Business Without Borders:

The Importance of Cross-Border Data Transfers to Global Prosperity

U.S. CHAMBER OF COMMERCE

HUNTON& WILLIAMS

U.S. CHAMBER OF COMMERCE

HUNTON& WILLIAMS

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Hunton & Williams LLP is an international law firm with nearly 800 lawyers serving clients in 100 countries from 19 offices around the world. The firm's Global Privacy and Cybersecurity practice is a leader in its field and has been ranked as a top law firm globally for privacy and data security.

I. INTRODUCTION

The movement of information across national borders drives today's global economy. Cross-border data transfers allow businesses and consumers access to the best available technology and services, wherever those resources may be located around the world. The free-flow of data across borders benefits all industry sectors, from manufacturing to financial services, education, health care and beyond. The seamless transfer of information is as critically important as it is inexorably linked to the growth and success of the global economy.

To function in the international marketplace, businesses need reliable, continuous access to data, wherever they are located. Routine business activities, such as providing goods and services to customers, managing a global workforce, and maintaining supply chains, require the transfer of data among corporate locations and to service providers, customers, and others situated around the world. In addition, as the Internet has facilitated the growth and success of micro-multinationals, these small businesses now have access to billions of potential customers beyond their borders and are able to compete based on the quality of their offerings, unconstrained by geographic limitations.

Despite the myriad benefits of allowing data to flow freely between countries, some governments continue to push for restrictions on cross-border data transfers. This limits the ability of companies to process, store, and access information on a global basis, and impedes end users from being able to choose the best available technologies and access information regardless of location.

Recent restrictions proposed in response to allegations regarding foreign government surveillance inappropriately conflate concerns about access to data for national security and law enforcement purposes with commercial use of, and access to, data. Other restrictions are rooted in government efforts to bolster domestic industry and support national companies. Ultimately, however, instead of creating jobs, these rules reduce efficiency, increase costs to local businesses, and block access to customers abroad, as they simultaneously prevent local consumers from obtaining the products and services of their choosing. Restrictions on cross-border data transfers may isolate domestic economies from the economic growth potential associated with the digital economy.

Regardless of intent, data transfer restrictions imposed by national laws that impede the free flow of data cause significant ramifications globally. Among other consequences,

these restrictions create barriers to entry for companies seeking to expand into new markets. For example, when data localization requirements increase the cost of launching a business in a particular jurisdiction, capital investments may be diverted to other countries with more pragmatic legal regimes.

Localization requirements also may have the effect of decreasing data security. Forcing companies to maintain local data centers frequently results in the establishment of minimally-resourced facilities that are more likely to permit network intrusions and data compromises. In the end, compliance costs are passed on to consumers when prices for goods and services are increased to fund local outposts rather than having centralized service centers that maximize efficiency. In addition, data transfer restrictions often have a disproportionate effect on smaller businesses, in some cases potentially thwarting growth opportunities altogether and preventing today's startups from becoming tomorrow's multinationals. For these businesses, data transfer restrictions have the effect of cutting the "world" out of the "World Wide Web."

Privacy safeguards are critical, and businesses play a key role in protecting the information under their control. But privacy need not be the enemy of prosperity – we can embrace strong, innovative privacy regimes that also promote trade and growth. This report offers recommendations for a path forward by highlighting existing privacy rules that can be implemented on a more global scale, and proposes new mechanisms to facilitate cross-border data transfers.

The paper begins by detailing the significance of data flows and digital trade to the global economy, illustrating these themes with case studies that demonstrate the wide variety of benefits that result from unimpeded data transfers. Next, it provides an overview of existing data transfer restrictions, refutes unjustified rationales for imposing data localization requirements, and offers insights into the very real impact data transfer restrictions have on the economy. The report describe existing, commonly used data transfer mechanisms and comments on the benefits and shortcomings of each, then focuses on how best to forge a path forward through international cooperation, highlighting favorable data transfer regimes that could be scaled to expand their applicability. Finally, the text concludes by exploring opportunities for new data transfer regimes and outlining foundational principles for future policymaking.

Technological advances and an increasingly globalized economy have brought us to a policy crossroads: one path leads to a "splinternet" of economic isolation, characterized by misguided attempts to safeguard data by building protectionist walls. Since the dawn of the global trading system, this isolationist approach has repeatedly caused

economic stagnation.[1] The other path is one of shared global economic growth fueled by an increasingly interconnected digital economy. Ideally, this would be supported by regulatory frameworks that encourage competition by opening borders for businesses of all sizes, driving innovation, creating jobs and lowering prices. This paper makes a case for seizing the opportunities presented by this critical juncture, and maps out a path toward prosperity.

II. BACKGROUND: GROWTH OF THE DATA ECONOMY

- 5 billion people are expected to be connected to the Internet by 2020
- 75% of the value-add created by the Internet is generated by co mpanies in traditional industries, such as manufacturing
- Small and medium-sized enterprises that rely heavily on Internet services have 22% greater revenue growth than companies that do not
- In 2011, top firms in the ICT sector hired more than 14 million people
- The value of e-commerce is estimated at $8 trillion per year

In today's digital economy, data should not be constrained by national boundaries. The Information Age is defined in part by the huge volume of electronic data that continuously flows across jurisdictions, and digital trade is now a mainstay feature of our modern world. The Internet is a powerful engine of economic growth that has fostered competitive trade markets, enabling companies of all sizes and in all sectors to compete in a global marketplace free from geographic limitations.

1 *See* William J. Bernstein, A Splendid Exchange, How Trade Shaped the World (2008) (chronicling the history of the modern trading system, including directly linking dwindling trade-based economic growth with the emergence of protectionist laws, *e.g.*, Spain's attempt to divert silk trade routes away from Mexico, and the decline of Barbados resulting from efforts to protect local industry at all costs). "Today's debates over globalization repeat nearly word for word in some cases, those of earlier eras. Whenever trade arrives, resentment [and] protectionism … will follow." *Id.* at 347.

Business Without Borders:

The Importance of Cross-Border Data Transfers to Global Prosperity

There is little doubt that the rapid expansion of digital commerce has had a far-reaching and permanent impact on the global economy, affecting both large and small businesses. For example, a 2011 study by the McKinsey Global Institute indicated that in five years the Internet had contributed more than 10% to the growth in GDP of the countries studied, and more than 20% to the growth in GDP of the most mature countries.[2] In 2012, more than 2.3 billion people were estimated to have access to the Internet,[3] and that number is expected to increase to 5 billion by 2020.[4] Discussing the growth in e-commerce, the Organisation for Economic Co-operation and Development (OECD) reported that the Information Communications Technologies (ICT) sector is responsible for an increasing share of total business revenue around the world, attracting investment (more than half of all venture capital in the United States went to ICT in 2011)[5] and expanding employment, with top companies in the sector hiring more than 14 million people worldwide in 2011 (up 6% from 2010).[6] Although the United States is a significant beneficiary of the explosion in digital commerce,[7] the United States is not alone in profiting from digital trade: a recent study of 400 companies in Latin America showed that online commerce already accounts for a significant portion of the region's trade activities, with the majority of companies that participate in e-commerce reporting revenue growth of more than 25% between 2011

---

2 Matthieu Pélissié du Rausas et al., McKinsey Global Instit., Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity 16 (2011), *available at* http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Internet%20matters%20-%20Nets%20sweeping%20impact/MGI_internet_matters_full_report.ashx (last visited Apr. 22, 2014) (the mature countries are Canada, France, Germany, Italy, Japan, South Korea, Sweden, the United Kingdom and the United States; the other countries in the study were Brazil, China, India and Russia).

