G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Technology and Innovation

2017 | No.39

DEAR WORLD LEADERS: TEAR DOWN YOUR DIGITAL WALLS

JOSH KALLMER

DEAR WORLD LEADERS: TEAR DOWN YOUR DIGITAL WALLS

2017 | No.39

JOSH KALLMER

SUMMARY:

The modern economy depends implicitly on the movement of digital information across borders. While the data traversing our search engines, social media platforms, and e-commerce sites is what captures the imagination, cross-border data flows arguably have their greatest impacts outside of the technology sector, in business-to-business contexts. It is not surprising that, as companies have internationalized, and innovation has accelerated, governments in every part of the world have struggled to respond. While it is appropriate for governments to rely on national regulatory tools to address these policy considerations, they too frequently do so in a manner that neglects the benefits of global coordination. In this environment of tectonic political change, the world's leading governments have the opportunity to both advance these important public interests and to secure the benefits of a data-driven global economy. To do so, however, they must pursue their national priorities mindful of the global character of the challenges. This means seeking international compatibility of national regulatory approaches, using international organizations to find policy recipes that coexist with national law, and negotiating new international rules to advance shared interests. Only a shared commitment to global coordination, mindful of course of national conditions, will ensure success in driving economic growth and protecting public interests.

About the Author

Josh Kallmer is senior vice president for Global Policy at ITI, a technology industry association representing 60 of the world's leading innovation companies.

Photo Credit: holbox / Shutterstock.com

National borders have it rough. Since before the 1648 Peace of Westphalia established the nation-state as the basic unit of the international order, the forces of commerce and conflict have continuously challenged the meaning and viability of national borders. On many occasions, most notably after World War II, governments themselves have worked to reduce the significance of borders, in many ways to the benefit of humankind. They constructed a tapestry of trade rules to spur business and raise living standards, built financial institutions to stabilize markets and drive development, and established regional organizations to enhance market opportunities and political leverage. Having weathered these convulsions in both wartime and peacetime, national borders now face the qualitatively new challenge of cross-border data flows.

We are, of course, in a moment of ascendancy for national borders. The election of Donald Trump as U.S. President, the United Kingdom's decision to leave the European Union, and the increasing influence of nationalist parties and populist movements in Europe and around the world reflect renewed fidelity to the nation-state. Yet, these sentiments only amplify the challenge that data poses to national borders. For as much as national leaders and public officials may wish to manage economic activity, even to confine it within their territories, the nature of data is such as to render that impracticable, if not impossible. There is, therefore, a heightened responsibility for policymakers to use their national regulatory tools in ways that reflect the essentially international nature of information and commerce.

> *"There is a heightened responsibility for policymakers to use their national regulatory tools in ways that reflect the essentially international nature of information and commerce."*

A Global Economic Environment Powered by Data

The modern economy depends implicitly on the movement of digital information across borders. While the data traversing our search engines, social media platforms, and e-commerce sites is what captures the imagination, cross-border data flows arguably have their greatest impacts outside of the technology sector, in business-to-business contexts. In 2015, the global value of cross-border data flows surpassed the value of trade in goods for the first time in history.[1] Some experts project that, by 2025, half of global economic output will be created digitally.[2]

The ubiquity of cross-border data flows is the product of two distinct, but mutually reinforcing, economic trends. The first trend deals with qualitative changes in how firms organize themselves. While companies have for centuries traded goods and services, and made investments across borders, only recently have they themselves become global as well. Over the past generation, many firms have created geographically distributed business networks to optimize how they develop, design, produce, market, and deliver goods and services around the world. A manufacturer of consumer appliances, for example, may conduct research and development in Switzerland and Japan; design its products in the Netherlands and the United States; source inputs from Korea and China and incorporate them into manufacturing operations in Taiwan; and distribute finished products through regional hubs in Singapore, Turkey, and Brazil.

