November 9, 2017

The Honorable Bob Latta
Chairman, Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

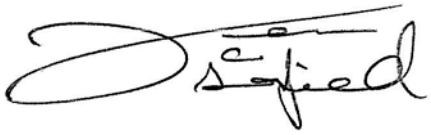
RE: Question for the Record
Hearing on "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs"

Dear Chairman Latta:

Thank you again for the opportunity to testify before the Subcommittee on October 12, 2017, on the importance of digital trade to U.S. jobs and the economy. Enclosed you will find my response to the question for the record submitted to me by Dr. Burgess.

As the Subcommittee continues its work and oversight on this matter, please consider me as a resource.

Sincerely,



Dean C. Garfield
President & CEO

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

The Honorable Michael C. Burgess

1. In your testimony you note that enabling cross-border data flows and curbing data localization are important to the success of multinational technology companies like the ones in your association. In what ways do these policies impact the health care and public health sector?

In my testimony I explained how all industries – from manufacturing to agriculture – rely on cross-border data flows to remain competitive in the global economy, and the health sector is no different. The free flow of data allows health care professionals to collaborate overseas to run tests and find cures to diseases. It allows new, cutting-edge treatments to be disseminated among hospitals and local doctors and reach patients at never before realized rates, regardless of their country of origin. It helps public health officials respond to and treat public health outbreaks across oceans before diseases can be spread to new areas. The health sector, perhaps more than many others, has been transformed by the internet and the free flow of data across borders.

However, concerns about the security of that data and protecting the privacy of patients must be addressed in order to fully realize these benefits and build trust between doctors, patients, companies, and governments. Some countries, such as China and Australia, have opted to force companies to keep patient data within the borders of their countries – this is a mistake. Measures of this type degrade the ability of doctors, academics, and health professionals to collaborate and share information to bring state-of-the-art treatment to their markets. Additionally, as I explained in my testimony, restricting the ability of companies to transfer information over border raises the cost for companies to host and process data. In the health sector, what this translates to is increased healthcare costs and a degradation of the ability of American technology companies and health companies to do business in those markets.

Concerns about security and privacy, of course, are legitimate and worth considering. First, it is important to understand that data security is not a function of its location. Security is the result of companies and governments using best security practices across their networks and technologies. For responsible handlers of data, this is built into their systems and cultures, regardless of location of data facilities. In fact, requiring specifically health data to be stored within certain borders can make it less secure because bad actors will know exactly which systems need to be breached to obtain access to that data.

In addition, medical data privacy can be achieved without incurring the economic costs and discriminatory nature of forced data localization. Governments absolutely should protect the privacy of their citizens, but this can be done with interoperable, globally oriented privacy regimes. I believe that the Cross-Border Privacy Rules (CBPR) created under the auspices of the Asia-Pacific Economic Cooperation Forum (APEC) is a good example of such an international program. Under this system, companies and government certify to a set of privacy standards to which data must be handled in order to be transferred between countries. Countries can also set sector-specific standards for particularly sensitive data, such as medical data, to further ensure that their citizens are adequately protected when it is being transferred overseas.

I hope that this thoroughly answers your question, and I am happy to expand further if you have any additionally follow-up. Thank you.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org