Insight

Impact of Data Localization Requirements on Commerce and Innovation

JENNIFER HUDDLESTON, JACQUELINE VARAS | JUNE 16, 2020

Executive Summary:

- Data localization laws – regulations that require data collected on a country's citizen to be retained and/or processed in that country – can create barriers impacting both innovation and online commerce.
- The United States has sought to ban these requirements in trade agreements to limit their detrimental impact on digital trade.
- Data localization requirements could splinter the current global internet into many more regional systems and deter innovation in a wide variety of data-utilizing sectors.

Introduction

The online sale of goods and services is increasingly important to commerce, both in the United States and globally. In 2019, U.S. online sales amounted to nearly $150 billion, 11 percent of total retail sales. Adjusted for inflation, e-commerce has grown by over 1,000 percent since 2000.[i] Similarly, 12 percent of global goods trade is conducted online. During the COVID-19 pandemic, more businesses are relying on such online commerce due to social distancing restrictions.

The United States is a leader in e-commerce, housing some of the most globally competitive suppliers of digital goods and services. For instance, four U.S. companies – Amazon, Microsoft, Google, and IBM – are the top providers of cloud computing services in the world. Beyond the global reach of these large companies, many smaller innovative service providers and local, small businesses are able to leverage an online presence to provide services around the globe. But even while businesses and consumers have become more reliant on e-commerce and the global network undergirding it, that could create barriers for companies seeking to compete in the global marketplace.

This paper discusses the current data localization laws, the impacts of data localization on commerce, and the impacts of data localization on innovation.

Current Data Localization Laws

Data localization laws are laws that require data related to the country's citizens to be processed and/or retained in that country. The data covered by these laws can range from all personal data to only specific types of data such as health or financial information. These laws can impact not only online service, but also more traditional sectors of the economy such as banking.

States with tight control and censorship or governments that do not value free expression may also have data

localization laws. For example, China has data localization requirements that affect all personal, business, and financial data. Russia has data localization requirements for all personal data, and Kazakhstan requires all data for servers on the country's specific domain (.kz) be local. Furthermore, India's data localization requirements apply to payment service providers and government procurement.

There may be more benign intentions behind some data localization laws that can be observed in other country's requirements. For example, Australia requires health records to be stored locally, and Canada requires public service providers to follow data localization requirements. More recently, European countries have sought localization requirements in an effort to exert more control over privacy, content, and data standards. While these requirements may be well-intentioned, they can still have detrimental unintended consequences in the global marketplace and may limit the options available to a country's citizens.

Data Localization in Trade Agreements

Globally, half of all services trade depends on access to cross-border data flows. Recognizing the benefits of the digital marketplace, the United States has typically sought to ban data localization requirements in modern trade agreements.

The first example is the United States-Mexico-Canada Agreement (USMCA). USMCA is the new, renegotiated North American Free Trade Agreement (NAFTA), a 25-year-old pact signed just as the internet was gaining popularity. USMCA, while not perfect, makes several important updates to NAFTA including an entire chapter on digital trade. This chapter prohibits tariffs on digital goods, discrimination against foreign suppliers of digital goods and services, and data localization laws. According to the U.S. International Trade Commission (ITC), "protection from localization laws is essential for U.S. carriers seeking to manage data processing and network management functions from a centralized location." In estimating USMCA's economic impact on the United States, ITC notes that "USMCA's Digital Trade chapter, along with provisions related to investment and e-commerce, contribute significantly to the model's estimated 0.17 percent increase in U.S. services sector output and 1.2 percent increase in services exports to the world."

While USMCA was the first U.S. trade agreement to incorporate a data localization ban, it was not the first-ever trade agreement. In fact, the data localization ban in the USMCA was taken from the text of the Trans Pacific Partnership (TPP), a trade agreement originally including the United States and 11 nations in the Asia-Pacific that later became the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) after the United States withdrew from the agreement. Both the original TPP and the new CPTPP included the same language banning data localization that was later incorporated into USMCA: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

Since then, the Trump Administration has tried to incorporate similar language in each of its new bilateral trade agreements. For instance, the same language was included in the U.S.-Japan trade deal negotiated in September 2019. Furthermore, it is a U.S. objective that data localization bans be included in both the U.S.-EU and U.S.-Kenya trade deals currently in negotiations.

Due to local privacy laws, not all countries have been willing to incorporate data localization bans into their trade agreements with the United States. For instance, the Trump Administration's update to the U.S.-Korea trade deal, signed in September 2018, included weaker language pledging to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." Similarly, the European

Union refuses to include data localization bans in its trade agreements. The EU's support for data localization was one of the primary reasons why negotiations of the Transatlantic Trade and Investment Partnership (TTIP) failed under President Obama and has similarly complicated the Trump Administration's negotiations with the EU.