The second trend involves the breathtaking innovation in information and communications technology (ICT) that has occurred over the past quarter century. Advances in semiconductor technology have enabled computers and other devices to operate at speeds and levels of sophistication unthinkable just a few years ago. Investments in undersea cables and terrestrial networks have allowed more data to flow more quickly to more places, contributing to an 18-fold increase of international data traffic between

1 See James Manyika et al, "Digital Globalization: The New Era of Global Flows," McKinsey Global Institute, March 2016.

2 Robert D. Atkinson, "International Data Flows: Promoting Digital Trade in the 21st Century," Testimony before the House Judiciary Committee Subcommittee on Courts, Intellectual Property, and the Internet, November 3, 2015.

2005 and 2012.[3] Cloud computing has permitted organizations to store and manage information in a substantially more cost-effective and secure manner. Rapidly improving sensor technology has enabled an ever-greater number of consumer devices and industrial machines to connect both to one another and to the Internet, with estimates of more than 20 billion connected devices by 2020.[4] And we are on the precipice of a revolution in artificial intelligence (AI), in which computing systems will continuously teach themselves, for example, how to drive cars more safely, tend to our health more effectively, or detect financial fraud more quickly.

The convergence of these trends has made digital information the indispensable currency of international business in every sector of the economy. GE equips its aircraft engines with sensors that constantly transmit performance information from airplanes around the world to its facilities in Ohio, allowing airlines to anticipate maintenance needs and reduce flight delays. U.K. retailer Tesco analyzes data in real time among its thousands of grocery stores to optimize inventory and manage energy use, allowing it to save money and reduce food spoilage. Australian mining company Rio Tinto continuously analyzes data from its mines around the world, allowing it to improve logistics and more cleanly and safely manage the extraction of ore from various locations. And the Industrial and Commercial Bank of China (ICBC), by some measures the largest company in the world, analyzes vast quantities of customer information in real time, allowing it to improve both customer experiences and fraud detection.[5]

Cross-border data flows have transformed not just how companies do business, but how people live. We rely on the movement of digital information across borders to carry out countless numbers of everyday transactions, whether flying on an airplane, reviewing a bank account balance, using a credit card, shipping packages internationally, or checking the weather. The U.S. Centers for Disease Control and Prevention (CDC) uses massive international data sets to analyze social networks in order to help halt the spread of HIV and other communicable diseases. Online courses and certificate programs, such as those provided by Khan Academy, provide access to education for literally millions of people in underdeveloped and remote parts of the world. The European Space Agency uses sensor-equipped satellites to predict potentially devastating weather events, such as hurricanes and droughts.

The movement of data across borders not only makes our lives easier, it creates real opportunities to solve humanity's biggest challenges.

Governments Struggle to Respond to Data-Driven World

It is not surprising that, as companies have internationalized, and innovation has accelerated, governments in every part of the world have struggled to respond. The core purpose of a government, after all, is to advance certain state interests (e.g., national security, public health, economic growth) on behalf of certain people (e.g., citizens and other residents) within a defined territory. This is true regardless of an economy's level of development and without making a value judgment about the nature or quality of its governance. National governments think in national terms, operate within national borders, and act in furtherance of national priorities.

> *"The relentless evolution of a data-driven global economy has fundamentally altered the relationship between governments and companies."*

The relentless evolution of a data-driven global economy — through the transformation of how companies organize themselves and their instinctive reliance on data — has fundamentally altered the relationship between governments and companies. The importance of a company to an economy no longer depends primarily (if at all) on the location of its headquarters, or the passports of its shareholders,

3 See James Manyika et al, "Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy," McKinsey Global Institute, April 2014.

4 See Gartner, "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," February 7, 2017.

5 See Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," Information Technology and Innovation Foundation, February 2015.

or even the proximity of its business units. What matters instead are the contributions that a company — however it is organized — makes to growth, job creation, innovation, exports, and other public goods in that economy. A "foreign" automotive company in the United States may, for example, construct a manufacturing facility in the United States; hire American auto workers; establish local research and development (R&D) facilities that stimulate U.S. innovation more broadly; and rely on U.S. construction firms, U.S. accountants, and U.S. steel companies for the goods and services upon which much of its operations depend. By the same token, a "U.S." automotive company may invest in production facilities overseas, but in doing so create demand for parts exports from the United States, as well as increased support from U.S.-based employees in the areas of design, marketing, sales, and general company operations.

