Statement of the U.S. Chamber of Commerce

ON: **Cross-Border Data Flows**

TO: **U.S. House of Representatives Committee on Energy and Commerce**
Subcommittee on Commerce, Manufacturing, and Trade

DATE: **September 17, 2014**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are also active members. We are therefore cognizant not only of the challenges facing smaller businesses, but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—e.g., manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on issues are developed by Chamber members serving on committees, subcommittees, councils, and task forces. Nearly 1,900 businesspeople participate in this process.

The U.S. Chamber of Commerce is pleased to take this opportunity to address the importance of cross-border data flows to the U.S. business community. The Chamber is the world's largest business federation, representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and is dedicated to promoting, protecting, and defending America's free enterprise system.

The movement of information across national borders drives today's global economy. Cross-border data flows allow businesses and consumers access to the best available technology and services, wherever those resources may be located around the world. The seamless flow of data across borders benefits all industry sectors, from manufacturing to financial services, education, health care and beyond. The seamless transfer of information is as critically important as it is inexorably linked to the growth and success of the global economy.

To function in the international marketplace, businesses need continuous, reliable access to data, wherever they are located. Routine business activities, such as providing goods and services to customers, managing a global workforce, and maintaining supply chains, require the transfer of data among corporate locations and to service providers, customers, and others situated around the world. In addition, as the Internet has facilitated the growth and success of micro-multinationals, as small businesses now have access to billions of potential customers beyond their borders and are able to compete based on the quality of their offerings, unconstrained by geographic limitations.

The global value of e-commerce is estimated at $8 trillion per year. And this amount is not limited just to large multinational technology companies: 75 percent of the value-added created by the Internet is generated by companies in traditional industries, such as manufacturing, and small- and medium-sized enterprises that rely heavily on Internet services have 22 percent greater revenue growth than companies that do not.

A survey released this week by the International Trade Commission found that digital trade increased U.S. GDP by $517.1-$710.7 billion (3.4-4.8 percent) as U.S. firms sold $935.2 billion in products and services online in 2012. With 95 percent of the world's consumers located outside of the U.S. borders and the world population increasingly connecting online, this number is only poised to grow. Consequently, we must work to ensure that the United States remains a worldwide leader in this economic revolution and that American companies have access to the world's growing middle class.

Despite the myriad benefits of transferring data between countries, some governments continue to push for restrictions on cross-border data flows. This limits the ability of companies to process, store, and access information on a global basis, and impedes end users from being able to choose the best available technologies and access information regardless of location.

Recent restrictions proposed in response to allegations regarding foreign government surveillance inappropriately conflate concerns about access to data for national security and law enforcement purposes with commercial use of, and access to, data. Other restrictions are rooted in government efforts to bolster domestic industry and support national companies. Ultimately, however, instead of creating jobs, these rules reduce efficiency, increase costs to local businesses, and block access to customers abroad, as they simultaneously prevent local

consumers from buying the best products and services. Restrictions on cross-border data flows only serve to isolate domestic economies from the economic growth potential associated with the digital economy.

Uses of Cross-Border Data Flows

Policymakers and citizens often fail to appreciate the many benefits of cross-border data flows in their day-to-day lives. Maintaining the ability to transfer data is not just essential to business operations and revenue growth, but it also facilitates socially beneficial global initiatives and help improve the health and well-being of people around the world. Chamber members, across all sectors, rely on cross-border data flows for a variety of function, and it is important to highlight that most companies are not using or selling the data itself as a cash generative business, but are using it to create better products and services.

Medical Data

A number of multinational medical device manufacturers routinely transfer data across jurisdictional boundaries for maintenance and repair purposes.[1] For instance, one device manufacturer lamented the difficulties engineers face when attempting to carry out critical functions, such as providing real-time service on large medical equipment to facilitate effective patient care. Sophisticated equipment of this nature often cannot be readily transported to repair facilities, and in some cases the device requiring service is the only machine of its type in a particular geographic area.

If an engineer who is specially trained to service a highly complex machine is not permitted to access the device remotely to conduct repairs (because she may incidentally access the data of patients who benefitted from the machine that morning), then patients who need the machine that afternoon may be turned away. In this example, cross-border data transfer restrictions literally could have life or death consequences for patients. Some of the data that is transported are used for purposes well beyond commercial purposes, including public health and safety concerns.

Stopping Fraud

Cross-border data flows are used to identify fraudsters who, after racking up huge debts in one country, are able to start fresh with a clean slate by moving to another jurisdiction. Blocking credit histories from following individuals across borders also affects law-abiding expatriates who are unable to open accounts or obtain loans because they have no way to prove they have a strong credit history in their country of origin.