3 International Telecommunication Union, Measuring the Information Society 6-7 (2012), *available at* http://www.itu.int/pub/D-IND-ICTOI-2012/en (last visited Apr. 22, 2014).

4 National Science Foundation, Transitions and Tipping Points in Complex Environmental Systems 9 (2009), *available at* http://www.nsf.gov/geo/ere/ereweb/ac-ere/nsf6895_ere_report_090809.pdf (last visited Apr. 22, 2014).

5 Org. for Econ. Co-operation and Dev., OECD Internet Economy Outlook 14 (2012), *available at* http://www.oecd-ilibrary.org/science-and-technology/oecd-internet-economy-outlook-2012_9789264086463-en (last visited Apr. 22, 2014).

6 *Id.* at 39. In addition, the international advisory firm Forrester Research estimated that the global cloud computing market will grow from $35 billion in 2011 to around $150 billion by 2020 as this service becomes key to many organizations' IT infrastructures. Jack Clark, *Cloud computing: 10 ways it will change by 2020*, ZDNet (July 31, 2012), http://www.zdnet.com/cloud-computing-10-ways-it-will-change-by-2020-7000001808 (last visited Apr. 22, 2014).

7 Pélissié du Rausas et al., *supra* note 2, at 4.

and 2012.[8] The value of digital commerce to the global marketplace is truly staggering: an estimated $8 trillion a year.[9]

Furthermore, it is not only large enterprises that benefit from digital trade. A global study found that small and medium-sized companies that rely heavily on Internet services typically have 22% greater revenue growth than those that use the Internet minimally. Smaller organizations that conduct business on the Internet tend to grow twice as rapidly as their offline counterparts.[10]

Technological developments have had a major impact on the amount of data being generated on a daily basis. Computing power has increased exponentially, doubling every year and a half since the 1970s.[11] In addition, significant technological advances in how data are recorded and retained have provided businesses and consumers with access to inexpensive data storage that may be accessed in real time from anywhere in the world. The ease and speed with which we now collect and analyze data, from social media posts to medical records, have led to the creation and storage of vast quantities of information, which in turn has fueled an explosion in the number of cross-border data transfers. The geographic reach and growth of companies also drives the transfer of enormous amounts of data. All cross-border trade and services rely on data moving across borders to meet basic business needs, from emailing colleagues in different offices to streamlining global supply chains among geographically dispersed offices. Small and medium-size businesses are able to connect with billions of potential customers around the world, competing on quality of products rather than location.

The free flow of data also is critical to traditional businesses such as manufacturers, health care providers, educators, and financial institutions. Some estimates indicate that 75% of the value created by Internet commerce accrues to companies that rely on, but

8 Mark Keller, *Latin America's New Trade Routes*, Latin Bus. Chronicle, Nov. 6, 2013, http://www.latinbusinesschronicle.com/app/article.aspx?id=6553 (last visited Apr. 22, 2014).

9 James Manyika & Charles Roxburgh, McKinsey Global Institute, The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity 1 (2011), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer (last visited Apr. 30, 2014).

10 David Dean et al., Boston Consulting Group, The Internet Economy in the G-20 (2012).

11 Jonathan Koomey, *The Computing Trend that Will Change Everything*, MIT Technology Review Special Business Report, Apr. 9, 2012, *available at* http://www.technologyreview.com/news/427444/the-computing-trend-that-will-change-everything (last visited Apr. 22, 2014).

do not necessarily develop, Internet-enabled products.[12] Even companies that do not engage in direct sales over the Internet must transfer data, records, and communications relating to the tangible goods and services they provide. This information must frequently cross borders.

A recent report, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, illustrates this concept, noting the ubiquitous nature of data transfers, and the degree to which they affect all industry sectors. The report indicates that "a purchase made in a store requires access to card processing and other financial services backed by data transmission and hosting services to process the transaction. The vendor needs leasing, distribution, logistics, and facility management services to deliver the good. Likely, a number of different services, such as utilities, consulting, engineering or creative were needed to produce the good in the first place."[13]

An inevitable consequence of the exponential growth in the amount of data we create and use is the demand for constant, reliable access to the data, especially with an increasing number of businesses deriving their revenue primarily – or solely – from electronic transactions. Nearly all businesses transfer a combination of employee, consumer, and corporate customer personal data across borders as part of their everyday business functions. Conversations with businesses in a variety of sectors have indicated that, for many, "it's critical that we move data around the world" and that these transfers "ensure consistency and efficiency throughout all business units and functions across the globe."[14] They improve "reliability, security, and data accuracy."

12 Josh Meltzer, *Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries* 1 (Brookings Inst. Global Econ. & Dev., Working Paper No. 69, 2014), *available at* http://www.brookings.edu/~/media/research/files/papers/2014/02/internet%20international%20trade%20meltzer/02%20international%20trade%20version%202.pdf (last visited Apr. 22, 2014).

13 Eur. Ctr. for Int'l Political Econ., The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce 5 (2013), *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf (last visited Apr. 22, 2014).

14 To assess the real-world impact of cross-border data transfer restrictions on global organizations, we contacted high-profile companies operating on a multinational basis and asked for their insights regarding these important issues. We received responses from more than 30 companies, representing a variety of industry sectors including consumer goods, health care, financial services, retail, telecommunications, manufacturing and information technology, and operating in nearly every country on earth. The information we obtained offers unique and valuable insights into the demographics, practices and concerns of companies that regularly confront challenges related to cross-border data transfer restrictions. Comments and other data derived from this effort are discussed throughout this report.

III. CASE STUDIES: BENEFITS WITHOUT BORDERS

Policymakers and citizens often fail to appreciate the many benefits of cross-border data transfers in their day-to-day lives. As illustrated in the case studies in this report, data transfers are not just essential to business operations and revenue growth, but also facilitate socially beneficial global initiatives and help improve the health and well-being of people around the world.

A. Medical Data Transfers: Health Care Without Borders

A number of multinational medical device manufacturers routinely transfer data across jurisdictional boundaries for maintenance and repair purposes.[15] For instance, one device manufacturer lamented the difficulties engineers face when attempting to carry out critical functions, such as providing real-time service on large medical equipment to facilitate effective patient care. Sophisticated equipment of this nature often cannot be readily transported to repair facilities, and in some cases the device requiring service is the only machine of its type in a particular geographic area.

If an engineer who is specially trained to service a highly complex machine is not permitted to access the device remotely to conduct repairs (because she may incidentally access the data of patients who benefitted from the machine that morning), then patients who need the machine that afternoon may be turned away. In this example, cross-border data transfer restrictions literally could have life or death consequences for patients. As one company noted, "Some of the data that is transported are used for purposes well beyond commercial purposes, including public health and safety concerns."