The movement of digital information has created a similarly new dynamic for governments. When a government restricts the cross-border movement of auto parts or legal services, it may disrupt companies' supply chains, but it does not destroy the value of their underlying assets. When a government restricts the cross-border movement of data, in contrast, it undermines a much broader and deeper set of economic relationships. That is because data is not so much a discrete asset as a diffuse resource, connective tissue among economic actors spread around the world. To realize its value, data needs to constantly move among people or organizations. When governments interrupt the movement of data, the social and economic costs can be immediate, widespread, and severe.

The basic incongruity between the interests and instruments of national governments, on the one hand, and the nature and structure of a data-driven global economy, on the other hand, creates serious challenges for policymaking. The problem is not that governments are seeking to address the public policy issues raised by an increasingly digital world. They are and should be — both citizens and companies have strong interests in protecting privacy, enhancing public safety, preventing anti-competitive behavior, and protecting children from harmful content, among other interests. The problem is that, when it comes to data flows, national policy tools are often ill-equipped to address challenges that are by their nature global. These misalignments exist across policy areas but are most pronounced in the contexts of privacy and data protection, law enforcement and national security, and economic competitiveness and job creation.

Privacy and Data Protection

Nowhere is the tension between international data flows and national regulation more acute than in the area of privacy and data protection. The privacy of one's "personal data" is a core public interest in economies around the world, and few question that it is appropriate for governments to establish ground rules for the treatment of personal information by both companies and the state. Yet, in advancing this legitimate public interest, governments frequently overlook the global character of both data and the companies that rely on it and take approaches that unintentionally undermine their economic interests, without meaningfully increasing privacy protections.

> ***"Under EU data protection law, EU citizen data may only leave Europe where authorities attest to the adequacy of a third country's data protection rules"***

The recent effort of the European Union and the United States to agree on a mechanism for transatlantic data transfers provides the most salient example. The protection of personal data has long been a foundational principle of EU law, understandably in light of many European countries' tragic histories of coercive government surveillance. Data protection is a core element of the EU's Charter of Fundamental Rights, and a 1995 Data Protection Directive provides detailed parameters for the protection of EU citizen data. In May 2018, a General Data Protection Regulation (GDPR) will replace the directive with an even more comprehensive framework for the protection of personal data.

Under EU data protection law, EU citizen data may only leave Europe where authorities attest to the "adequacy" of a third country's data protection rules (or otherwise approve data transfers on the basis of contractual or other mechanisms). In 2000, the EU and the United States established the Safe Harbor Framework, which required companies transferring EU citizen data to the United States to provide certain protections for that data. The Safe Harbor Framework assured the European Commission of the adequacy of U.S. privacy protections, thereby ensuring that the data flows rapidly coming to underpin transatlantic commerce could continue uninterrupted.

> *"The tool the EU uses to achieve its priorities is counterproductive from a global perspective."*

The June 2013 revelations of former National Security Agency (NSA) contractor Edward Snowden indicating that the U.S. government had accessed a wide range of personal information, including EU citizen data, dealt what was ultimately a mortal blow to the Safe Harbor Framework. The EU promptly sought to renegotiate the agreement, seeking heightened obligations on companies' handling of EU citizen data and demanding that the U.S. government constrain the activities of its national security and intelligence authorities.

In October 2015, as EU and U.S. negotiators were closing in on a strengthened pact, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Framework altogether. Facing a short deadline to satisfy the standards set out by the CJEU, negotiators hustled in early 2016 to replace the Safe Harbor Framework with the EU–U.S. Privacy Shield.

