Responses to Written Questions Submitted by Honorable Roger Wicker to Andrew DeVore

Question 1. I'm interested in how Amazon interacts with small businesses or other marketplace sellers that use your platform. In many instances, Amazon is selling products as a direct competitor to small business on its platform. Does Amazon use any data it collects from small businesses or other marketplace sellers using its platform to inform decisions related to the items that Amazon will sell directly to consumers? Please explain.

Response. Customer trust is of utmost importance to Amazon. More than half of all products sold on Amazon are sold by third-party sellers, and sellers are important customers. Just like any retailer, we have information about the items sold in our store and use it to provide a better customer experience, including analytics to improve efficiencies in fulfillment and shipping and to empower all of our sellers. We provide an array of innovative services, tools, and data to our selling partners to help them sell more, increase their efficiency, and manage their inventory. We also advise them on opportunities to expand their product offerings. Furthermore, data and information such as price, best sellers, product recommendations, and customer reviews are all publicly available, and are used by not only Amazon and our selling partners, but by large and small retail competitors alike.

We are proud of the great success that hundreds of thousands of small and medium-sized businesses have found on Amazon since we opened our store to third-party sellers more than 15 years ago. Our seller partners use Amazon's websites in multiple languages and network of more than 100 fulfillment centers to reach customers across the world, and their sales are growing faster than our own retail sales.

Written Questions Submitted by Honorable Jerry Moran to Andrew DeVore

Question 1. Your written testimony discussed the concept of "privacy by design" as a solution for incorporating privacy safeguards in the development of the services and products that Amazon offers. Given their "multiple layers," are there concerns or barriers to clearly and succinctly explaining to the consumer what these protections are?

Response. Customer trust is of utmost importance to Amazon, and we endeavor not only to make our use of data and privacy protections clear to customers in simple and easy to understand terms of use, but in the intuitive presentation and use of our products and services. Just one example of this is the visual indicator that appears on the Echo device to let you know when the wake word has been detected and audio is being streamed to the cloud to operate the service.

Question 2. Efforts to draft meaningful federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Response. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. As a result, when we collect data customers may perceive as particularly sensitive, we consider whether to take additional steps to mitigate the risk that customers will be surprised or upset by our collection or use of that data.

We similarly believe it is important to focus legislative attention on data that presents a privacy risk to an individual. Sensitive data is personal information that identifies a particular individual or a device that belongs to that individual, either alone or when linked with other sensitive categories of data such as health information, financial information, and any information about an individual aged 13 or younger.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at https://internetassociation.org/positions/privacy/ as they begin to explore a potential national framework.

Question 3. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee federal legislation affecting cross-border data flows?

Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy

questions we start with the customer and work backwards. We appreciate NTIA's recognition that the regulatory landscape needs to be harmonized in order to avoid a contradictory patchwork of obligations that will burden organizations and confuse users. For the United States to lead on privacy, we need a consistent approach to privacy that provides clarity for American consumers and businesses.

We also agree with NTIA that any action addressing consumer privacy should be applied comprehensively across private sector organizations that use personal data. The distinction between "physical" and "digital" is increasingly blurring, and now largely meaningless. What many refer to as the "digital economy" is best understood as a set of technologies now in widespread, if not universal, use throughout the economy in industries as diverse as advertising, agriculture, automotive, manufacturing, and retail. Industries not thought of as "digital" will reap huge benefits, as will society as a whole. Thus, treating tech-enabled businesses or innovation leaders differently makes little sense, particularly as new technology proliferates rapidly across every industry.

Question 4. Also included in NTIA's request for comments, how should the U.S. Government encourage more research and development of products and services that improve privacy protection?

Response. The U.S. Government has long been the global leader in innovation policy and research and development. Thoughtful policymaking that puts the consumer first will lead to continued innovation in privacy protective products and features that people will enjoy, while a patchwork of regulatory obligations will divert significant resources from developing such features. Privacy regulations that place additional overhead and administrative demands on organizations, potentially displacing research and development, should be required to produce commensurate consumer privacy benefits. We agree with NTIA that being overly prescriptive can result in compliance checklists that stymie innovation, and a patchwork of regulations would exacerbate this problem.

Question 5. As GDPR includes requirements like the "right to portability" and the "right to be forgotten," it is clear that these provisions aim to promote the consumer's ownership of their data by requiring companies to abide by their requests to permanently delete or transport their personal data to another company. However, how are these concepts enforced when the consumer's data is submitted as an input to one or multiple proprietary algorithms employed by the company?

Response. We have for many years made it easy for customers to access their personal data, ranging from order history, content and devices, to voice recordings. Personal data varies by customer and may range from purchasing history to address and credit card information to customer service interactions. We provide access to personal and customer information in a manner most customers have found relevant and useful for the services that they use.