B. Data Integrity: Maintaining Accuracy in an Era of Heightened Mobility

In addition to technological advances, the Information Age has been marked by an unprecedented increase in human mobility. Massive numbers of individuals cross borders on a daily basis for both personal and professional reasons, and in many

15 In addition to medical devices, other types of machinery may be repaired in a virtual environment, thus sparing consumers time and effort. For example, a recent report highlighted the fact that Tesla Motors is now able to make safety changes to plug-in electric vehicles using "over-the-air software updates," calling into question the use of the term "recall" when discussing this type of maintenance. *See* Angela Greiling Keane, *Tesla's Musk Has Point About 'Recall,' Ex-Regulator Says*, Bloomberg News, Jan. 21, 2014, http://www.bloomberg.com/news/2014-01-21/tesla-s-musk-has-point-about-recall-ex-regulator-says.html (last visited Apr. 22, 2014).

cases these trips result in temporary or permanent migration abroad. International relocations have created new challenges for businesses that provide information about consumers' financial histories and help companies keep track of, and in touch with, their customers.

Data transfer restrictions may impede efforts to identify fraudsters who, after racking up huge debts in one country, are able to start fresh with a clean slate by moving to another jurisdiction. Blocking credit histories from following individuals across borders also affects law-abiding expatriates who are unable to open accounts or obtain loans because they have no way to prove they have a strong credit history in their country of origin.

Along the same lines, the data hygiene industry helps companies maintain accurate databases so that they can preserve customer relationships when it is not uncommon for individuals to move and change telephone numbers on an almost annual basis. Aside from the inefficiency of having to maintain the relevant data by country, laws that restrict the centralization of customer records increase threats to data integrity by preventing customer files from being cross-checked for errors.

C. The Industrial Internet: Creating Efficiencies for Manufacturing and Energy Development

Few large-scale manufacturers or energy producers limit their business operations to a single country. Most operate multinationally, with many running major operations in dozens of jurisdictions. Current data transfer restrictions are ill-suited to help those companies develop and take advantage of the efficiencies they can create using the breadth and depth of their knowledge and experience in their areas of expertise. For example, a representative of a company in the energy sector highlighted the ways in which his business is able to help oil and gas manufacturers function at top capacity while promoting safety and ensuring continuity of service. To achieve this, the company must remotely collect operational data from equipment in use in locations scattered across the globe, then employ diagnostic and prognostic analyses of the data to alert customers of necessary maintenance and potential risks. Hampering companies' ability to monitor the data transmitted by such equipment from around the world both decreases efficiency and increases the likelihood of a preventable accident that could damage infrastructure and even result in loss of life.

D. International Insurance Providers: Immediate Responses to Remote Crises

The insurance and reinsurance industry offers another strong argument in favor of allowing the rapid and nimble movement of data across borders. In the event of a

major natural disaster, immediate access to clients' insurance contracts and records is essential to deploying needed resources to policyholders and helping begin the rebuilding process for affected individuals. When cross-border data transfer restrictions impede the movement of these data, or restrict the storage of such data outside the country of origin, the results can be disastrous. For example, if a particular country requires an insurer to maintain all its data pertaining to citizens of that country within the country's borders, the insurer may have no way to access the data it needs to help affected residents recover from a tsunami, earthquake, or other major disaster. As one insurer explained, "If our data center is under 10 feet of water, we can't assess who has coverage or how to start processing valid claims." The insurer added that the ability to maintain backup copies of insurance coverage data in multiple remote locations helps the company ensure continuity of service even in the face of massive power outages and physical destruction of servers or other company property that typically would be used to validate coverage and provide assistance.

E. Human Resources: Managing a Global Workforce

Regardless of industry sector, all companies large and small have one thing in common: employees. Perhaps no commercial data transfer need is as acute, or as universal, as the need for companies to be able to access data about their workforce around the world. Having a complete and accurate picture of the company's personnel, wherever in the world they may sit, is essential to deploying and managing intellectual capital effectively. As one company indicated, "Without cross-border transfers of personal data, [we] could not effectively pool employee data to evaluate employees against their peers outside the country of collection for ratings, promotions or assignment planning."

Along similar lines, a U.S.-based manager at a large multinational has team members in more than 20 countries; she needs to have their records at her fingertips for myriad purposes from performance reviews and promotion decisions to coaching and mentoring activities. A centralized corporate directory, the existence of which could be threatened by stringent data transfer restrictions, also is key for obvious logistical purposes. Furthermore, innovation is driven by cross-cultural project teams collaborating in virtual environments, working together to solve problems and develop products from locations around the world. And IT technicians staggered across time zones help ensure that assistance is always available for employees working unconventional hours or logging in from remote locations. Modern businesses simply cannot thrive, or even function effectively, without the ability to manage their talent on a global basis.

F. Global Health Care: Tracking Pandemics, Saving Lives

The Internet has proven to be an invaluable resource for global health organizations, enabling them to make massive leaps forward in monitoring the outbreak and spread of infectious diseases around the world. But this type of tracking is possible only through the rapid collection and dissemination of real-time medical data concerning patients in multiple countries. Owing in part to increasing globalization and modern transportation, what may appear as an isolated cluster of illness in one region of one country easily could explode into a national epidemic or a global pandemic in a matter of weeks or even days.

Unless epidemiologists and other medical professionals are able to communicate freely about emerging health crises with their colleagues located elsewhere, there is little the medical community as a whole can do to slow or stop the spread of disease outbreaks. Although these types of data exchanges rarely require the sharing of information such as a person's name or personal identification number, they do sometimes involve disclosing the age, gender, race and other details about affected patients to identify trends and provide clues to solve complicated medical mysteries. From a legal standpoint, however, this type of information frequently is considered highly sensitive, and transferring it to third parties is prohibited by certain data protection laws. Some of these laws have exceptions for emergency situations, but a rapidly spreading illness may not qualify as an "emergency" until it is too late.

IV. RESTRICTIONS ON CROSS-BORDER DATA TRANSFERS

Despite the multitude of benefits associated with allowing data to flow freely across borders, governments around the world continue to step up efforts to impose restrictions on cross-border data transfers. Although in some cases the restrictions are meant to promote privacy, too often the motives are protectionist or reflect the conflation of commercial issues with national security concerns. These misguided policy choices take us down a path that stifles job growth and leads to economic stagnation.

Unfortunately, regardless of intent, many of the regulations affecting the commercial use of data impose unduly restrictive constraints on international data flows, doing more harm than good to the affected economies. Initiatives aimed at improving data transfer regulations should refrain from focusing on a single set of rigid, one-size-fits-all

rules. Instead, such initiatives should focus on developing flexible, privacy-protective regulations that can coexist with, and adapt to, technological advances.

