A U.S. Perspective on Foreign Data Protection Policies: Impacts on Economic Competitiveness and National Security

Eric Lundell
President and CEO, ITTA, Inc.

Bobby Shields
Manager, S&T Policy, ITTA, Inc.

**Please note that the views expressed in this presentation are our own, and do not necessarily represent the opinion of International Technology and Trade Associates, Inc (ITTA)*
Mr. Lundell serves as the President and CEO of ITTA, which provides advisory services in a range of policy, regulatory and business development areas. Mr. Shields leads ITTA's science and technology business practice.

The U.S. federal government has not developed a unified data protection law or regulatory system. Rather, the United States relies upon a "patchwork" of state laws and sector-specific federal laws to protect U.S. citizens' data and information. However, recent incidents of major data breaches (such as the Marriot hack) have prompted members of the U.S. Congress to begin considering efforts on comprehensive data protection legislation.

As members of Congress discuss and debate possible data protection legislation, the United States' peers and competitors are advancing their own national data protection policies. The intents and purposes of these laws and regulation are manifold: to protect consumer privacy; to enhance government surveillance powers; to increase competitiveness of domestic businesses; and so on.

This article reviews U.S. perspectives on the impact of foreign data protection policies on U.S. economic and national security interests. We examine three cases: the EU's General Data Protection Regulations (GDPR); China's Cybersecurity Laws; and India's data localization policies.

Each case presents regulatory challenges to U.S. business interests that could, in turn, undermine U.S. global economic competitiveness. Many in the U.S policy community argue that a weakened economy undermines the U.S. defense industrial base, U.S. military strength, and thus, U.S. national security. Moreover, foreign data protection regulations may also curtail the development of cutting-edge technologies vital to U.S. national security and weaken cyber threat information sharing practices.

1. China's Cybersecurity Law

1.1 Background on China's Cybersecurity Law

In an effort to improve cybersecurity and better control data transfers, the People's Republic of China adopted the Cybersecurity Law in November 2016. Since adopting the measure, the Chinese government has begun to implement various provisions of law.

Overall, the Chinese Cybersecurity Law is a comprehensive set of provisions governing the use of information and communication technology (ICT) in China. The law outlines Chinese policies on issues such as personal information protection, data management, and cross-border data transfers.

The three key provisions of the Cybersecurity Law salient to this article are: cybersecurity inspections of businesses in China; protections for "critical information infrastructure;" and data localization requirements.

First, on November 1, 2018, the Chinese government began to enforce a cybersecurity provision that empowers China's Public Security Bureaus (PSBs) to conduct inspections of companies that use or provide internet services in China. Under this measure, PSBs are given broad authority to physically or remotely access and inspect company networks that may impact national security or public safety.

Second, the Cybersecurity Law imposes new requirements on entities that operate so-called "critical information infrastructure" (CII). Notably, the Chinese government has not yet provided a clear definition of CII. As detailed in an August 2018 Brief [1] by the Center for Strategic and International Studies (CSIS), operators of CII must use network products and services that have undergone a national security review process, store certain data within China's borders, and undergo periodic security assessments. However, the Chinese government has not yet approved implementing regulations for this provision.

Third, the Cybersecurity Law's data localization provision requires that CII and other data deemed "important" or "personal" can only be transferred outside of China if it successfully passes a security assessment by the Chinese government. Like the CII provision above, the Chinese

[1] "How Chinese Cybersecurity Standards Impact Doing Business in China", CSIS BRIEFS, 2018

government has not yet approved implementing regulations for this data localization requirement.

1.2 Impact on the U.S. Economy and National Security

China's Cybersecurity Law presents a significant challenge to U.S. companies currently operating within China's borders as well as U.S. companies looking to expand operations into China.

To begin, the law's vague language in its inspection provision gives PSBs authorities broad discretion when inspecting corporate networks and data. For example, although there are no clear definitions for terms such as CII and "important" or "personal" data, Chinese government entities may use a broad interpretation of these definitions when determining whether it has authority to access and inspect a U.S. company's network or data. If interpreted liberally, China's Cybersecurity Law could extend to virtually any U.S. company operating in China.

Many business representatives and policy experts have warned that Chinese government officials could use the guise of "national security" or "public safety" to inspect a U.S. corporation's sensitive data. Given the widespread allegations of Chinese government's theft of foreign trade secrets and intellectual property to benefit its own domestic industry, U.S. industry has justifiably raised alarms at the prospect of allowing Chinese government officials expansive access to their networks and data.

