Cross-Border Data Transfer: Myths vs. Facts

The rapid and seamless movement of data across borders is essential to the 21st century global economy — driving growth and innovation across all sectors. Some countries, however, are considering — or have implemented — measures that mandate data localization and restrict cross-border data flows. These kinds of laws not only impede local innovation and undermine data security, but also put local business at a competitive disadvantage. This document seeks to dispel misconceptions regarding data localization requirements and cross-border data transfer requirements.

1. X MYTH: Data localization requirements and data transfer restrictions benefit the economies of the countries that implement them.

✔ **FACT:** Data localization requirements and data transfer restrictions hurt local companies by preventing them from accessing the most innovative software services and products, including cloud applications, artificial intelligence solutions, and cybersecurity tools. This can prevent local industry from participating in global supply chains and accessing customers in foreign markets, while severely hampering local innovation. Such data restrictions also increase costs within the implementing country for goods and services that use data in various phases of their life cycles including design, production, marketing, and sales, making local products and services less competitive vis-à-vis foreign products and services — in both domestic and export markets. As these restrictions create a significant burden on the implementing country's overall competitiveness, they also undermine the country's attractiveness as a destination for investment and R&D. Data localization requirements and restrictions on international data transfers have been estimated to reduce economic growth by billions of dollars in the countries that have implemented them.[1]

2. X MYTH: Transferring data cross-borders is only a priority for multinational technology corporations.

✔ **FACT:** Cross-border data transfers power innovation and growth across the globe and all sectors of the economy — from manufacturing and farming to local start-ups and service providers. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output. In contrast, businesses in countries that have localization mandates or restrict data flows will be at a competitive disadvantage because they will not have access to the same cutting-edge services.

[1] For example, according to the European Centre for International Political Economy, the negative economic impacts range from a reduction in Gross Domestic Product (GDP) of 1.1 percent in China to a reduction in GDP of 1.7% in Vietnam. Conversely, ECIPE also estimates that, if such data restrictions are lifted, local firms stand to benefit significantly due to substantial increases in the availability of productivity-enhancing data-intensive services, such as computer services, technical services, and R&D services, and due to gains in total factor productivity for local firms.

3. X MYTH: It is necessary to restrict cross-border data transfers to allow law enforcement to conduct investigations of user data where there is evidence of criminal conduct.

✔ **FACT:** It is not necessary to impose data localization requirements for law enforcement authorities to gain access to the data. Laws in some countries authorize law enforcement authorities, following appropriate judicial proceedings, to access data based on the citizenship or residency of the data subject rather than the location where the data is stored. If such laws do not exist, or if they are in conflict with laws of a country in which such data is stored, countries have several options for obtaining the data. International agreements — including Mutual Legal Assistance Treaties (MLATs) or Agreements (MLAAs), multilateral treaties such as the United Nations Convention on Transnational Organized Crime, and other agreements, such as those authorized by the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act — can establish foundations for mutual legal assistance and reciprocal transfers of law enforcement data. In addition, courts may issue requests to authorities abroad for the transfer of data through letters rogatory; moreover, direct international cooperation between law enforcement agencies, including undertaking joint investigations, can create avenues for accessing data stored abroad. With the multiple pathways available for pursuing data stored overseas, data localization laws are unnecessary to enable effective law enforcement investigations.

4. X MYTH: Data localization requirements and data transfer restrictions are necessary to ensure cyber and data security.

✔ **FACT:** How data is protected is much more important to security than where it is stored. Far from keeping data more secure, data localization requirements and limits on data transfers can actually undermine data security. When governments restrict a company's ability to move data, they create unnecessary obstacles to data security.

Cross-border data transfers are important for cybersecurity for several reasons. First, storing data at geographically diverse locations can enable companies to reduce network latency, maintain redundancy and resilience for critical data in the wake of physical damage to a storage location, and obscure the location of data to reduce risk of physical attacks. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.

5. X MYTH: Data localization requirements and data transfer restrictions are necessary to protect personal data.

✔ **FACT:** Data localization requirements and data transfer restrictions are not necessary to ensure that companies process and use data consistent with a country's data protection laws.

Organizations that transfer data globally should implement procedures to ensure that data transferred outside of the country continues to be protected. Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate global data transfers. In both the public and private sectors, data protection frameworks should prohibit data localization requirements, which can frustrate efforts to implement security measures, impede business innovation, and limit services available to consumers.