Question 6. Are the outputs of the company's algorithm decidedly the consumer's personal information and required to be deleted or transported at the request of the consumer? If so, do these requirements remain the same if the data outputs are anonymized?

Response. An algorithm is simply a step-by-step set of directions to accomplish a particular task or achieve an identified outcome. Amazon uses machine learning tools and algorithms across multiple products and service features, and their outputs typically are neither personally identifiable nor sensitive. GDPR recognizes a number of lawful bases for processing EU personal data, including legitimate interest, consent, and contract performance. We have a long-standing commitment to privacy and data security. Privacy is built into our services from the ground up – we design and continually improve our systems with customer security and privacy in mind. We strive to limit, de-identify, or pseudoanonymize data where possible or appropriate for customer services. We comply with GDPR access and deletion according to the lawful bases for processing EU personal data.

Question 7. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Response. Our long-standing commitment to privacy aligned us well with the GDPR principles; however, meeting its specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices. Although data in aggregated form is not subject to GDPR, companies must often use individually tracked data as an input to achieve aggregated outputs, so the process is subject to all of the restrictions and administrative burdens of GDPR. We encourage Congress to ensure that additional overhead and administrative demands any legislation might require actually produce commensurate consumer privacy benefits.

Written Questions Submitted by Honorable Shelley Moore Capito to Andrew DeVore

Question 1. According to a study by Pew Research, only 38% of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns. I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Response. Our customer-centric approach has led Amazon to follow privacy by design principles since our founding. We design our products and services so that it is easy for customers to understand when their data is being collected and control when their data is shared. While written disclosures and policy notices are an important foundation for transparency, we do not rely on disclosures alone when collecting customer data. We strive to make that collection intuitive to the customer based on product functionality, and that collection is directly tied to a concrete customer benefit. Where the collection of data is less likely to be intuitive to the customer, we strive to help the customer understand the data collection with conspicuous messaging, such as an indication that we are collecting the data together with a "learn more" link.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Response. Creating smart privacy policies and practices takes careful attention, and a strong focus on the customer makes it easier to make good decisions. As new laws take effect, overly prescriptive rules and regulations may have the unintended result of longer, and less transparent, privacy policies.

Furthermore, new inventions like Amazon's Echo can create novel challenges for providing customers transparency and control, requiring invention and innovation to deliver great products that preserve customer trust. We need to ensure any potential new consumer privacy framework does not prevent the ability to invent new mechanisms for consumer transparency and privacy control. With the Echo, we had to invent new transparency techniques for a device that did not have a screen. But, when you start with the customer and work backwards, the correct answer is often right in front of you. With the Echo, we were able to use product design to communicate to customers about data collection. For example, the light ring at the top of the Amazon Echo turns blue to alert the customer that the device has heard the "wake word" and is streaming the customer's voice recording to the cloud.

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information. What are some of the measures your companies are doing to teach consumers – and specifically older consumers – about what data they share on your platforms?

We design our products and services so that it is easy for all of our customers to understand when their data is being collected and control when their data is shared. We endeavor to provide this transparency not just in the terms of use and account settings for each experience, but in the experience itself. For example, customers can manage their Alexa privacy settings from a single page in the Alexa app and on the Amazon website. This includes the ability to listen to and delete voice recordings associated with their account and control skill permissions.

We are also developing product services and features with all of our customers in mind. For example, customers with disabilities and older customers can especially benefit from Alexa's presence in their lives, and from the greater independence a voice user interface can provide. Our teams are working hard to ensure Alexa devices and the Alexa Mobile app are accessible to these customers and have an easy device setup. We are also working to launch new features enabling Alexa to meet daily customer needs through a combination of building new experiences and extending functionality.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Response. Product recommendations, which help customers discover items they might not otherwise have found, are core to the Amazon shopping experience. Customers see these features in clearly labeled formats like "Frequently bought together" and "Customers who viewed this item also viewed." We use aggregate data from our customers' browsing and purchase behavior in order to make recommendations, such as suggesting baby wipes and tear-free shampoo for a customer purchasing diapers.

At Amazon our entire business is built and based on customer trust and this is also true for our advertising program. We take the privacy of our customers very seriously. All information used to provide customers with interest based ads is anonymized and maintained and used in separate dedicated systems. We provide clear and prominent notice regarding our advertising practices both on our properties and where possible in ads that we deliver on third party properties. We make it simple for users to opt out of receiving interest based ads from us.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Response. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. Customers should know how their data is being used and be empowered to make their own individual determination of the benefits they gain from choosing to use new services and technologies. We believe that

policymakers and companies like Amazon have very similar goals – protecting consumer trust and promoting new technologies. Congress should contemplate a federal framework that meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and their attendant rights; that includes mechanisms for customers' rights and controls that provide commensurate privacy benefits to customers; that is mindful of the impact of regulation on small- and medium-sized companies; and that applies consistently across all entities and segments of the economy.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at https://internetassociation.org/positions/privacy/ as they begin to explore a potential national framework.

