November 9, 2018

Mr. David Redl
Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725

Attn: Privacy RFC
Washington, D.C. 20230

Re: Comments on Developing the Administration's Approach to Consumer Privacy (Docket Number: 180821780-8780-01)

Dear Administrator Redl,

Thank you for the opportunity to submit comments on the administration's approach to consumer data privacy.

It is important to emphasize that whatever the administration's approach, data localization should not be part of any privacy policy. The practices of data localization popping up around the world make sensitive consumer data less secure. India is the most recent bad example on data localization.

The following opinion about the vulnerabilities associated with localization, which makes data less, not more, secure, was printed in the Washington examiner on October 17, 2018:

> The Reserve Bank of India issued a directive that requires data on payment transactions occurring in India to be stored within Indian borders as of Oct. 15, 2018. This practice, known as data localization, is an approach some countries have pursued as a means of ensuring law enforcement and government access to data, but the security consequences will ripple throughout the digital universe.
>
> Requiring data storage in a particular location increases the security risk to data from more citizens, businesses, and governments. Companies carefully select where they will store data and how they will store data based off of security concerns. Often, data isn't even stored in one place — it is scattered throughout servers that make up various clouds, and some of that data is constantly moving. If criminals know that sensitive records, particularly bank transactions, credit card numbers, and routing information, are stored in one place, their targets become significantly easier to exploit.
>
> India, like China, is aiming for fully digital payments promoted by the government through its Cashless India Campaign, but moving all monetary exchanges as well as document exchanges to digital makes security even more important.

India wants “unfettered” access to data, and that includes American data, especially anyone traveling into India or anyone communicating with someone in India. What’s troublesome is that a vast majority of Americans won’t know that a foreign government is stockpiling their personal banking information when they travel in and out of India.

Targeting banking information and financial institutions was only the first step for the Indian government to get “unfettered” access to all data. The Indian parliament is also considering a bill that would mandate all data collected, disclosed, shared, or processed within India to be stored within India. This would give Indian officials access to data, not only on its own citizens, but data passing through India on foreign nationals, including Americans. The next phase isn’t isolated to financial transactions and banks — it implicates American technology companies.

Americans need assurances that their rights are respected, but data localization directly impacts our protections under the law.

While India has expanded its market to allow investment beyond its borders, companies might shy away from Indian markets because of stringent data localization laws. Data localization across the entire Indian economy would cost up to 0.8 percent of the country’s GDP, decrease investments by 1.3 percent, and create welfare losses equivalent to 11 percent of the monthly salary. It is clear that data localization does not do anyone justice, except for the governments who seek unfettered access to data on their subjects.

The heightened security and privacy risks caused by localization to all types of data outweighs any potential law enforcement gain, especially when these concerns have been confronted in other countries by focusing law enforcement access to data, rather than the jurisdiction where data is held. In the United States, the Clarifying Lawful Overseas Use of Data, or CLOUD Act sponsored by Sen. Orrin Hatch, R-Utah, and Rep. Doug Collins, R-Ga., updated U.S. law to create a more efficient mechanism of reciprocal treaties where nations can request data directly from service providers located within each other's borders, as long as the foreign government has laws in place sufficiently protecting privacy, human rights, and due process. The CLOUD Act also allows American companies to challenge a law enforcement demand in court if the demand would cause the company to violate another country's laws.

Though China and Vietnam have passed data localization laws, other countries that desire to be part of global commerce that have considered localization saw how damaging this policy would be. Rather than localization, Brazil instituted compliance requirements, which still allow for data to move freely. Companies must indicate where data might be stored, managed, or processed, and an agreement between the company and authorities over the exchange of information or certify that the jurisdiction of the company's remote services will not impede government access to data where warranted.

The goal is not to interfere with law enforcement; the reality is that data localization would cause more headaches for law enforcement on the cybersecurity front than it is worth. Data localization is not the answer to law enforcement difficulties. Agreements on how and when data can be accessed may take longer to negotiate, but in the end, it creates a more secure environment where citizen's most sensitive data will be protected from bad actors.

India and the U.S. should work through the process outlined by the CLOUD Act to address concerns about law enforcement access to data, while maintaining American security and constitutional protections.

I am happy to respond to any questions or comments you might have on this or other matters as it relates to consumer data privacy.

Regards,

Katie McAuliffe
Executive Director
Digital Liberty