Data transfer restrictions generally fall into two categories: data localization requirements and privacy regulations. Data localization rules, which usually are binary in nature, impose an outright ban on transferring data out of the country, or a requirement to build or use local infrastructure and servers.[16] These regulations often are based on misperceptions that are easily refuted. Accordingly, it is more effective to demonstrate the flawed reasoning behind the laws and persuade policymakers to repeal them altogether, rather than attempt to find common ground on the localization issue. Conversely, privacy regulations are nuanced and rooted in important cultural and societal concerns. Such rules generally seek to protect legitimate interests and fundamental rights. Thus, it is imperative that governments work together to understand the underlying interests when developing solutions to ensure that local privacy regimes do not unnecessarily restrict trade.

In the past year, high-profile revelations regarding government surveillance activities resulted in a number of proposals regarding data localization and transfer restrictions.[17] Although some of the adverse reactions are understandable, thus far most of the efforts to alleviate concerns regarding surveillance have failed to address the real issue. The means by which governments access foreign personal data should have no bearing on the laws that regulate corporate data transfers or the mechanisms companies employ for cross-border transfers.[18] Efforts to reform government surveillance must directly address government actions – these concerns cannot be resolved by creating new restrictions on businesses.

16 *See generally* Anupam Chander & Uyen P. Le, Breaking the Web: Data Localization vs. the Global Internet (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 (last visited Apr. 22, 2014) (rebutting common rationales for localization by arguing that some countries are using national security as an excuse to implement localization rules that enable authoritarian governments to suppress free speech and monitor their own populations).

17 For example, the Safe Harbor framework was heavily criticized following revelations regarding U.S. law enforcement access to EU personal data held by certain Safe Harbor-certified entities. Also, in 2011, the Brazilian Congress introduced the Marco Civil da Internet, a draft bill to establish the country's first set of Internet regulations. The bill included requirements regarding personal data protection. Following revelations in 2013 on the NSA's surveillance program, the Brazilian government introduced new amendments, including a requirement that companies store any type of Brazilian data on servers physically located in Brazil. This provision generated significant controversy and opposition, and ultimately the localization requirements were removed from the bill.

18 The political rhetoric connecting government surveillance to commercial data transfers ignores the fact that a completely separate legal regime often controls law enforcement access to data.

Business Without Borders:

The Importance of Cross-Border Data Transfers to Global Prosperity

During the last few years, there have been a number of data localization proposals around the world. Whether in response to national security surveillance concerns, a desire to protect domestic industry or some combination of the two,[19] these proposals are based on a number of false assumptions and ultimately fail to meet any of the stated goals.

Myth: *Data localization will promote domestic industry.*

Fact: Data localization requirements reduce competitiveness by walling off domestic businesses from the billions of potential customers outside of the home country's borders. This isolation reduces investment and access to capital – the ability to assess a potential borrower's creditworthiness or to spot potentially fraudulent activity often depends on the ability to move data across borders. Recent studies found restrictions on data transfers from the EU to the United States would reduce the EU's GDP by €104 billion to €170 billion ($143 billion to $235 billion) and also lead to a 6.7% decline in EU services exports.[20]

A forthcoming study demonstrates that economy-wide data localization requirements also could reduce GDP by 1.1% in the EU, .7% in Indonesia and 1.1% in South Korea. The loss of competitiveness resulting from localization requirements could reduce investments by 3.9% in the EU, 2.3% in Indonesia and 3.1% in Vietnam, and decrease exports from Indonesia by 1.7%.[21]

Myth: *Requiring local data centers will create jobs.*

Fact: Jobs are created by businesses that leverage a global network of data centers, using the best available technology to increase efficiency regardless of location. This enables domestic industries to focus on the quality of their products and services, better positioning them to compete in global markets. Data centers can cost

19 *See, e.g.*, Press Release, Eur. Comm'n, What does the Commission mean by secure Cloud computing services in Europe? (MEMO/13/898) (Oct. 15, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-898_en.htm (last visited Apr. 30, 2014) (proposing the creation of a virtual "Schengen Area" for data in response to surveillance revelations and supporting the development of European cloud computing solutions).

20 Eur. Ctr. for Int'l Political Econ., *supra* note 13.

21 Hosuk Lee-Makiyama, *The Costs of Data Localization,* Eur. Ctr. for Int'l Political Econ. Global Econ. Blog (Apr. 22, 2014), http://blog.ecipe.org/2014/04/the-costs-of-data-localization.html (last visited Apr. 30, 2014).

hundreds of millions of dollars to build and operate, and even a cutting-edge data center requires fewer than 150 workers.[22]

Myth: *Data localization increases security.*

Fact: Data security depends on a plethora of controls, not on the physical location of a server. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take a data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions.

Myth: *Data localization will lower costs for domestic business.*

Fact: : **Requirements for local servers could hurt domestic industry by compelling local businesses to sacrifice efficiency and seek out more expensive, less reliable services.** Localization requirements may limit the ability of firms to access logistics and supply chain infrastructure, conduct effective research, secure appropriate insurance, or readily participate in financial markets. Moreover, one source indicates that every minute a data center is down can cost a company as much as $7,900.[23] Regions with inconsistent electric grids frequently experience hours of downtime, resulting in substantial costs. Economic growth is better served by companies that are able to leverage the most efficient and reliable services from around the world.

22 Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, Wall St. J., Nov. 13, 2013, http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688 ("On average, it costs $60.9 million to build a data center in Brazil, compared with $51.2 million in Chile and $43 million in the U.S. Monthly operating costs, including for energy, average $950,000 in Brazil, compared with $710,000 in Chile and $510,000 in the U.S."). *See also* Jon Swartz, *Top secret Visa data center banks on security, even has moat*, USA Today, Mar. 25, 2012, http://usatoday30.usatoday.com/tech/news/story/2012-03-25/visa-data-center/53774904/1 (describing Visa's main data center, which processes 2,500 transactions per second and required an estimated investment of hundreds of millions of dollars; it is run by about 130 on-site employees).

23 Jason Verge, *Study: Data Center Downtime Costs $7,900 Per Minute*, Data Ctr. Knowledge, Dec. 2, 2013, http://www.datacenterknowledge.com/archives/2013/12/03/study-cost-data-center-downtime-rising (last visited Apr. 22, 2014).

Unlike data localization rules, transfer restrictions related to privacy protection aim to address a broader range of legal and social concerns. The remainder of this report focuses on privacy-related restrictions (as opposed to data localization requirements) and suggests a path forward that would simultaneously promote privacy and facilitate economic growth by reducing impediments to cross-border data transfers.

Procedures to protect privacy and secure data are vital to modern business operations. Given the concerns of consumers and governments alike, companies strive to develop trustworthy products that meet privacy expectations. Increasingly, those expectations include ensuring that privacy protections travel with the data, regardless of where they are transferred, stored, or accessed.

Nearly 100 countries globally have enacted some form of data privacy legislation. The legal landscape in this area varies on multiple fronts, ranging from general disagreement on basic concepts (such as what constitutes personal data) to overarching philosophical differences on data collection and use. The concepts of "privacy" and "data protection" may overlap across jurisdictions, but the ways in which individual countries seek to protect the data of their citizens, and how they strike a balance between public and private interests in this area, often are rooted in cultural norms. Consequently, global companies are confronted by a patchwork of disparate data privacy laws, many of which place some restrictions on the transfer of personal data from one jurisdiction to another.

