Business Roundtable℠
More Than Leaders. Leadership.

Testimony of Denise E. Zheng
Vice President, Policy, Business Roundtable

Before the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Communications, Technology, Innovation, and the Internet

On *"The Internet and Digital Communications: Examining the Impact of Global Internet Governance"*

July 31, 2018

Chairman Wicker, Ranking Member Schatz, Members of the Subcommittee, thank you for the opportunity to testify on behalf of Business Roundtable regarding international policies related to the internet and digital platforms – more broadly referred to as "information and communications technology" (ICT) – and their impact on competitiveness, investment, and innovation.

Business Roundtable is an association of chief executive officers (CEOs) of the world's largest multinational companies. Collectively, our member companies employ more than 16 million people across all sectors of the economy. It is a commonly held misperception that ICT policies only affect the technology industry. The reality is that few companies can compete and succeed today without making extensive and effective use of data and digital platforms.

Recently there has been a rapid increase in the number of complex, conflicting, and uncoordinated ICT public policies from governments around the world. This trend undermines global digital innovation and trade by creating policy and regulatory fragmentation, business uncertainty, overwhelming compliance costs, and other unintended consequences.

Trends in Global ICT Policy

Governments have a responsibility to develop ICT policies that provide for national security, protect public safety, and ensure individual privacy. But too often, countries are defining security, privacy, and safety in an overly broad manner, resulting in a wide array of laws and regulations that erect barriers to an interoperable and open global internet. In some cases, nations impose ICT policies for the stated purpose of cybersecurity and privacy, even though the policies are designed primarily to keep U.S. companies out and protect local industries. In other cases, the global patchwork of various cybersecurity and privacy requirements creates a compliance nightmare that is cumbersome and costly for large companies and impossible for small companies and startups.

The European Union (EU) and China are currently the most active players in developing and implementing ICT policies. But India, Russia, South Korea, and other Asian and Latin American countries are ramping up efforts to develop and enforce a wide range of cybersecurity, privacy, and data localization policies. Already at least 34 different countries have data localization requirements, while approximately 120 countries have data privacy laws and many more countries are considering legislation in this area.[1]

The following sections highlight a selection of ICT policies that have a significant impact on Business Roundtable members and other U.S.-based companies.

Data Localization

China has the most aggressive data localization laws. China's Cybersecurity Law that went into effect in June 2017 requires all "important information" and "personal information" to be stored in China. Under this regime, "network operators" are prohibited from transferring covered data outside of China without undergoing a government-mandated security assessment. As currently defined, the law could cover any entity that owns or operates a computer network and applies to a vast and ambiguous assortment of different types of data. China is not the only country with data localization requirements: India, Russia, Nigeria, and South Korea all have enacted laws that prohibit the transfer of a range of business and consumer data outside of their respective jurisdictions. In some cases, these laws mandate physical servers be installed in-country as a condition of doing business.

This growing number of localization requirements is already proving costly for many industry sectors, including health, retail, finance, insurance, energy, manufacturing, and technology. These mandates are making it increasingly difficult for U.S. companies to do business in key markets such as Asia and Latin America.

Cybersecurity

Cybersecurity regulations are expanding globally. For example, China, which has some of the most heavy-handed regulations, requires companies in industries deemed to be "critical" to demonstrate that their technology systems are "secure and controllable." Such companies must undergo inspections and assessments of company networks and are mandated to disclose computer program source code to the Chinese government for review. The European Council recently proposed a new cybersecurity regulation (the EU Cybersecurity Act) that would create a security certification regime for ICT products and services. If the law takes a mandatory, rather than voluntary, approach, it could have the effect of dictating how American firms design, develop, manufacture, and deliver ICT products and services.