Question 6. In April, the European Union (EU) passed the General Data Protection Regulation (GDPR) in order to protect personal data and uphold individual privacy rights. These new regulations have created uncertainty for U.S. firms, despite several already coming into compliance. Innovation is important to small businesses, especially in rural America. The new European standards have created massive hurdles for these businesses to be in compliance. Many small companies in Europe are already expressing an inability to afford the legal consequences. For example, if a rural grocery store advertises online and provides a link to coupons. Under the GDPR compliance rules, this simple practice can result in expensive legal consequences. For those who do business in Europe, do you think GDPR has the potential to have negative impacts on rural small businesses in Europe?

Response. Yes. GDPR carries significant compliance requirements for the handling, retention, and deletion of personal data. Amazon is a well-resourced company with exceptional technical talent; however, meeting GDPR's specific requirements caused us to divert significant resources away from our core mission of invention on behalf of customers. Small- and medium-sized businesses are important customers for Amazon, and we remain concerned this regulation can have the effect of hampering small- and medium-sized businesses with less resources.

Question 7. California has already passed a sweeping consumer protection law that threatens established business models throughout the digital sector. I appreciate the industry taking the initiative in creating a framework, in addition to the privacy principles released by the US Chamber of Commerce.

As we begin discussing the appropriate position of the federal government, can you describe what actions we should investigate more closely for any potential national framework?

Response. Privacy issues are complex, and there is great risk of unintended consequences from privacy regulation that is not carefully crafted to deliver clear privacy benefits. When answering privacy questions we start with the customer and work backwards. Customers should know how their data is being used and be empowered to make their own individual determination of the benefits they gain from choosing to use new services and technologies. We believe that policymakers and companies like Amazon have very similar goals – protecting consumer trust and promoting new technologies. Congress should contemplate a federal framework that meets individuals' reasonable expectations with respect to how the personal information they provide

companies is collected, used, and shared, and their attendant rights; that includes mechanisms for customers' rights and controls that provide commensurate privacy benefits to customers; that is mindful of the impact of regulation on small- and medium-sized companies; and that applies consistently across all entities and segments of the economy.

Amazon is a member of the Internet Association (IA) and we encourage policymakers to look to the IA's Privacy Principles available at https://internetassociation.org/positions/privacy/ as they begin to explore a potential national framework.

Question 8. Who, in your opinion, is the appropriate regulator to oversee any framework and why?

Response. A national privacy framework should primarily be enforced by the Federal Trade Commission (FTC). The FTC is the U.S. regulator with core competency and subject matter expertise on consumer privacy, and should continue to serve that role in future frameworks.

Question 9. According to recent research by Magid, a media research firm, 35% of millennials share their password to access streaming services. I certainly understand that the terms and conditions of these services already note that access is for personal use and not to be shared with others. And that the account holder remains responsible for the actions of that third party. However, as the number younger generations sharing their password grows so has the potential for abuse. This "overly sharing of passwords" and the younger generation operate differently than many my age.

Are your policies flexible to cover a third party that may use a friend's or spouse's password? Is this something we should consider as we create federal guidelines?

Response. We take account security very seriously and have a number of ways we can identify logins that do not appear to come from the account owner. We do understand that many customers have a legitimate need to share the benefits of our services, so we have designed those services to allow such sharing without needing to share passwords. Prime members can share benefits in their Amazon Household without having to share individual passwords.

Sharing benefits through Amazon Household requires both adults to link their accounts in an Amazon Household and agree to share payment methods. Each adult keeps their personal account while sharing those benefits at no additional cost. Teen logins allow up to four teens (aged 13 – 17) in the same household to have their own independent Amazon login connected to their parent's account.

Question 10. Thank you Mr. DeVore for meeting with me earlier this week, I wanted to touch on something we discussed in my office. Smart speakers (like Alexa, Google Home, HomePod) have dominated the market place in recent years. They have opened up our homes to A.I. integration allowing us to control our homes, plan out our lives, or purchase things just by asking. However, these always on devices have also raised privacy concerns. It is important to note that always listening is not always recording. Could you briefing go through how my voice is recorded on your devices, stored, and secured?