The Privacy Shield should be celebrated. By placing heightened but measured obligations on both companies and the U.S. government, it reflects a thoughtful and pragmatic effort to comply with EU law in a manner that permits data flows and supports innovation. It does not, however, resolve the underlying infirmity of transatlantic (much less global) privacy policy, which is that individual economies can effectively impose their own regulatory preferences on the rest of the world. By establishing a standard of adequacy, and then requiring that other countries provide "essentially equivalent" privacy protections in order to satisfy it, the EU takes a unilateral approach to what is, at its heart, a shared challenge. The issue is not whether governments have the right to determine their core privacy and data protection priorities. Of course, they do. The issue is that the tool that the EU uses to achieve its priorities — bilateral adequacy determinations — while irresistible from a domestic perspective, is counterproductive from a global perspective, for several reasons.

First, it would be impossible to administer. Every economy in the world would need to evaluate the data protection laws of every other economy, tying regulators in knots and making business planning prohibitively complex. Second, it would be incredibly costly, especially for developing countries. Because national privacy regimes constantly evolve, countries would need to perpetually monitor the domestic laws of every other country. Third, it would inflict significant and unintended economic damage. To take the transatlantic example, EU and U.S. companies are so deeply integrated into each other's business networks — the value of services delivered digitally across the Atlantic is more than half a trillion dollars — that restricting the flow of data to the United States would potentially hurt EU-based companies as much as, if not more than, U.S.-based companies. That is to say nothing of the significant collateral damage that consumers would experience.

Law Enforcement and National Security

A data-driven global economy creates profound considerations for what is inarguably the most important function of government, which is to keep people safe. In principle, governments have a legitimate interest in accessing digital information where it is necessary to enforce domestic laws or protect public safety and national security. But governments too often seek to do so in a way that disregards the global nature of both business and data. In doing so, they not only chill innovation and investment; they also infringe the interests of other countries and may even harm their own law enforcement and national security interests.

Consider the use of court orders requiring the disclosure of digital information relevant to law enforcement or counterterrorism efforts. Governments may, for example, have an interest in

the information that alleged criminals or terrorists have transmitted through apps created by, or stored in the cloud on the servers of, technology firms. Yet, in an environment in which companies operate in multiple jurisdictions, everyone has mobile devices, and data moves among them seamlessly, effectuating such an order may be anything but straightforward. The French government may have jurisdiction over a suspect, for example, but the data at issue may be stored with a cloud provider that is based in the United States, on a data center located in Chile. Or the French government may have jurisdiction over the cloud provider, but the data may be stored in Chile and concern a Japanese person who has no connection with France. Other fact patterns are similarly vexing.

> *"The increased movement of digital information compounds unresolved problems of international cooperation on law enforcement."*

In such situations, every government has an incentive to interpret its laws in a manner that maximizes its own ability to obtain important information. Yet, this individually rational approach can lead to collectively perverse results. As some countries have adopted measures that would extend their jurisdiction to data located in other countries (even where the suspect has no connection to the first country), some of those other countries have enacted blocking statutes that prohibit companies from making such disclosures. Brazil, for example, has sought the personal information of alleged criminals that is stored on the servers of global technology companies in the United States. Absent the use of legal processes sanctioned by the U.S. government, U.S. electronic privacy laws prohibit the disclosure of information in response to such extraterritorial requests. At the same time, U.S. authorities have sought the personal data of non-U.S. citizens stored abroad on the servers of technology firms over which the United States has jurisdiction. Like U.S. law, the EU's GDPR will prohibit technology companies from complying with such requests in the absence of a valid international agreement for the transfer of such data. Essentially, the increased movement of digital information compounds unresolved problems of international cooperation on law enforcement, which to date mostly relies on mutual legal assistance treaties (MLATs) that often take months to operate. With information moving swiftly and seamlessly in the digitized world, there is a growing belief that structures for international cooperation on law enforcement should be similarly swift and seamless. Furthermore, information relevant to an investigation in question is increasingly likely to be not in someone's desk drawer, but in a "cloud" outside the jurisdiction of the police, and thus cooperation issues are occurring with much greater frequency.