[1] In addition to medical devices, other types of machinery may be repaired in a virtual environment, thus sparing consumers time and effort. For example, a recent report highlighted the fact that Tesla Motors is now able to make safety changes to plug-in electric vehicles using "over-the-air software updates," calling into question the use of the term "recall" when discussing this type of maintenance. *See* Angela Greiling Keane, *Tesla's Musk Has Point About 'Recall,' Ex-Regulator Says*, BLOOMBERG NEWS, Jan. 21, 2014, http://www.bloomberg.com/news/2014-01-21/tesla-s-musk-has-point-about-recall-ex-regulator-says.html (last visited Apr. 22, 2014).

Creating Efficiencies for Manufacturing and Energy Development

One of our members operating in the energy sector uses cross-border data flows to help oil and gas manufacturers function at top capacity while promoting safety and ensuring continuity of service. To achieve this, the company remotely collects operational data from equipment in use in locations scattered across the globe, then employ diagnostic and prognostic analyses of the data to alert customers of necessary maintenance and potential risks. Hampering companies' ability to monitor the data transmitted by such equipment from around the world both decreases efficiency and increases the likelihood of a preventable accident that could damage infrastructure and even result in loss of life.

Responding to Remote Crises

The insurance and reinsurance industry offers another strong argument in favor of allowing the rapid and nimble movement of data across borders. In the event of a major natural disaster, immediate access to clients' insurance contracts and records is essential to deploying needed resources to policyholders and helping begin the rebuilding process for affected individuals. When cross-border data transfer restrictions impede the movement of these data, or restrict the storage of such data outside the country of origin, the results can be disastrous. For example, if a particular country requires an insurer to maintain all its data pertaining to citizens of that country within the country's borders, the insurer may have no way to access the data it needs to help affected residents recover from a tsunami, earthquake, or other major disaster. If the data center is under 10 feet of water, it is impossible assess who has coverage or how to start processing valid claims. The ability to maintain backup copies of insurance coverage data in multiple remote locations helps the company ensure continuity of service even in the face of massive power outages and physical destruction of servers or other company property that typically would be used to validate coverage and provide assistance.

Managing a Global Workforce

Regardless of industry sector, all companies large and small have one thing in common: employees. Perhaps no commercial data transfer need is as acute, or as universal, as the need for companies to be able to access data about their workforce around the world. Having a complete and accurate picture of the company's personnel, wherever in the world they may sit, is essential to deploying and managing intellectual capital effectively. A centralized corporate directory, the existence of which could be threatened by stringent data transfer restrictions, also is key for obvious logistical purposes. Furthermore, innovation is driven by cross-cultural project teams collaborating in virtual environments, working together to solve problems and develop products from locations around the world. And IT technicians staggered across time zones help ensure that assistance is always available for employees working unconventional hours or logging in from remote locations. Modern businesses simply cannot thrive, or even function effectively, without the ability to manage their talent on a global basis.

Tracking Pandemics, Saving Lives

The Internet has proven to be an invaluable resource for global health organizations, enabling them to make massive leaps forward in monitoring the outbreak and spread of infectious diseases around the world. But this type of tracking is possible only through the rapid

collection and dissemination of real-time medical data concerning patients in multiple countries. Owing in part to increasing globalization and modern transportation, what may appear as an isolated cluster of illness in one region of one country easily could explode into a national epidemic or a global pandemic in a matter of weeks or even days.

Unless epidemiologists and other medical professionals are able to communicate freely about emerging health crises with their colleagues located elsewhere, there is little the medical community as a whole can do to slow or stop the spread of disease outbreaks.

Restrictions on Cross-Border Data Transfers

Localization requirements also may have the effect of decreasing data security. Forcing companies to maintain local data centers frequently results in the establishment of minimally-resourced facilities that are more likely to permit network intrusions and data compromises. In the end, compliance costs are passed on to consumers when prices for goods and services are increased to fund local outposts rather than having centralized service centers that maximize efficiency. In addition, data transfer restrictions often have a disproportionate effect on smaller businesses, in some cases potentially thwarting growth opportunities altogether and preventing today's startups from becoming tomorrow's multinationals. For these businesses, data transfer restrictions have the effect of cutting the "world" out of the "World Wide Web."

Despite the multitude of benefits associated with allowing data to flow seamlessly across borders, governments around the world continue to step up efforts to impose restrictions on cross-border data transfers. Although in some cases the restrictions are meant to promote privacy, too often the motives are protectionist or reflect the conflation of commercial issues with national security concerns. These misguided policy choices take us down a path that stifles job growth and leads to economic stagnation.