Moreover, the law's data localization regulations could undermine U.S. trade-in-services with China. A September 25, 2017 statement[2] by the U.S. delegation to the World Trade Organization outlined the potential negative consequences of China's data localization efforts:

> *The result would be to discourage cross-border data transfers and to promote domestic processing and storage. The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates. Companies located outside of China supplying services on a cross-border basis would be severely affected, as they must depend on access to data from their customers in China.*

[2] "COMMUNICATION FROM THE UNITED STATES, MEASURES ADOPTED AND UNDER DEVELOPMENT BY CHINA RELATING TO ITS CYBERSECURITY LAW", WTO, 2017

Furthermore, once fully implemented, China's Cybersecurity Law could be "weaponized" to meet Beijing's broader geopolitical goals. For example, the Chinese government could potentially use PSBs cybersecurity inspections as a retaliatory measure against the U.S. in the context of the ongoing trade war. Indeed, Chinese officials could conduct overly burdensome reviews and inspections to slow down U.S. business operations in lieu of the imposition of additional tariffs on U.S. products.

China's Cybersecurity Law also presents national security concerns for the United States. The U.S. policy community (and especially the Trump Administration) has increasingly advanced the conviction that U.S. "economic security" is a fundamental component of U.S. national security. The Trump Administration believes that a vibrant economic sector promotes a robust defense industrial base and strong military. Ultimately, a secure and strong economy strengthens the United States' strategic position against China in the escalating great power competition.

The concept is a guiding principle of the Trump Administration's trade and economic policies. Indeed, over the past year, major trade policy decisions of the Trump Administration (to include Section 232 tariffs on steel and aluminum and Section 301 tariffs on Chinese products) were predicated on this concept of "economic security is national security."

If China's Cybersecurity Law begins to yield major negative impacts on U.S. businesses, the Trump Administration will not only see this as an affront to its economic interests — but also as a threat to its national security apparatus.

2. The EU's GDPR

2.1 Background on the GDPR

The European Union previously relied upon a patchwork of data privacy laws across EU member states, much like the United States' current data privacy regulatory framework. Seeking a unified regulatory approach, the EU adopted the General Data Protection Regulation (GDPR) in April 2016, which later went into effect in May 2018.

The GDPR is often considered the most comprehensive piece of data protection legislation in the world. In general, GDPR places the responsibility of data protection on organizations that process personal information of EU citizens. It establishes the principle of "privacy by design

and by default" for organizations that control or process such data. It also requires organizations to maintain a data protection officer to ensure the privacy of EU citizen data. The GDPR lays out strict financial penalties for organizations that do not meet its privacy standards. The maximum fine under the GDPR is 4 percent of an organization's annual turnover or 20 million Euros (whichever figure is greater).

GDPR's data privacy requirements apply to *any* organization — to include any organization outside the EU's border — that offers goods and services to individuals in the EU or that monitors their behavior. As such, the GDPR has a global reach.

Each nation within the EU is required to create an independent public Data Protection Authority (DPA) to enforce the GDPR. However, the DPAs cannot formally enforce the GDPR outside of its borders. As such, the EU must rely upon agreements with foreign courts and other relevant bodies to effectively enforce the GDPR outside of the EU.

2.2 Impact on the U.S. Economy and National Security

The GDPR places considerable regulatory burdens on U.S. companies. Any U.S. organization that controls or processes EU citizens' data is subject to DPA enforcement. Fines of up to 4 percent of an organization's annual turnover or 20 million Euros pose a significant financial risk to U.S. companies. Costs of complying with GDPR regulations—and the potential inefficiencies resulting from such compliance—can also hurt U.S. companies.

However, there are still many "unknowns" regarding how GDPR enforcement will manifest in the coming years. For instance, it remains unclear how DPAs will interact with counterparts in the United States to penalize non-complaint U.S. companies. Furthermore, the cost of GDPR compliance for U.S. companies relative to foreign counterparts is unclear. In turn, we do not yet know how the GDPR might affect the competitiveness of U.S. companies compared to foreign counterparts.

One potentially significant technological consequence of GDPR is that it will limit the amount of global data available to U.S. organizations, which will, in turn, complicate the development of artificial intelligence (AI) algorithms. AI systems require large amounts of data to process in order to mature their algorithms. As such, data limitations resulting from GDPR enforcement could ultimately impede AI development. And while this concern applies to data protection regulations across the globe, the GDPR represents the most significant risk to U.S. AI developers, given the large amount of data shared between U.S. and EU entities.

As the global leader in AI technology, the United States would suffer the greatest opportunity cost from a decrease in available data. A slowdown in AI development would jeopardize the rapid growth of AI in U.S. industry. Consequently, the U.S. national security community, which relies heavily upon industry to develop and operationalize cutting-edge AI capabilities, would assuredly be concerned about the impact on AI-related national security efforts.

However, some experts have countered these concerns, noting that the GDPR may ultimately facilitate AI development. For example, in a June 2018 *TechCrunch* article[3], Ivy Nguyen of Zetta Venture Partners argues that the GDPR will require companies to better organize and manage their data. These data management processes will help organizations better understand their data and, in turn, more effectively develop and deploy AI systems. Moreover, GDPR also requires all EU citizen data to be portable (i.e., available for download by a user), meaning that more data will be digitized and thus accessible for AI development and application.