These outcomes are irrational from a global perspective, for several reasons. First, they are legally unsustainable. No set of conflict of laws rules can coherently resolve a situation where the act of complying with the law of one jurisdiction constitutes a violation of the law of another jurisdiction.

They are also economically harmful. As discussed in the following section, an understandable response of many governments to extraterritorial requests is to require that companies store and maintain data within their borders. Yet, "data localization" requirements do nothing to increase the security of information (which is a function of how, rather than where, data is stored), and in fact may undermine data security, and they almost always impede the ability of an economy to grow and innovate.

Finally, as legal stalemates deprive governments of information they need, they actually prevent governments from carrying out their law enforcement or national security missions.

Economic Competitiveness and Job Creation

Some of the greatest anxiety governments have about a digitized global economy concerns its economic impacts. With such rapid change in the nature and pace of innovation, governments are asking valid questions about how they can grow their economies, create jobs, attract investment, and, in many cases, pull people out of poverty and improve the quality of their citizens' lives. Unfortunately, as with their efforts to protect privacy and advance security, in pursuing

their economic policy priorities, governments all too often take measures at the national level that ignore the global nature of the challenges they face.

Many governments erroneously believe that they need to keep data within their borders in order to benefit from an increasingly global, increasingly digital economic environment. China has enacted data localization measures in a range of contexts, including in the areas of banking, insurance, and cloud computing. Indonesia's Information and Electronic Transaction Law requires that any company providing Internet-enabled services locate its data centers domestically. Russia recently amended its Personal Data Law to require that companies store all Russian citizen data in databases physically located in the country. And Vietnam's Decree on Information Technology Services mandates that companies that provide Internet-enabled services maintain at least one server within the country.

Government measures that require the localization (or otherwise restrict the movement) of data for perceived competitiveness and economic development reasons suffer the same basic deficiency as those described above relating to privacy and security. In each case, governments are using national tools to regulate an environment that is fundamentally international. In doing so, they actually work against their own economic policy interests in a variety of ways. By suggesting a need for government protection, they send damaging signals about their ability to innovate in the absence of regulation. They stifle entrepreneurs and small businesses entrepreneurship and prevent domestic companies from learning to compete in the absence of protection. And they deprive their firms and workers of cutting-edge technologies and opportunities to access global business networks.

Indeed, few of the countries that have adopted data localization measures have found that they deliver lasting, structural benefits to their economies. Data centers, for example, are expensive to build but are highly automated and create few permanent jobs. Recent research by the European Centre For International Political Economy (ECIPE) suggests that existing or proposed data localization measures meaningfully reduce gross domestic product (GDP) in several countries, including in Indonesia (by 0.5 percent), China (by 1.1 percent), and Vietnam (by 1.7 percent).[6]

It is natural and appropriate for governments to want the economic environment to serve their efforts to promote growth, job creation, and other interests. But localizing economic activity that requires a global context in which to operate is counterproductive.

Optimizing National Policies to Meet Global Challenges

As discussed above and evidenced around the world, national legislative or regulatory tools are frequently ill-equipped to address the public policy issues raised by a data-driven global economy. The solution, however, is not to replace national rules with global rules. The nation-state remains the critical unit of the international order, and national measures (or supranational measures, in the case of the EU) are generally the most viable means of protecting important public interests.

The solution, instead, is to "optimize" national approaches for the global character of the challenges, to forge a system of global norms and rules relating to the movement and treatment of data that reflects shared international values and allows governments to regulate in the public interest as they define it. With leadership from key countries, above all the major economies of the Group of 20 (G20), it is possible to chart a course for more coordinated, thoughtful, and effective policymaking with respect to cross-border data flows. The following are proposed elements of such an effort.