Even countries that do not impose specific cross-border data transfer restrictions may, nevertheless, regulate certain data transfers through limitations on data sharing or disclosure. For example, in the United States, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) restricts how certain entities share health information.[24] In the Philippines, the data controller is required to ensure that any third-party processor, whether domestic or international, provides a comparable level of data protection as is required by the Data Privacy Act 2012.[25] These laws are neutral regarding the geography of the data recipient. Other national laws, particularly

24 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

25 *See* Data Privacy Act of 2012, Rep. Act No. 10173, § 21, *available at* http://www.gov.ph/2012/08/15/republic-act-no-10173 (last visited Apr. 22, 2014) ("Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.").

those aimed at the financial services sector, also may impact whether and how personal data are transferred.[26]

26 For example, German tax law mandates that documents required for tax and audit purposes, such as contracts with customers and commercial correspondence regarding payments, must remain within the jurisdiction of the German tax authorities (i.e., in Germany) because the transfer of these records abroad could hinder the ability of German tax authorities to exercise their inspection powers. To transfer these types of records, a formal waiver must be obtained from the competent German tax authority. In South Korea, the Insurance Business Act requires insurance companies to maintain all basic resources in-house, including IT systems.

The Annex to this report contains an illustrative list of privacy regimes around the world and their attendant cross-border data transfer restrictions.

V. ECONOMIC IMPACTS

"Some of the world's governments believe that limiting the private sector's ability to transfer, store, and process data across borders will somehow protect user privacy and improve security. Yet these well-meaning efforts are ultimately counterproductive. The movement of data is no less important to the global economy than the movement of money. And it's not just critical for banks but also for our clients—for any company that does business in many countries. Cross-border data flows, just like cross-border financial flows, allow companies to integrate their personnel, manage their global supply chains and customer networks, and maintain the competitiveness they need to grow and thrive. The free movement of data is fully compatible with legitimate security concerns. As we know, companies try and strike this balance every day."

Michael Corbat, Chief Executive Officer, Citigroup

"There's no doubt in my mind that the way in which we can access and use information has incredibly strongly increased the power we have as economic agents and the freedom we have as individuals, hence the risks that you were point out of what happens if we try to stop that."

Marco Annunziata, Chief Economist and Executive Director of Global Market Insight, General Electric Company

(quote from Atlantic Council 2013 Strategic Foresight Forum - the Challenges and Opportunities of the Third Industrial Revolution)

As we heard repeatedly during our discussions with business leaders, companies across all industry sectors are deeply concerned about the very real and negative impact data transfer restrictions have on their operations. Compliance with multiple data transfer regimes often is a highly complex endeavor. Unfortunately, in this case, there is no

correlation between complexity and effectiveness when it comes to protecting data. In light of the difficulty in complying with a patchwork of overlapping and conflicting data transfer regimes, some companies have chosen to avoid particular markets altogether. For the vast majority of businesses, processing personal data is not a cash-generative endeavor. Accordingly, the level of regulation "feels disproportionate to the risk posed to people's privacy by most large corporations." Too often, data transfer restrictions have caused companies to postpone entering a foreign market due to compliance concerns, or have required them to invest significant resources to comply with cross-border data transfer laws in markets in which they operate.[27]

Ensuring that business operations comply with all applicable data protection laws can be costly. For example, data transfer restrictions raise the specter of financial burdens associated with building bespoke data storage centers in multiple locations to accommodate a host of national laws. Some companies based in the European Union reported having to invest significant resources to restructure their IT systems to restrict EU-originating personal data from being transferred to "non-adequate" jurisdictions in violation of EU law. On the flip side, certain U.S.-based businesses have chosen to avoid capital investments in the EU because "the myriad of byzantine compliance requirements" discourage the establishment of IT infrastructure in European countries. When businesses are discouraged from entering or investing in new markets, consumers and businesses alike may be deprived of access to world-class products and services.

But the costs to companies of complying with cross-border data transfer restrictions are not limited to cash expenditures. Implementing compliant data transfer mechanisms often requires lead time of months, even years, slowing growth and preventing expansion. With regard to specific transfer mechanisms in Europe, companies expressed frustration with the amount of time required to obtain approval for binding corporate rules (BCRs), as well as with delays involved in using standard contractual clauses in jurisdictions that require notification to, or prior approval of, the national data protection authority (DPA).

Aside from internal considerations regarding the allocation of resources and time required to implement compliance mechanisms, companies indicate that cross-border data transfer restrictions may also adversely affect their interactions with customers and

27 The potential economic consequences are not theoretical. . As goods exports are highly dependent on the efficient provision of services (up to 30% of manufacturing input values come from services), EU manufacturing exports to the United States could decrease by up to -11%, depending on the industry. Eur. Ctr. for Int'l Political Econ., *supra* note 13, at 5. *See also* Meltzer, *supra* note 12, at 22.

their ability to market their products and services. One company representative stated that his company has had "significant difficulties selling to customers in Europe if they think that their data are being transferred outside the EEA."
On the policy front, companies are increasingly nervous about the future legal landscape in this area. Nearly all of the industry leaders with whom we spoke indicated that they believe "conflicting or overly burdensome" privacy regimes are likely to become more problematic and that comprehensive restrictions on data transfers are a looming concern. Businesses worry that "the EU is in danger of using a sledgehammer to crack a walnut."

Companies operating in multiple jurisdictions report that "the way data transfer agreements need to be implemented is often illogical and impractical." Many feel that regulatory authorities fail to appreciate "the practical implications of regulations that prohibit or restrict cross-border transfers" or that they seem to have "a misunderstanding of why companies transfer data." Companies perceive not only "a great deal of ignorance and paranoia" surrounding data transfers, but also inconsistency. For example, "most companies send emails to the U.S. every day, but aren't happy storing their emails in the U.S." – a paradox that was reiterated in our discussions with stakeholders, some of whom noted that certain clients no longer wish to transfer data to, or store data in, the United States.

VI. DATA TRANSFER MECHANISMS

There is broad consensus among organizations across all industry sectors that a competitive global marketplace that fosters innovative solutions (such as cloud computing) depends on the ability to move data around the world. Data transfer mechanisms must be flexible and able to accommodate large-scale data transfers, but without formalistic, bureaucratic rules that ultimately may not ensure real data protection.

Many regimes waive general data transfer restrictions where transfers are made to specific, preapproved jurisdictions. For example, in the EU, personal data may be transferred freely to countries deemed by the European Commission to have "adequate" data protection laws in place.[28]

28 The approved recipient countries as of December 20, 2013 were: Andorra, Argentina, Canada (where the data are subject to the Canadian Personal Information Protection and Electronic Documentation Act), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay. The list of recipient countries approved by the European Commission can be viewed at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited Apr. 22, 2014).

The following section describes mechanisms companies often use to comply with applicable legal restrictions when transferring data across borders. To illustrate the benefits and shortcomings of the various approaches, we have included excerpts from our discussions with business leaders regarding their experiences with the various data transfer mechanisms are included.