Unfortunately, regardless of intent, many of the regulations affecting the commercial use of data impose unduly restrictive constraints on international data flows, doing more harm than good to the affected economies. Initiatives aimed at improving data transfer regulations should refrain from focusing on a single set of rigid, one-size-fits-all rules. Instead, such initiatives should focus on developing flexible, privacy-protective regulations that can coexist with, and adapt to, technological advances.

Data transfer restrictions generally fall into two categories: data localization requirements and privacy regulations. Data localization rules, which usually are binary in nature, impose an outright ban on transferring data out of the country, or a requirement to build or use local infrastructure and servers. These regulations often are based on misperceptions that are easily refuted. Accordingly, it is more effective to demonstrate the flawed reasoning behind the laws and persuade policymakers to repeal them altogether, rather than attempt to find common ground on the localization issue.

Conversely, privacy regulations are nuanced and rooted in important cultural and societal concerns. Such rules generally seek to protect legitimate interests and fundamental rights. Thus, it is imperative that governments work together to understand the underlying interests when developing solutions to ensure that local privacy regimes do not unnecessarily restrict trade. Furthermore, procedures to protect privacy and secure data are vital to modern business

operations. Given the concerns of consumers and governments alike, companies strive to develop trustworthy products that meet privacy expectations. Increasingly, those expectations include ensuring that privacy protections travel with the data, regardless of where they are transferred, stored, or accessed.

In the past year, high-profile revelations regarding government surveillance activities resulted in a number of proposals regarding data localization and transfer restrictions. Although some of the adverse reactions are understandable, thus far most of the efforts to alleviate concerns regarding surveillance have failed to address the real issue. A useful step in the right direction would be for members of Congress to more vocally distinguish between issues of law enforcement and national security collection and use of data with that of the private sector.

The means by which governments access foreign personal data should have no bearing on the laws that regulate corporate data transfers or the mechanisms companies employ for cross-border transfers. The political rhetoric connecting government surveillance to commercial data transfers ignores the fact that a completely separate legal regime often controls law enforcement access to data. Efforts to reform government surveillance must directly address government actions – these concerns cannot be resolved by creating new restrictions on businesses.

Separating Fact from Fiction: Forced Data Localization

During the last few years, there have been a number of data localization proposals around the world. Whether in response to national security surveillance concerns, a desire to protect domestic industry or some combination of the two,[2] these proposals are based on a number of false assumptions and ultimately fail to meet any of the stated goals.

Myth: Data localization will promote domestic industry.

Fact: Data localization requirements reduce competitiveness by walling off domestic businesses from the billions of potential customers outside of the home country's borders. This isolation reduces investment and access to capital – the ability to assess a potential borrower's creditworthiness or to spot potentially fraudulent activity often depends on the ability to move data across borders.

Myth: Requiring local data centers will create jobs.

Fact: Jobs are created by businesses that leverage a global network of data centers, using the best available technology to increase efficiency regardless of location. This enables domestic industries to focus on the quality of their products and services, better positioning them to compete in global markets. Data centers can cost hundreds of millions of dollars to build and operate, and even a cutting-edge data center requires fewer than 150 workers.

[2] *See, e.g.*, Press Release, Eur. Comm'n, What does the Commission mean by secure Cloud computing services in Europe? (MEMO/13/898) (Oct. 15, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-898_en.htm (last visited Apr. 30, 2014) (proposing the creation of a virtual "Schengen Area" for data in response to surveillance revelations and supporting the development of European cloud computing solutions).

Myth: Data localization increases security.

Fact: Data security depends on a plethora of controls, not on the physical location of a server. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take a data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions.

Myth: Data localization will lower costs for domestic business.

Fact: Requirements for local servers could hurt domestic industry by compelling local businesses to sacrifice efficiency and seek out more expensive, less reliable services. Localization requirements may limit the ability of firms to access logistics and supply chain infrastructure, conduct effective research, secure appropriate insurance, or readily participate in financial markets.

Opportunities for International Cooperation in Trade Agreements

The ability to transfer data across borders has become inextricably intertwined with the ability to trade freely. Current trade discussions, such as the U.S. – EU Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA), present opportunities to bridge differences among privacy regimes and developing regional data transfer mechanisms.