Harmonization or Mutual Recognition of National Approaches

The most immediate, and potentially the most important, step that governments can take is to increase the international compatibility of their approaches to certain issues. Trade negotiators frequently use concepts of "harmonization" or "mutual recognition" to eliminate unnecessary, counterproductive regulatory differences, while maintaining countries' preferred levels of

6 See M. Bauer, H. Lee-Makiyama, E. van der Marel, and B. Verschelde, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE, May 15, 2014.

regulation, for example in the areas of food safety and fuel efficiency. The idea is the same for data flows. Just as governments analogize regulatory standards and create certification schemes for physical products to be sold in each other's' markets, they could do so for digital information, so that data can flow more fluidly between them. In other words, governments can respect the central role of national law in their overall policy environments, while at the same time enhancing the interoperability of their approaches.

The challenges in the law enforcement and national security context — where companies' compliance with the law of one country puts them out of compliance with the law of another — cry out for this type of cooperation. The overall objective would be to develop agreed international practices for requesting and sharing information quickly and predictably, consistent with commonly-held legal principles.

> *"With few exceptions, international organizations are not settings for countries to develop or enforce legally binding rules."*

First, assuming it is possible to isolate the personal data of specific individuals, countries could focus not on the location of data but on the nationality or residency of the person to whom the data relates. In other words, Germany and Canada could agree that German law would govern court orders for the personal data of a German citizen or permanent resident, even if the data were stored in a data center in Canada.

Second, countries could build on pre-existing cooperation and information sharing to develop common approaches to both the specific offenses that could give rise to an information request, as well as the evidentiary burdens that one must satisfy in order to justify such a request. This would address the problem of dueling national laws, as it would become unnecessary to determine which law applies in order to move forward with a request.

Third, countries could commit to expedited time periods for carrying out the various steps of their agreement, ensuring that the pace of cooperation is commensurate with the urgency of the investigation. Doing so would help resolve the months-long delays that characterize the existing system for requesting information under MLATs.

Greater cooperation on law enforcement and national security requests for information would enable countries to apply their own laws in a manner that both comports with the approaches of other countries and reflects the global nature of business and information. It would help ensure that authorities can obtain access to the information they need, while not relying on data localization or other measures that not only harm innovation and economic growth, but also impede privacy and security.

International Organizations

International organizations have an important role to play in driving governments toward more interoperable approaches to policymaking with respect to data flows. With few exceptions, international organizations are not settings for countries to develop or enforce legally binding rules. That quality is an asset, because it allows government officials to explore new approaches in a "lower risk" environment, without unintentionally committing their governments to inappropriate obligations.

Take the efforts of many countries to make progress on privacy issues through the Asia-Pacific Economic Cooperation (APEC) forum, which comprises 21 economies (including the United States, China, Japan, and Russia) and represents 54 percent of global GDP. In 2011, APEC established a Cross Border Privacy Rules system (CBPRs) in order to enhance the compatibility of countries' privacy rules and ensure high levels of personal data protection. Under the CBPRs, companies commit that their privacy policies reflect the nine privacy principles articulated in the 2004 APEC Privacy Framework (which include concepts such as notice, choice, and accountability), and they subject themselves to the oversight of certified "Accountability Agents." For

their part, countries ensure that they have a privacy enforcement authority, which coordinates with APEC on enforcement matters.

As of today, five economies (Canada, Japan, Mexico, South Korea, and the United States) have signed on to the CBPRs, with others suggesting they may do so in coming months. Governments like the CBPRs because it helps them reconcile national differences over privacy protections without lowering standards. Companies are increasingly interested in the CBPRs because, by allowing governments to "speak a common language" on privacy, it enhances their ability to plan investments and other business activities with certainty and predictability. For example, the CBPRs helps governments ensure that they have comparable approaches to companies' obligations to give people notice of how their personal data is used, how personal data will be used, and what remedies people will have in the event their data is used improperly.