At this point, only time will tell exactly how the GDPR will impact AI development in the United States.

Lastly, the GDPR may undermine cyber threat information gathering and sharing between U.S. threat analysts. In short, GDPR forbids the publication of information that identifies EU individuals. GDPR thus bans publication on so-called WHOIS databases, which provide information on registered owners and operators of domain names and IP addresses. According to security experts, including Chris O'Brien from EclecticIQ[4], these databases have traditionally help inform threat analysts in their research for cybersecurity threats. With these databases, cyber threat gathering and information sharing in the United States may become less effective.

3. India's Data Protection Policies

3.1 Background on India's Data Protection Policies

The Indian government has begun pursuing stricter data

[3] https://techcrunch.com/2018/06/07/gdpr-panic-may-spur-data-and-ai-innovation/

[4] https://www.informationsecuritybuzz.com/articles/gdprs-impact-on-threat/

protection policies over the past several months, with a focus on data localization.

In April 2018, the Reserve Bank of India (RBI) established a requirement for all global payment firms to store transaction data of Indian customers within its borders. This data localization requirement went into effect on October 15, 2018.

Despite protests over the regulatory burdens of RBI's data localization requirement, major U.S. payment firms such as Visa and MasterCard confirmed in October that they had begun complying with this new rule. According to news reports[5], however, these companies remain in discussions with RBI to try to relax data storage requirements on certain, older financial transactions.

In addition to the RBI requirement, the Indian parliament will soon consider a comprehensive data protection bill. The proposed legislation, called the Personal Data Protection Bill, was drafted by the Indian Ministry of Electronics and Information Technology (MEITY) and is now undergoing reviews within the Indian bureaucracy. The Indian parliament is expected to introduce the bill around June 2019.

Although it is still under review and subject to change, the current version of the bill places restrictions on cross-border data transfers. It requires that every "fiduciary" (meaning any processor or controller) of personal data of an Indian citizen must have at least one copy of the personal data stored in India. More sensitive personal data must be processed in India. The bill also prescribes several conditions for the transfer of non-sensitive personal data outside of India.

3.2 Impact on the U.S. Economy and National Security

U.S. companies and many members of the U.S. Congress have characterized India's data localization policies as a form of protectionism that hurts U.S. business. For example, Nigel Cory of the Information Technology and Innovation Foundation has argued[6] that data localization policies place regulatory burdens on businesses by forcing them to use or establish local services. This duplicative cost makes "these firms and their services less competitive compared to local firms, which may only use domestic data services." Many in the U.S. Congress are concerned about these developments. For instance, U.S. Senators John Cornyn (R-Texas) and Mark Warner (D-Virginia) said in an October 2018 letter to Indian Prime Minister Narendra Modi that data localization disrupts bilateral digital trade and, in turn, threatens the U.S.-India economic partnership.

Indeed, given India's massive potential as an export market with its 1.3 billion population, many view restrictions on digital trade with India represents as a significant opportunity cost for U.S. businesses.

India's burgeoning economy is not alone in its growing preference for data localization and limitations on cross-border transfers. Others, such as Indonesia and Vietnam, have similar policies. Growing trend of data localization policies across emerging, high-potential economies represents a major threat to the U.S. digital services economy—and the broader U.S. economy.

And, as discussed earlier, the Trump Administration believes that a weakened economy also impacts the defense industrial base and U.S. military posture.

4. Conclusion

As the U.S. Congress debates its own data protection legislation over the next several months or years, global partners and competitors are taking actions to protect and control their data. Taken together, this global web of data protection laws and regulations can severely impact the U.S. business community and undermine efforts to advance key technologies of economic and national security importance such as AI.

Data protection can also be viewed in the context of the emerging great power competition between the United States and China. Many in the United States view China's Cybersecurity Law as part of a broader effort to promote its domestic industry at the expense of U.S. economic and security interests. Predatory actions against U.S. companies resulting from the Cybersecurity Law could put the United States at an economic and security disadvantage against its rising competitor.

In light of these challenges, U.S. policymakers will likely push for pro-business data policies to promote digital trade and services and fight against "digital protectionism." These efforts require balance between legitimate demands for personal privacy and promotion of digital innovation that contributes to U.S. prosperity and security.

[5] https://www.livemint.com/Industry/Wmq7Sr5YtNBPcet8aGBRQP/Visa-Mastercard-begin-storing-India-payments-data-locally.html

[6] https://www.livemint.com/Opinion/bHelcN7RR5rQ5r3hPxXGRP/Opinion--The-RBIs-misguided-digital-protectionism.html