Data Transfer Provisions in Trade Agreements

Addressing cross-border data transfers through trade agreements is not a novel approach. A number of trade agreements have even acknowledged the significance of cross-border data transfers to the global economy as a fundamental tenet of the agreement. For example, Article 14.5 of the U.S.-Panama Trade Promotion Agreement highlights the importance of helping small- and medium-sized enterprises "overcome obstacles" that impede their participation in electronic commerce and maintaining "cross-border data flows of information as an essential element in fostering a vibrant environment for electronic commerce."[3]

Similarly, Article 15.8 of the United States-Korea Free Trade Agreement (KORUS) recognizes "the importance of the free flow of information in facilitating trade" and pushes the parties to the agreement to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[4]

---

[3] Trade Promotion Agreement, U.S.-Pan., art. 14.5, June 28, 2007, *available at* http://www.ustr.gov/trade-agreements/free-trade-agreements/panama-tpa/final-text (last visited Apr. 22, 2014).

[4] Free Trade Agreement, U.S.-S. Kor., art. 15.8, June 30, 2007, 46 I.L.M. 642. Both the KORUS and the EU – Korea Trade Agreement (KOREU) include provisions specific to financial services, with KOREU stating "each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier." Free Trade Agreement, Eur. Union-S. Kor., art. 7.43, Aug. 20, 2010, 2010/0075 (NLE).

In addition, the Chamber's members support an ambitious Trans-Pacific Partnership Agreement (TPP) that preserves the ability to transfer data across borders and look forward to a final TPP is likely to include provisions aimed at preventing member countries from adopting national laws that would restrict cross-border transfers of personal data. Despite these positive steps, more needs to be done to embed strong, binding commitments in future agreements.

The Transatlantic Trade and Investment Partnership

The TTIP represents one of the best opportunities to institute cutting-edge data transfer protections, notwithstanding misplaced concern related to U.S. government surveillance issues. Ideally, the TTIP should address data transfers by including three key features: (1) a commitment to allowing cross-border data transfers; (2) a prohibition on data localization requirements; and (3) a non-exhaustive list of data transfer mechanisms. In conjunction with the third issue, the agreement should also ensure ongoing cooperation between the United States and EU with respect to developing new data transfer mechanisms. The TTIP also must meaningfully limit the transfer prohibitions allowed under the General Agreement in Services (GATS) Article XIV.[5] If the United States and the EU are able to implement strong and ambitious provisions in the TTIP, that agreement may serve as a template and baseline for the TISA negotiations that will affect nearly 70 percent of the global economy.[6]

Conclusion and Recommendations

Cross-border data transfers are indispensable to the growth of the digitized global economy. Cross-border data transfers are critical for all modern business. The global economy simply cannot afford to revert to digital isolationism. The question is whether governments will implement legal regimes to promote a beneficial expansion of the data economy, or if the cumbersome systems currently in place will continue in force, hindering innovation and slowing progress. The path forward must include cooperation between regulators and businesses working together to determine how best to address important concerns about privacy and data security without crippling economic growth.

Regardless of the specific geographic or political context, the following key concepts are critical to ensuring agile cross-border data transfer regimes that will facilitate the global data flows of the future:

- Recognition that there are many different approaches to regulating cross-border data transfers, and that differing mechanisms can ensure a similar desired level of data protection.
- Movement away from rigid one-size-fits-all regulations toward more outcome-focused regimes.
- A clear delineation between the issue of government access to data and the distinct issue

[5] General Agreement on Trade in Services art. XIV, Apr. 15, 1994, 1869 U.N.T.S. 183, *available at* http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV (last visited Apr. 30, 2014).

[6] OFFICE OF THE U.S. TRADE REPRESENTATIVE, NOTICE NO. 2013-21836, PARTICIPANTS IN TRADE IN SERVICES AGREEMENT (2013), *available at* http://www.regulations.gov/#!documentDetail;D=USTR_FRDOC_0001-0270 (last visited Apr. 22, 2014).

of cross-border data transfers in a commercial context.

- Assurance that the frameworks we develop today are fit for tomorrow.
- Implementing strong, binding trade agreement commitments that prohibit data localization requirements, support unimpeded data flows, and encourage interoperability among privacy regimes.

Technological advances and an increasingly globalized economy have brought us to a policy crossroads: one path leads to a "splinternet" of economic isolation, characterized by misguided attempts to safeguard data by building protectionist walls. Since the dawn of the global trading system, this isolationist approach has repeatedly caused economic stagnation. The other path is one of shared global economic growth fueled by an increasingly interconnected digital economy. Ideally, this would be supported by regulatory frameworks that encourage competition by opening borders for businesses of all sizes, driving innovation, creating jobs and lowering prices.

The Chamber encourages Congress to seize the opportunities presented at this critical juncture and push towards preserving the ability to transfer data across border and in turn continue the flow of benefits.