[1] Pfeifle, S. (2017, September) *Is the GDPR a data localization law?* Retrieved from https://iapp.org/news/a/is-the-gdpr-a-data-localization-law/

The financial services sector, in particular, faces an expanding number of international cybersecurity regulations, with more than 40 different international cybersecurity policies already in place,[2] ranging from risk assessments to penetration testing to incident reporting. In this environment, companies must reconcile competing and redundant cybersecurity regulations that divert significant resources from truly effective cybersecurity measures toward time-consuming compliance activity, such as certifications and questionnaires.

Privacy

In May 2018, the EU's General Data Protection Regulation (GDPR) went into effect and established the most expansive privacy regime in the world. The GDPR covers nearly all types of personal data and affects business-to-consumer as well as business-to-business firms. The GDPR has an extraterritorial application meaning that its scope covers any company, regardless of whether it is based in the EU or not, that meets the law's threshold requirements for processing personal data of individuals in the EU.

This means that some companies, such as those that cannot justify spending the resources necessary to demonstrate compliance with the GDPR, are forced to take steps to block EU-based users from using their products and services, including from visiting their websites, to avoid facing steep fines of up to 20 million euros or 4 percent of annual revenue, whichever is higher. The GDPR limits transfers of personal data outside of the EU unless certain adequacy standards are met; it also requires companies to notify EU and national regulators of security breaches of personal data within 72 hours of the incident.

The EU is actively promoting the adoption of the GDPR as a model for privacy regulations in other countries. In addition, Brazil and other Latin American countries are proposing or have enacted laws that adopt many aspects of the GDPR.

The risk of domestic regulatory fragmentation within the United States for privacy is also high. In addition to several existing sector-specific federal and state privacy regulations, California recently passed a consumer privacy bill that applies broadly across many sectors. Numerous other data privacy legislative proposals are pending in state legislatures that, if passed, would further increase the complexity of privacy regulations across the United States. That is why Business Roundtable is working to develop privacy principles that strengthens protections for consumers but also preserves innovation in the digital economy.

Government Access to Data

The growth of digital communications over the past two decades has created new challenges as well as opportunities for law enforcement. For instance, several countries have sought to

[2] World Bank Group, Financial Sector Advisory Center (2017, October) *Financial Sector's Cybersecurity: A Regulatory Digest.* Retrieved from http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf

restrict the use of encryption or imposed data localization mandates to facilitate law enforcement's access to data for investigative purposes or government surveillance.

Both China and Russia mandate companies decrypt and localize data for law enforcement and surveillance. In 2016, Russia passed a law that explicitly required internet service providers to provide backdoor access to encrypted data and store all consumer communications for six months. France, the United Kingdom, Brazil, India, and other countries have also enacted laws that regulate the use of encryption in digital communications.

Not only do these laws erode security and privacy on the internet, they also have a significant impact on the interoperability of digital platforms across borders and undermine consumer trust in technology.

Consequences of Uncoordinated International ICT Policies

The current state of global ICT policy is complex, chaotic, and fragmented and could undermine growth and innovation in the digital economy and emerging technologies.

Fragmentation and Legal Uncertainty

As CEOs that run the largest American companies, Business Roundtable members operate in many jurisdictions and serve customers around the globe. The international regulatory environment for ICT policy is forcing companies across all sectors to reconcile overlapping, duplicative, and sometimes conflicting requirements. The legal uncertainty that results from policy and regulatory fragmentation undermines investment, growth, and job creation. Ambiguous requirements and inconsistent enforcement in some countries increases the risk of doing business and can lead companies to reject, defer, or reconsider investments.

Compliance Costs

The GDPR alone is estimated to cost Fortune 500 companies a combined $7.8 billion to comply, or about $16 million per firm.[3] Another survey found that large organizations of 25,000 or more employees each are budgeting an average of $30 million to comply with the GDPR. Much of the cost is related to "check the box" exercises that demand significant investment from companies regardless of their risk profile. Some companies have decided to discontinue offering products and services in the EU because compliance costs are so high that they can no longer justify being in the market. It is not unusual for those surfing the web in the EU to come across websites from vendors that have nothing more than a note saying that due to GDPR requirements, the site cannot be accessed.