A. Consent

The vast majority of privacy laws that restrict cross-border data transfers permit such transfers with the consent of affected individuals.[29] To be valid, consent generally requires that the individual be notified of (1) the fact that her personal data will be transferred outside of the originating jurisdiction, specifying to which jurisdictions the data will be transferred, and (2) the fact that the recipient countries may not afford the same level of data protection as the originating country.

Although consent is a common exception to data transfer restrictions, and more than 70% of the businesses we contacted indicated that they rely on consent, it has a number of drawbacks.

First, consent usually must be obtained in writing (either as a legal requirement or for evidentiary purposes), which can be difficult and cumbersome in practice. Second, if the individual does not provide consent, or later revokes her consent, the data exporter needs to find an alternative transfer mechanism. Third, whereas other transfer mechanisms, such as the Safe Harbor framework or standard contractual clauses (discussed later), may be implemented to cover all data in a particular transfer, consent must be obtained from each individual separately.

B. Standard Contractual Clauses

Standardized contracts serve as a transfer mechanism in a number of data privacy regimes. These contracts typically contain provisions that address issues such as data security, limitations on further use and disclosure of personal data, and liability for damages to affected individuals in the event of a violation.

The European Economic Area (EEA) is the most prominent region in which standard contractual clauses serve as a vehicle for the legal transfer of personal data across borders. For transfers of data outside of the EEA, the European Commission has approved standard contractual clauses to cover (1) transfers to an agent or service provider processing personal data on the data exporter's behalf, and (2) transfers to a third party

29 Consent plays a prominent role in the data transfer regimes of many jurisdictions. In the EU, consent operates as a derogation (i.e., an exception).

who will process the personal data for its own purposes. While European jurisdictions outside of the European Union, such as Norway, Serbia and Switzerland, do not use Commission-approved standard contractual clauses, their standard data transfer agreements borrow heavily from the Commission's clauses and are broadly similar. Other countries that encourage the use of binding agreements as a compliant data transfer mechanism include Israel, Russia and South Africa.

Standard contractual clauses are a useful tool on which most businesses rely. Our discussions indicated that a very high percentage of companies (nearly 85% of those we consulted) use them in some capacity, likely because, among the few available methods for legally transferring personal data across borders, executing a standard contract can be far easier than implementing more comprehensive accountability regimes such as the Safe Harbor framework or BCRs (discussed later).

Some companies have criticized the utility of standard contractual clauses, which diminish as the volume and complexity of data flows increase. As one company representative said, "Data transfer agreements contain impractical clauses that don't work well in a large multinational – e.g., a customer right to approve subcontractors."[30] And although standard contractual clauses may be used to legitimize multiple transfers worldwide, in practice, the requirement to negotiate and execute separate agreements with every data exporter and importer, and for every new category of data or purpose not covered by a preexisting agreement, represents a significant bureaucratic burden that may be particularly onerous for small and medium-sized enterprises.

Standard contractual clauses generally work best for linear transfers of data from point A to point B. Their rigid structure is not well suited to the web of data transfers and onward transfers between service providers and subcontractors, which frequently occur on a fluid basis, particularly in cloud-based platforms. Moreover, the use of standard contractual clauses requires the prior approval of the DPA in some jurisdictions (e.g., Norway, Austria, and Spain), creating a bottleneck to adoption. One of the company representatives with whom we spoke commented bluntly that standard contractual clauses are "no longer fit for purpose of the 21st century."

C. Safe Harbor Framework

The Safe Harbor framework[31] was negotiated by the U.S. Department of Commerce and

30 The possibility of a DPA auditing the premises of a subcontractor has dissuaded many cloud service providers from using standard contractual clauses.

31 *See* Export.gov, Safe Harbor Privacy Principles: Issued by the U.S. Department of Commerce on July 21, 2000, *available at* http://www.export.gov/safeharbor/eu/eg_main_018475.asp (last visited Apr. 22, 2014).

the European Commission "to bridge [the] different privacy approaches [in the United States and the EU] and provide a streamlined means for U.S. organizations" to transfer personal data from the EU in compliance with the EU Data Protection Directive (the EU Directive).[32] The framework was developed because the European Commission does not consider data privacy protections in the United States to be "adequate." Organizations that self-certify to the Safe Harbor framework are legally permitted to receive personal data originating from the EEA.

The Safe Harbor framework is composed of a set of Privacy Principles and Frequently Asked Questions.[33] To certify to the Safe Harbor, organizations generally are required to (1) conform their privacy practices to the Safe Harbor Privacy Principles; (2) file a self-certification form with the Department of Commerce; and (3) publish a Safe Harbor privacy policy that states how the company complies with the Privacy Principles.

The Department of Commerce also has developed a Safe Harbor framework for Switzerland, enabling participating U.S. entities to receive Swiss-originating personal data. The two Safe Harbor frameworks serve as a key data transfer mechanism for many U.S. businesses, with more than 4,000 currently self-certified to either or both of the frameworks. Nearly 70% of the companies we contacted said that they rely on the Safe Harbor for cross-border data transfers to the United States.

The Safe Harbor framework has been heavily criticized following recent revelations regarding U.S. law enforcement access to EU personal data held by certain Safe Harbor-certified entities. This criticism is unwarranted. The critics are inappropriately conflating law enforcement access to personal data once the data are outside of the originating jurisdiction, with the mechanism that was used to transfer the data out of the jurisdiction in the first place. Unfortunately, this key distinction has been overlooked, as has the fact that other cross-border data transfer mechanisms are similarly vulnerable with respect to access by government agencies once data are in the recipient country. On November 27, 2013, the European Commission proposed 13 recommendations for changes to the Safe Harbor framework, including improving transparency, simplifying alternative dispute resolution mechanisms and making them more affordable for EU data subjects, and increasing active enforcement through regular audits and monitoring

32 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 (EC).

33 The seven Safe Harbor privacy principles are notice, choice, onward transfer, security, data integrity, access and enforcement. Export.gov, *supra* note 31.

of certified entities.[34] Companies have already felt the effects of this debate, noting, for example, that, "key clients [have] started to insist on [a] blanket ban on data transfer to the USA" – notwithstanding the fact that the Safe Harbor remains a valid data transfer mechanism.

In February 2014, the European Parliament passed a motion requiring the European Commission to reassess the adequacy of the Safe Harbor and consider revising or revoking it.[35] Subsequently, on March 12, 2014, the European Parliament passed a resolution setting forth its findings and recommendations regarding the NSA's surveillance program.[36] The resolution included a call to suspend the Safe Harbor framework, alleging that it does not adequately protect European citizens. The Parliament's resolution did not have immediate consequences for the validity of the Safe Harbor, as only the Commission is empowered to suspend or revoke the Safe Harbor framework.

Currently, the European Commission and the U.S. Department of Commerce are involved in ongoing talks concerning the Commission's 13 recommendations for the Safe Harbor. There appears to be progress toward an agreement on many of the Commission's recommendations, as well as with respect to other proposed revisions to the framework that were introduced during the negotiations. For now, the future of the Safe Harbor remains unsettled, and certified entities cannot be certain of the longevity of this data transfer mechanism. The Article 29 Working Party has made clear that if the negotiations fail, it expects the Commission to suspend the Safe Harbor.[37] That said, given the significant number of organizations that currently are self-certified to the Safe Harbor, the European Commission will need to consider carefully any actions that would interfere with the continued operation of the Safe Harbor framework.

