August 20, 2018

The Honorable Ed Markey
United States Senate
255 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Markey:

Thank you for your letter to Jeff Bezos dated July 26, 2018. We take feedback on our products, services, and how we operate from customers and stakeholders very seriously. On behalf of Amazon Web Services (AWS), please find below a response to your inquiry.

Customer trust, privacy, and security are our top priorities at AWS. We have long been committed to working with federal and state legislatures to modernize outdated laws to enhance the privacy and security of our customers by preventing law enforcement from accessing data without a warrant. We have repeatedly challenged government subpoenas for customer information that we believed to be over-broad and have won decisions that have helped to set the legal standards for protecting customer speech and privacy interests.

Amazon Rekognition is a service we announced in 2016. Since then, we have seen customers use the image and video analysis capabilities of Amazon Rekognition in ways that materially benefit both society (e.g. preventing human trafficking, inhibiting child exploitation, reuniting missing children with their families, and building educational apps for children), and organizations (e.g., security through multi-factor authentication, processing documents, and preventing package theft). AWS is not the only provider of services like this and we remain excited about how image and video analysis can be a driver for good in the world, including in the public sector and law enforcement.

We have an Acceptable Use Policy ("AUP") that prohibits the use of our services for "[a]ny activities that are illegal, that violate the rights of others, or that may be harmful to others." This includes violating anybody's Constitutional rights – essentially any kind of illegal discrimination or violation of due process or privacy right. Customers in violation of our AUP are prevented from using our services.

We also take claims about Amazon Rekognition inaccuracy very seriously. The advantage of a cloud-based machine learning application like Amazon Rekognition is that it is constantly improving. As we continue to improve the algorithm with more data, our customers immediately get the benefit of those improvements. We continue to focus on our mission of making Amazon Rekognition the most accurate and effective tool for identifying people, objects, and scenes – and that certainly includes ensuring that the results are free of any bias that impacts accuracy.

Regarding the ACLU's recent blog post about its trial of Amazon Rekognition, in which it said they found 28 incorrect matches out of 535 Members of Congress from a data set of 25,000 mugshots, using an 80% confidence level, we have been unable to verify the findings as ACLU has not published the data set, methodology, or results in detail despite a direct request from us to do so. However, when we conducted our own test of Amazon Rekognition using a dataset of over 850,000 faces commonly used in academia

(30x larger in size than the ACLU reported dataset) and all Members of Congress (House and Senate) using a confidence threshold setting of 99% (as we recommend in our customer documentation), our misidentification rate dropped to zero despite the fact that we are comparing against a larger dataset of faces.

With regard to the specific questions you raised in your letter, I can provide the following answers: we do not disclose information about our customers without their permission, which is a fundamental tenet of earning and maintaining customers' trust in AWS. All customers, including law enforcement agencies, must abide by AWS's terms and conditions, and our Acceptable Use Policy, which require compliance with all laws, including applicable civil rights laws. Customers in violation of our terms will be prevented from using our services. If there is an issue with AWS services or content, or to report potential abuse of AWS services, customers and individuals can contact abuse@amazonaws.com.

Customers provide their own datasets for use in Amazon Rekognition, which means the customer must provide both the photo of the person or object they want to match and the database of photos against which they wish to make that match. Amazon Rekognition does not identify if an image or video includes a person under 13, but provides customers the ability to estimate the age range of a person based on an image or video. AWS’s terms and conditions explicitly require customers to comply with applicable laws, including COPPA, in their use of Amazon Rekognition. Any use by a customer of Amazon Rekognition must comply with COPPA, including the obligation to obtain a parent’s verifiable consent to collection of a child's personal information. Amazon Rekognition’s public documentation directs customers to COPPA-related resources provided by the United States Federal Trade Commission. Moreover, our customers' trust, privacy, and the security of customer content are our highest priority and we implement appropriate and sophisticated technical and physical controls, including encryption at rest and in transit, designed to prevent unauthorized access to, or disclosure of, customer content and ensure that our use complies with our commitments to customers. Please see https://aws.amazon.com/rekognition/faqs/ for more information.

With any technology, there are always questions about responsible use. With machine learning, for example, there’s a difference between using machine learning to identify a food object and using machine learning to determine whether a face match should warrant considering any law enforcement action. The latter is serious business and requires much higher confidence levels. We continue to recommend that customers use a minimum 99% confidence level for law enforcement matches, and then use the matches as only one input among others that are appropriate for the particular use. But, machine learning is a very valuable tool to help law enforcement agencies, and while being concerned it’s applied correctly, we should not pre-emptively ban a technology because of potential for misuse, particularly when we know it is being used for good in many demonstrated instances. It is a very reasonable idea, however, for the government to weigh in and specify what confidence levels it wants law enforcement agencies to meet to assist in their public safety work.

Thank you again for contacting Amazon. Please feel free to contact me if I can provide any further information or be of any further assistance on this or any other matter.

Michael Punke

Michael Punke
Vice President, Global Public Policy, Amazon Web Services