> *"The TPP contains what would be groundbreaking legal obligations on countries to permit cross-border data flows and avoid data localization measures"*

The primary virtue of the CBPRs is that it coexists with domestic law. It does not displace national approaches to privacy protection or prescribe specific procedures for how countries should structure or administer their privacy regimes. As long as countries fulfill APEC's previously agreed core principles and provide for meaningful enforcement of those principles, the CBPRs enables economies with different governance structures and levels of development to interact more fluidly on data protection issues. In doing so, the CBPRs is a supple, thoughtful response to privacy protection in a world where company operations are spread across borders and data moves among them instinctively.

International Trade Rules

Of course, certain economies may be prepared to work toward binding legal rules in relation to cross-border data flows. These efforts deserve strong support, as they represent the best means of clarifying the "rules of the road" for international commerce and creating the type of business certainty that is so critical to companies' decisions to commit to and invest in foreign markets. There are three basic models for pursuing international trade rules, any of which could address the movement of digital information.

The first is to develop multilateral rules in the World Trade Organization (WTO). The challenge of this model is that each of the 164 member countries of the WTO must agree to do so. Given that countries such as China, Russia, India, and Indonesia are reluctant to permit largely free cross-border data flows, any achievements in the WTO would necessarily have a "lowest common denominator" quality to them.

The second model is for a subset of countries to negotiate a separate, "plurilateral" agreement, which may become a part of the WTO system in the future. The promising but currently stalled negotiations among 23 economies (one of which is the EU) toward a Trade in Services Agreement (TiSA) are a textbook example of this approach. The value of a plurilateral agreement is that countries that want to move more quickly to liberalize their markets self-select to do so. Their agreements tend to have significant commercial value in and of themselves, but they can also serve to motivate other countries to sign on in the future.

The third model is to pursue binding legal commitments on data flows in the context of bilateral or regional free trade agreements (FTAs). The much-maligned Trans-Pacific Partnership (TPP) agreement — which (before the United States withdrew from the agreement) included the United States, Japan, Vietnam, and nine other Asia-Pacific countries — is the archetype of this model. Concluded in November 2015, the TPP contains what would be groundbreaking legal obligations on countries to permit cross-border data flows and avoid data localization measures, among other important provisions relating to digital issues.

(Fortunately, the remaining 11 TPP economies are moving forward with an agreement that will likely include substantially similar commitments.)

On topics such as data flows, trade agreements almost perfectly express the recognition by countries that certain issues have an indivisible global quality, and that it is in our shared interest to develop common approaches to them. Moreover, despite their reach in constraining governments, trade agreements can be ideal tools for governments to protect their ability to regulate in the public interest. That is because virtually all modern trade agreements, including both the WTO agreements and FTAs such as the TPP, contain exceptions for governments to pursue legitimate public policy objectives.

Whether the purpose is to protect public health, public safety, the environment, personal data, or national security, trade agreements give governments significant and meaningful cover to advance their own public interests — provided they are not doing so as a pretext for protectionism.

Tear Down These Digital Walls

The modern global economy depends irrevocably on cross-border data flows. The movement of digital information across borders not only oils the gears of international commerce; it also supports rising living standards around the world and creates the possibility of solving some of our largest social, environmental, and other challenges.

Yet, a data-driven global economy also presents legitimate and important public policy considerations, such as how to protect our personal information, ensure that our law enforcement and national security authorities can do their jobs, and provide broad-based economic growth and opportunities for our populations. While it is appropriate for governments to rely on national regulatory tools to address these policy considerations, they too frequently do so in a manner that neglects the benefits of global coordination.

In this environment of tectonic political change, the world's leading governments have the opportunity to both advance these important public interests and to secure the benefits of a data-driven global economy. To do so, however, they must pursue their national priorities mindful of the global character of the challenges. This means seeking international compatibility of national regulatory approaches, using international organizations to find policy recipes that coexist with national law, and negotiating new international rules to advance shared interests.

Only a shared commitment to global coordination, mindful of course of national conditions, will ensure success in driving economic growth and protecting public interests.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org