34 *See* Press Release, Eur. Comm'n, European Commission calls on the U.S. to restore trust in EU-U.S. data flows (IP/13/1166) (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_IP-13-1166_en.htm (last visited Apr. 22, 2014).

35 European Parliament Resolution on the US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)) Feb. 12, 2014.

36 *See* Press Release, Eur. Comm'n, Progress on EU data protection reform now irreversible following European Parliament vote (MEMO/14/186) (Mar. 12, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (last visited Apr. 22, 2014).

37 The Article 29 Working Party is an advisory group comprised of representatives from the data protection authorities of each EU Member State, the European Data Protection Supervisor and the European Commission. *See* Article 29 Working Party Letter to Viviane Reding, European Commission Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, Apr. 10, 2014, *available at* https://www.huntonprivacyblog.com/files/2014/04/20140410_wp29_to_ec_on_sh_recommendations.pdf (last visited Apr. 22, 2014).

D. Binding Corporate Rules

Binding corporate rules (BCRs) are legally enforceable internal rules within a corporate group that mandate a uniform level of protection for all intra-company data transfers. Once approved by a lead EU data protection authority, BCRs enable unrestricted global transfers of EU-originating personal data within a corporate group.[38] BCRs must (1) be binding on all entities within the corporate family; (2) be binding on employees; (3) include a complaints procedure; and (4) be supported by appropriate training, audits and privacy oversight. At least one corporate entity located within the EU must be liable for violations, cooperate with the relevant DPAs, and agree to pay compensation to affected individuals for violations.

The BCR document must address key substantive data privacy requirements, including purpose limitation; data quality and proportionality; legal bases for processing personal data; transparency and information rights; rights of access, rectification, erasure, and blocking; security and confidentiality; onward transfers; and third-party beneficiary rights. In practice, BCRs are far more than a mere data transfer mechanism: They provide and require a comprehensive corporate privacy compliance program. Although BCRs have been in existence for some time,[39] their application recently was extended to enable service providers to develop BCRs to cover data they process as agents on behalf of other companies.[40] BCRs are likely to be formally recognized in the proposed

38 Generally, BCRs cannot be used to enable data transfers to a third party outside of the corporate group, although a controller may be able to rely on a processor's BCR, in conjunction with contractual terms, as a means of establishing adequacy.

39 Article 29 Working Party, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74 (June 3, 2003); Article 29 Working Party, Model Checklist, Application for approval of Binding Corporate Rules, WP 102 (Nov. 25, 2004); Article 29 Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules," WP 107 (Apr. 14, 2005); Article 29 Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, WP 108 (Apr. 14, 2005); Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 153 (June 24, 2008).

40 Article 29 Working Party, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195 (June 6, 2012); Article 29 Working Party, Explanatory Document on the Processor Binding Corporate Rules, WP 204 (Apr. 19, 2013).

General Data Protection Regulation that would repeal and replace the EU Directive (the Proposed EU Regulation).[41]

A number of companies indicated that BCRs are disfavored as a data transfer mechanism for a variety of reasons, citing, for example, the "overly burdensome bureaucratic requirements and expense of getting [BCRs] established." Others agreed, describing BCRs as "far too costly," "impractical" and "time-consuming." For smaller entities, BCRs are "too large and complex" to implement. BCRs also are seen by some as not flexible enough to respond to the needs of certain types of organizations, with one company noting that BCRs require "a highly-centralized management/operating model" that is incompatible with his organization's structure and business practices. Many of the corporate executives we consulted expressed concern that a daunting amount of effort is required to implement BCRs, and one candidly said that "the costs outweigh the benefits far too much." In addition, BCRs are wholly inaccessible to smaller companies.

VII. FINDING A PATH FORWARD

As this report demonstrates, global businesses of all sizes need a flexible, practical, "future-proof" data transfer framework suitable for the 21st century. The ever-increasing volume of cross-border data flows will continue to strain regulators' finite resources, making data transfer mechanisms that require prior regulatory approval unworkable.[42] Organizations that operate in the global marketplace require a framework that is agile enough to accommodate present and future data flows while respecting local legal differences, recognizing similarities among local requirements, protecting individuals' rights, and enabling appropriate enforcement in the event of a violation.

41 The Proposed EU General Data Protection Regulation is currently under negotiation by the European Commission, European Parliament and the Council of the European Union. The final approved text is not expected before 2015. Viviane Reding, Vice-President of the Eur. Comm'n, Peter Hustinx, Eur. Data Prot. Supervisor, Claude Moraes, Member of the Eur. Parliament, Jens-Henrik Jeppesen, Ctr. for Democracy and Tech., Sergio Carrera, Ctr. for Eur. Policy Studies, Speaking at the Ctr. for Eur. Policy Studies: A New Data Protection Compact for Europe (Jan. 28, 2014).

42 The diversion of these finite resources results in collateral damage to other privacy priorities, siphoning attention from a host of initiatives including (1) privacy education and awareness campaigns; (2) investigations and enforcement actions; (3) routine audits; (4) security breach notification response; (5) public and stakeholder consultations; and (6) the development of privacy guidance. Further, when DPAs spend a disproportionate amount of time on international data transfer issues, fewer resources are available to address other data protection issues that may pose far greater privacy risks to individuals (e.g., blacklists, biometric profiling, persistent workplace surveillance, obtrusive use of closed-circuit TV, audio recording in public places, the processing of children's personal data, and the processing of sensitive personal data (including health data)).

Several existing data transfer mechanisms have proven pragmatic in meeting business needs, offering key advantages such as lowered costs and reduced time delays. In the words of one business, "The more pragmatic or permissive data transfer regimes have allowed the company to be more nimble and reactive to changing market conditions and have allowed the company to bring programs to market at a higher speed." The U.K.'s regime, for example, offers a practical approach to regulating cross-border data transfers. In the U.K., organizations are permitted to make their own assessments of adequacy and take responsibility for ensuring adequate protections.

Accountability-based frameworks such as BCRs, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules, and the proposed European Data Protection Seals program (discussed later) represent attempts to find common ground in a changing global environment. Ideally, these frameworks could be implemented by both large and small organizations.

This section examines the approaches that appear best suited to accommodate cross-border data transfers now and in the future. These approaches should be considered by stakeholders that are involved in current initiatives to explore how cross-border transfers should be addressed globally.

Importantly, these approaches would simplify restrictions without weakening privacy safeguards by focusing on the data exporter's (1) responsibility for ensuring that individuals' rights are not diminished as a result of the transfer, and (2) liability for violations that may result from the transfer. Going forward, the discussion around cross-border data transfers should focus on data stewardship and accountability. These principles increasingly serve as the foundation for successful global privacy programs; they reflect an organizational commitment to appropriate, responsible, risk-based approaches to data protection, regardless of an organization's size.

