for compliance with a legal obligation in Federal or State law to which the controller is subject.

6. EXCEPTIONS.

This Bill shall not apply to the processing of personal data—

(a) related to criminal convictions, offenses, investigations, or related security measures, subject at all times to any and all warrant or subpoena requirements as required by law; and

(b) related to an emergency involving imminent danger or risk of death or serious physical injury to an individual.

The data processed under the circumstances described in this Section shall be processed under the control of official authority

or when the processing is authorized by a State law providing for appropriate safeguards for the rights and freedoms of end users.

7. ENFORCEMENT.

The Federal Trade Commission shall be tasked with enforcement of this Act pursuant to the applicable terms and provisions as if the Federal Trade Commission Act (15 U.S.C. § 41 et seq.) was incorporated into and made a part of this Act.

8. PENALTIES.

Entities who violate these provisions shall be subject to a fine in the amount of the greater of $10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year of the violating controller.

VI. APPENDIX B: TERMS OF USE QUESTIONNAIRES

The following represent sample questions that users would have to answer prior to using their newly-purchased Amazon products. It is the hope of the authors that these questions would facilitate the education of Amazon consumers by illuminating key provisions of the PRIME Act.

First Sample Question:
Amazon reserves the right to share your personal data with third-party advertisers: (a) True or (b) False.

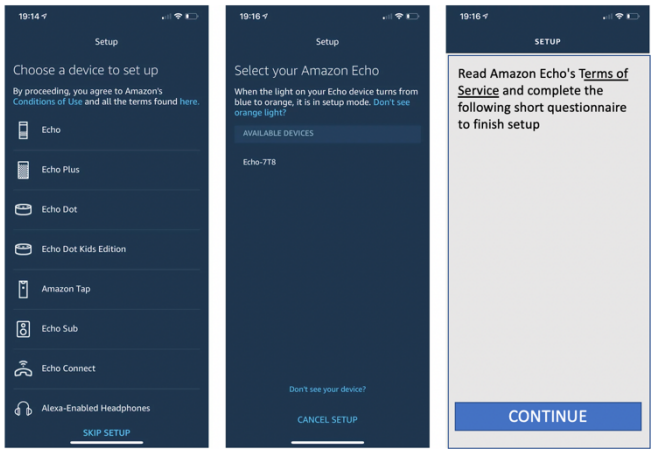
For this question, under the PRIME Act, Amazon may only share a user's personal data with third-party advertisers once the user gives affirmative consent to process his or her data for such purpose.

Second Sample Question:
If you wish for Amazon to delete your personal data from its records, how do you make such request? (a) Email datainfo@amazon.com*; (b) Call 1-800-856-3232; (c) Go to user settings; (d) All of the above.*

This question incorporates another important provision in the PRIME Act, the right to erasure, highlighting the various ways a user may request Amazon delete his or her personal data.

Third Sample Question:
Under what circumstances does Amazon have the right to share your personal data with law enforcement? (a) At any time; (b) With a valid warrant and/or subpoena as required by law; (c) When you are using Amazon Ring.

Because Amazon may only share a user's personal data with a valid warrant and/or subpoena under the proposed PRIME Act, this question provides users with the security and notice that they have regulations regarding how or what personal data is being shared and with whom.



The above figure represents a prompt that a user would see when attempting to complete setup for an Alexa-enabled Echo device.