Statement of Andrew DeVore

Vice President and Associate General Counsel

Amazon.com, Inc.

before the

United States Senate

Committee on Commerce, Science, and Transportation

September 26, 2018

Thank you, Chairman Thune, Ranking Member Nelson, and Members of the Committee. I am Andrew DeVore, Vice President and Associate General Counsel at Amazon. Amazon's mission is to be Earth's most customer-centric company. Our corporate philosophy is firmly rooted in working backwards from what customers want and continuous innovation to provide customers better service, more selection, and lower prices. We apply this approach across all areas of our business, including those that touch on consumer privacy.

Amazon's Approach to Privacy

Customer trust is our highest priority – we know we must get privacy right in order to meet our customers' high expectations. Many core features of the Amazon experience – including foundational shopping features like showing what other customers bought and product recommendations – depend on us using customer data responsibly and transparently. Understanding what products customers like and how customers use our services helps us make better recommendations, improve our products and services, and invent new products and services that will delight our customers.

While compliance with applicable laws provides a baseline for our privacy decisions, our foremost concern when considering privacy issues is customer trust. We have known from our very beginnings as an online bookstore that maintaining customer trust is essential to our success. Our customers trust us to handle their data carefully and sensibly in a secure and appropriate manner in line with their expectations. Any privacy mistake risks the loss of that trust and serious reputational damage even if there is no violation of privacy laws.

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. And we are not in the business of selling our customers' personal data.

Two examples – Product Recommendations and Amazon Echo – help highlight how, by working backwards from the customer, Amazon gets privacy issues right and builds products and services that earn customer trust. Product recommendations, which help customers discover items they might otherwise not 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.

In a vacuum, this might sound concerning – "Amazon is tracking what customers search and purchase." But because product recommendations are clearly labeled, intuitive to customers, and provide a valuable service, customers love them. Customers are not surprised that we collect and use data in this way. That is one of our goals – while our terms of use of course describe the collection of this data, we don't want customers to feel they need to read our terms to avoid being surprised. As product recommendations illustrates, we strive to make our data collection practices intuitive and transparent for customers by tying them directly to the shopping and discovery experience.

Alexa is a cloud-based voice service that lets customers play music, ask questions, make calls, send and receive messages, and get information, news, sports scores, and weather, among other things. On our Echo family of devices, customers speak to Alexa by saying the "wake word" (Alexa, Amazon, Echo, or Computer). So, from across a room, customers can say, "Alexa, play music," "Alexa, what's the weather forecast for tomorrow," or "Alexa, turn on the living room lights," and get an immediate response, with no need to use their hands or look at a screen.

With the Echo, Amazon invented a brand new category of devices totally unfamiliar to customers. So we knew we had to get privacy right to preserve our customers' trust. From early-stage development, we built privacy deeply into the Echo hardware and Alexa service by design, and we put customers in control.

As a result, we designed the wake word to function as an audible "on button" for Echo devices. Echo devices detect the wake word by using on-device keyword spotting technology that identifies acoustic patterns that match the wake word. No audio is sent to Amazon unless either the device detects the wake word or Alexa is activated by pressing the action button present on some Echo devices.

Once Alexa is activated, Echo gives customers clear notice it is streaming audio to the cloud. For instance, the light ring on Echo will turn blue or a blue bar will appear on Echo Show, an Echo device with a screen. Customers can also configure Echo devices to play a short audible tone to indicate the device has recognized the wake word and is streaming audio to the cloud. We also employ additional technical measures to minimize the amount of audio and background noise streamed to the cloud, and we give customers control of their recordings, including the ability to see and play back each recording associated with their account and delete those voice recordings one-by-one or all at once.

We also include an additional physical control for customers – a microphone off button that electrically disconnects the Echo device's microphones, combined with a dedicated red light confirming the microphones are off. As an additional safeguard, we designed the circuitry of Echo devices so that power can only be provided either to that dedicated red light or to the device microphones, not to both at the same time. So when the dedicated red light is on, customers know the microphones are off and no audio can be recorded and streamed to the cloud.

These multiple layers of privacy controls for Alexa and our Echo family of devices are a result of our privacy by design process, which incorporates privacy considerations into every stage of product development.

Policy Viewpoints

Our customer obsession leads us to four perspectives for the Committee's consideration as you consider a federal approach to privacy and specifically the effect of the California Consumer Privacy Act of 2018 (CCPA) and the European Union General Data Protection Regulation (GDPR).

First, built on our foundation as a retailer and our longstanding commitment to privacy and data security, we know data privacy issues are complex and greatly impact every sector of the economy. Legislation addressing these issues should be carefully crafted in a process that involves all the relevant stakeholders to ensure that we all share the benefits of technology with confidence that our data is being handled responsibly and transparently.

Second, while our long-standing commitment to privacy aligned us well with the GDPR principles, 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. We encourage Congress to ensure that additional overhead and administrative demands any legislation might require, actually produce commensurate consumer privacy benefits.

Third, Congress should consider possible unintended consequences of the CCPA approach. Amazon supports the CCPA's goals of giving consumers visibility and control when businesses collect and sell their personal information. But because the CCPA was quickly enacted there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best practices in privacy. For example, CCPA's definition of "personal information" goes beyond information that actually identifies a person to include any information that "could be linked with a person," which arguably is all information. The result is a law that is not only confusing and difficult to comply with, but that may actually undermine important privacy-protective practices like encouraging companies to handle data in a way that is not directly linked to a consumer's identity.

Finally, creating smart privacy policies and practices takes careful attention, and a strong focus on the customer makes it easier to make good decisions. When you start with the customer and work backwards, the correct answer is often right in front of you. Technology is an important part of modern life, and has the potential to offer extraordinary benefits we are just beginning to realize. 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. We share the goal of finding common solutions, especially during times of fast moving innovation. As technology evolves, so too will the opportunities for all of us in this room to work together.

Thank you, and I look forward to your questions.