[3] IAPP-EY (2017) *IAPP-EY Annual Privacy Governance Report 2017*. Retrieved from https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/

Data localization requirements can impose significant compliance burdens that raise the cost of hosting data by 30 to 60 percent for companies that are covered by such requirements.[4] A study done by the European Centre for International Political Economy estimates that enacted or proposed data localization mandates in China could cost up to 1.1 percent of its GDP and the cost of data localization requirements in the EU could cost nearly 0.4 percent of its GDP.[5]

Unintended Consequences

A fragmented international ICT policy landscape will likely have the most significant and adverse impact on startups and small- and medium-size companies with limited resources to navigate ambiguous requirements and opaque reviews in countries like China or excessive paperwork associated with complying with EU policies. These compliance costs will make it more difficult for such promising and innovative companies to thrive and expand.

Emerging technologies such as artificial intelligence and blockchain are also hindered by regulatory uncertainty and are the next likely targets for policy and regulatory fragmentation. The data minimization, automated decision-making, and "right to erasure" provisions of the GDPR can create barriers to the commercial development of important emerging technologies which improve and innovate new products and services for consumers. I will give you two specific examples of this: First, the GDPR imposes restrictions at every stage that a company collects, processes, uses, and retains personal data, and the impact of these restrictions on the development of machine learning tools is uncertain. Some companies may decline to integrate machine learning into their business to avoid such hurdles. Second, companies using blockchain and distributed ledger systems, technologies rooted in the notion that information should not be unilaterally amended or deleted from networks, will face difficulty in responding to data subject requests, authorized by the GDPR, to amend and delete their own data.

Recommendations

Congress has an important role in creating and fostering a global policy environment for an open, interoperable, and global internet and to promote the continued economic growth of the digital economy. To that end, Business Roundtable recommends the following actions:

- **Establish Alliances with Like-Minded Countries to Counter Protectionist ICT Policies.** The U.S. government should build alliances with like-minded countries to counter technology restrictions, protectionist cybersecurity and data localization requirements, and requirements for businesses to transfer technology and intellectual property as a condition to accessing foreign markets.

---

[4] Leviathan Security Group (2015). *Quantifying the Cost of Forced Localization. Retrieved from* https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

[5] European Centre for International Political Economy (2016 March). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States* Retrieved from http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

- **Lead in Development of International Norms, Best Practices, and Standards for ICT.** The U.S. government and U.S. companies should lead in developing norms, best practices, and standards for the internet and digital platforms. Areas of focus include cybersecurity, privacy, and cross-border data flows. At the same time, emerging technologies such as artificial intelligence, autonomous vehicles, blockchain, internet of things, and robotics require serious attention, because rules do not yet exist.

- **Seek to Align or Harmonize Requirements to Avoid Global Fragmentation.** In the face of an already fragmented environment, the U.S. government should play a leadership role to align or harmonize where possible existing ICT policies, regulations, and standards globally, and maintain that same approach for emerging technologies to avoid costly fragmentation. The United States cannot afford to be missing from important international forums on ICT issues, as China and other countries are actively seeking to rewrite the rules of the internet and digital economy that are fundamentally at odds with open markets and democratic values.

- **Protect Transatlantic Cross-Border Flows.** Congress should act to protect the EU-U.S. Privacy Shield by making the Privacy Shield Ombudsperson a permanent position of the U.S. Department of State. It should also act swiftly to confirm the nominees for the Privacy and Civil Liberties Oversight Board, which plays a critical role in fulfilling the requirements of the EU-U.S. Privacy Shield.

Mr. Chairman, Ranking Member Schatz and Members of the Subcommittee, thank you for the opportunity to present Business Roundtable's views on information and communications technology and their impact on competitiveness, investment, and innovation. The global policy environment around ICT represents a serious concern to leaders of these American companies that drive economic growth and job creation in the United States and across the world.