Impact of Data Localization Requirements on Innovation

Data localization not only impacts the current flow of commerce, it also risks deterring innovation and preventing the technological benefits of the unimpeded flow of data. Such requirements can splinter the internet and flow of data by placing barriers that limit consumer choices, place burdens on new entrants, and forego the benefits of a free and open internet. These can be particularly pronounced in specific industries such as the financial sector.

As more data move to cloud-based computing and emerging technologies lead to an increasing number of connected devices and data, data localization could risk splintering the internet from a single global system to a series of more limited regional systems due to data governance requirements. When authoritarian regimes impose such requirements, it limits the freedom of expression and knowledge sharing that is encouraged by a global internet. For example, China has significant localization requirements that result in tight state control and limit the access to information experienced by others online. The growing number of data localization in countries such as China, Vietnam, and Russia requirements may limit the free expression and consumer benefits associated with the digital age. This can happen when data requirements render the data far more accessible to an authoritarian regime. For example, Facebook creator and CEO Mark Zuckerberg warned that in an authoritarian regime with data localization requirements, governments could more easily increase surveillance capabilities and disrupt dissent and activism. Faced with these choices, increasing data localization laws would result in an increasing number of smaller and more tightly controlled networks that could be more easily subjected to authoritarian controls and silence unpopular or dissenting information as well as prevent the spread of commerce.

In other cases, these policies are enacted for protectionist reasons under the justification of providing local control over data privacy or supporting domestic industry. But such data localization laws will lead companies to limit the markets they offer their products in or engage in costly compliance that does not provide additional consumer benefits. Such behavior results in "data islands" that isolate data rather than easy global data flows for low-risk types of data when concerns would be better addressed through nuanced solutions. The European approach, including General Data Protection Regulation (GDPR) and localization requirements, creates additional barriers for American tech companies as well as for the growing number of non-tech companies that utilize data. The result are protectionist barriers that increase the cost of doing business in a country or region and decrease the benefits of cross-border flows.

Data localization creates barriers that not only affect consumers by limiting benefits of the existing global internet, but also make it harder for innovative products and services to enter or expand to other countries. Requirements for local presence or maintaining local content raise the costs of small and medium-size businesses that may be seeking to enter a new market. For example, a 2015 study by Leviathan Security Group found that data localization requirements raise the cost of hosting data by 30-60 percent. But such concerns impact not only small firms entering a market; they will have a significant impact on existing global players, too. Large, global firms must focus on compliance burdens and differing interpretations of what data are subject to the requirements rather than what they think will best server their consumers. In some cases, localization requirements that burden free expression or target specific types of data .

In some cases, data localization requirements are part of broader conversations around data protection or privacy. For example, discussions around data localization in Europe have been largely tied to concerns about potential espionage concerns following the Edward Snowden revelations and a desire to dictate data privacy and controls following GDPR. But the burdens associated with data localization requirements may not have desired impact on either of these concerns. For example, the costs of maintaining localized data could deter startups from investing more broadly in data security or protection. Additionally, there has not been any evidence that such requirements improve cybersecurity of the data subject to localization requirements or prevent foreign surveillance of the information.

Some laws have sought to target specific industries or types of data rather than broader regulations but can have similar disruptive effects. For example, India's data localization specifically targets payment processors. While this seemingly narrower law might not have the same overall disruptive effect on the internet as broader data localization requirements, it can still deter innovative solutions in an important field and effect the overall economics of e-commerce. FinTech and other payment industry solutions rely on data and often can involve cross-border transactions, making them subject potentially to multiple localization requirements. Targeting a specific industry could deter investment in innovative solutions to problems such as underbanking. Similar issues could arise in well-intentioned targeting of health data or other information that might be considered particularly risky or personal.

Beyond their impact directly on e-commerce, data localization requirements can have a larger impact by deterring beneficial innovation or market entry. They can also risk undermining many of the network benefits of global connectedness brought about by the internet.

Conclusion

Data localization laws place burdens on both trade and innovation. The economic costs of these burdens do not only fall on large players, but also on numerous small and medium-size firms that have benefited from the availability of global commerce and the internet. Even when considering more sensitive data such as financial or health information, such policies could limit innovative solutions, deter competition, and have unintended consequences on broader commerce.

[i] E-Commerce Retail Sales were adjusted for inflation using the Consumer Price Index.