Response. Alexa is a cloud-based voice service that lets customers play music, ask questions, make calls, send and receive messages, get information, news, sports scores, weather, and more. Alexa is available through a wide range of products, including Amazon's Echo family of devices, other Amazon products such as our Fire TV and Fire tablet devices, and devices developed by third party manufacturers participating in our Alexa Voice Service program. Alexa operates in a similar manner across the range of products on which it is available, although customers access Alexa differently based on the type of Alexa-enabled product they use.

From early-stage development, we built privacy deeply into the hardware and service by design, and with Alexa and Amazon's Alexa-enabled products we strive to put the control with our customers. On our Echo family of devices, customers speak to Alexa by saying the "wake word" (Alexa, Amazon, Echo, or Computer) or, on some Echo devices, by pressing the action button on the top of the device. Echo devices use "on-device keyword spotting" technology that analyzes acoustic patterns to detect when the wake word has been spoken using a short, on-device buffer that is continuously overwritten. This on-device buffer exists only in temporary memory (RAM); no audio is ever recorded to any on-device storage. The device is effectively always in standby mode, with the wake word functioning as an audible "on switch," and the device does not stream audio to the cloud unless the wake word is detected or the action button is pressed. The user experience also provides customers with a clear indication of when the device is turned on and audio is being streamed for the purpose of processing. When the wake word is detected or the action button is pressed, a visual indicator appears on the device to clearly indicate to the customer that it is streaming audio to the Amazon cloud (e.g., a blue light ring on the Echo device and a blue bar on the Echo Show's screen). We also offer a setting where customers can choose to hear an audible tone when their Echo device begins and ends streaming audio to the cloud.

When audio is streamed to the Amazon cloud, our systems for "automatic speech recognition" (converting audio to text) and "natural language understanding" (interpreting the meaning of text) determine the meaning of the customer's request so that Alexa can respond appropriately. Amazon encrypts all communication between Echo devices and Amazon's servers, and stores all customer data securely on our servers.

We also give customers control of their voice recordings in the cloud. Not only are customers able to see and play back the voice recordings associated with their account, customers can also delete those voice recordings one-by-one or all at once.

Echo devices also come with a "microphone off" button that enables customers to manually control when their device's microphone is on. When the button is pressed to turn the microphones off, the microphones are electrically disconnected and a dedicated red LED is illuminated to indicate the microphones are off. As an additional safeguard, we designed the circuitry of Echo devices so that power can only be provided either to this dedicated red LED or to the device microphones, not to both at the same time. As a result, if the dedicated red LED is illuminated, the microphones are off and cannot stream audio to the cloud.

Customer trust is of the utmost importance to our continued success, and we take that responsibility most seriously.

Question 11. Since I can ask Alexa to order me an Uber, I am curious about what information is shared with third parties to complete a booking or confirm a ride share? (Understanding that I've already given permission to perform these services)

Response. We design our products and services to limit the amount of personally identifiable information that may be shared, and to share that information in a way that's transparent to our customers. We do not share a customer's personally identifiable information with developers through these products and services without the customer's agreement. We take the privacy and security of our customers' data seriously, and we regularly review our privacy practices and related customer messaging and revise them as appropriate.

For example, when a customer with an Echo device interacts with an Alexa "skill" (Alexa's equivalent of an app) provided by a third party developer, we do not share the customer's identity with the skill developer. Only when a customer chooses to share their identity with a developer – e.g., if a customer takes steps to link their Amazon account to their Uber account so they can request a ride through Alexa

– is the developer able to associate usage of the developer's skill with that customer's name. We share with the developer the content of the customer's request to the skill so the skill can respond accordingly, but we only share personally identifiable information to which the customer has granted the developer access. As a result, customers are involved anytime we share their personally identifiable information with a skill developer. Customers can also change these permissions at any time from their Alexa app.

Responses to Written Questions Submitted by Honorable Todd Young to Andrew DeVore

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

What questions should policymakers be asking in developing data portability rights?

Response. We encourage policymakers to explore what specific consumer benefit is to be achieved by any new legislation, and how best to accomplish that benefit while avoiding potentially serious downside risks. There are circumstances where portability may be useful to a consumer, and others where it would not serve any useful purpose and may even be counterproductive, including potentially threatening the privacy of other individuals, posing fraud and security risks, and fueling third party markets that trade in personal data.

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Response. Consumers that have uploaded personal information into a service should be able to easily download that information so that they can transfer it to another service. But the right of portability should not require that a company produce that information in a proprietary format or in a way that creates security risks or exposes a company's trade secrets or intellectual property.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Response. Consumers that have uploaded personal information into a service should be able to easily download that information so that they can transfer it to another service. But the right of portability should not require that a company produce that information in a proprietary format or in a way that creates security risks or exposes a company's trade secrets of intellectual property.