A. Current Frameworks for Global Transfers of Personal Data

1. OECD GUIDELINES

On September 9, 2013, the OECD published revised *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, updating the original 1980 Guidelines.[43] The revised Guidelines recognize that there have been fundamental changes during the

43 Org. for Econ. Co-operation and Dev., OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, as amended by C(2013)79 (July 11, 2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last visited Apr. 22, 2014).

last three decades to the ways in which data flow across borders. The OECD's approach is based on the controller remaining responsible for personal data regardless of where the data processing occurs.

The revised *Guidelines* (1) highlight the need to enhance data protection at a global level through improved interoperability, and (2) recommend that data transfer restrictions imposed by member nations be proportionate to the associated privacy risks, taking into account the sensitivity of the personal data and the purpose and context of the data processing. If accepted by OECD member nations, the revised Guidelines could help usher in a new era in which cross-border data transfer restrictions are based on risk assessments that address individual data flows, rather than restrictions that rely on existing, country-specific adequacy assessments or overly simplistic one-size-fits-all approaches.

2. APEC CROSS-BORDER PRIVACY RULES

Building on its existing approach to cross-border data transfers, in 2012, APEC promulgated a set of Cross-Border Privacy Rules (CBPRs) meant to safeguard personal data throughout the Asia-Pacific region.[44] CBPRs were developed as a practical means of ensuring data protection across the region, notwithstanding the considerable variation in national data privacy laws and the absence of an independent regulator (and enforcement mechanism) in many APEC countries. Like the BCR framework, the CBPR system requires organizations to adopt internal privacy rules based on the nine Privacy Principles set out in the 2004 APEC Privacy Framework.[45] These internal programs are validated and overseen by APEC-recognized "Accountability Agents." Each participating economy must have its own Privacy Enforcement Authority that coordinates with the Cross-Border Privacy Enforcement Arrangement, which is an enforcement

44 In July 2012, the U.S. was approved as the first formal participant in the CBPR system. At the time, FTC Commissioner Edith Ramirez commented that, "[t]he APEC privacy rules offer the promise of significant benefits to companies, consumers and privacy regulators . . . . We hope that many more APEC economies will soon join and help realize the system's potential as a model for global interoperability among privacy regimes." Press Release, F.T.C., FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System (July 26, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/07/ftc-becomes-first-enforcement-authority-apec-cross-border-privacy (last visited Apr. 22, 2014). Mexico followed in January 2013 as the second participant.

45 *See* Asia-Pac. Econ. Cooperation, Elec. Commerce Steering Grp., APEC Privacy Framework (Nov. 2004).

network.[46] Although CBPRs currently are limited in their application, the framework's foundational principles are flexible enough to be adopted on a broader scale.

Like European BCRs, the CBPR system enables cross-border data transfers among entities in the same corporate group. Unlike BCRs, however, it also enables a data controller to transfer data to a controller or processor outside the corporate group and located in another country.

The EU's Article 29 Working Party and APEC currently are exploring interoperability between BCRs and CBPRs.[47] The two systems have obvious similarities, such as the requirements that organizations (1) adopt binding internal codes; (2) undergo a review and obtain prior approval from the relevant regulator; and (3) submit to regulatory oversight and enforcement mechanisms. The Article 29 Working Party conducted a study comparing the two systems and, in February 2014, published an opinion mapping the requirements for BCR authorization against the requirements for CBPR authorization.[48] This comparison helps organizations operating across both the EU and the APEC region compare the areas of commonality and differences between the two systems. The tool will facilitate the development of long-term strategies for global data transfers by allowing organizations to build their global privacy programs in a way that is structured to suit the implementation of both BCRs and CPBRs.

46 The CPEA aims to (1) facilitate information sharing across PE Authorities; (2) provide mechanisms to promote effective cross-border cooperation between PE Authorities; and (3) encourage information sharing and cooperation with enforcement authorities outside APEC. *See*, *e.g.*, Asia-Pac. Econ. Cooperation, Fact Sheet: APEC Cross-border Privacy Enforcement Arrangement (CPEA), *available at* http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement.aspx (last visited Apr. 22, 2014).

47 *See* Press Release, Article 29 Working Party, Promoting Cooperation on Data Transfer Systems Between Europe and the Asia-Pacific (Mar. 26, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130326_pr_apec_en.pdf (last visited Apr. 22, 2014); Press Release, APEC E-Commerce Steering Group, Promoting cooperation on data transfer systems between Europe and the Asia-Pacific (Mar. 6, 2013), *available at* http://www.apec.org/Press/News-Releases/2013/0306_data.aspx (last visited Apr. 22, 2014). *See also* Information Integrity Solutions, Towards a Truly Global Framework for Personal Information Transfers: Comparison and Assessment of EU BCR and APEC CBPR Systems (2013).

48 Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents (Feb. 27, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf (last visited Apr. 22, 2014).

3. EUROPEAN DATA PROTECTION SEALS

In the context of negotiating the Proposed EU Regulation, compromise amendments adopted by the European Parliament in October 2013 introduced the concept of a "European Data Protection Seal" (EDPS), which would permit certified organizations to transfer and receive personal data to and from other certified organizations. Like CPBRs, the EDPS would allow organizations to legally transfer personal data outside their corporate group if both the data exporter and the data importer are certified. Although an EDPS initially would require regulatory approval, it would offer a more flexible data transfer solution than many existing mechanisms, particularly because it could be used for both intra-company and third-party data transfers. Since the EDPS concept is still a work in progress, a unique opportunity exists to design a system that could be used worldwide. As the development of an EDPS progresses, it will be important to add realistic criteria for approval and a transparent decision-making process.

4. UK ADEQUACY APPROACH

Many existing national regimes already incorporate elements of an accountability-based approach, providing a useful blueprint for future cross-border data transfer frameworks. Specifically, several companies we spoke with praised the U.K.'s existing data transfer regime as offering a more practical alternative to mechanisms that require prior regulatory approval. One noted, "Ireland and the U.K. take a practical approach to data transfers, and understand that there must be a balance between data protection and the free flow of data for business." U.K. data protection laws enable data controllers to make their own adequacy findings when transferring personal data abroad, whether to a controller or to a processor and regardless of whether the recipient is within the same corporate group, provided the controllers ensure that the level of protection is "adequate in all the circumstances."[49] This type of case-by-case adequacy determination encourages a more nuanced approach than a set of standard clauses that apply in all circumstances, and it places the onus of ensuring compliance on the controller.

49 Data Protection Act, 1998, c. 29, sch. 1, (Eng.). The controller's adequacy assessment must take into account (1) the nature of the personal data being transferred, (2) the country of origin of the personal data, (3) the final destination of the personal data, (4) the purposes for which the personal data will be processed, (5) the duration of the processing, (6) the law of the recipient country, (7) the international obligations of that country, and (8) security measures.

5. OTHER FLEXIBLE SCHEMES

Several other jurisdictions regulate cross-border data transfers in a manner that provides flexibility to the data exporter while seeking to ensure the protection of data as it traverses the globe. In Mexico, for example, transfers of personal data to third parties located in foreign jurisdictions are permitted under a number of circumstances, including when the transfer is (1) to an affiliate or subsidiary of the data controller; (2) necessary to fulfill a contract with a third party; or (3) necessary for medical diagnosis, treatment or other health-related services.[50] In New Zealand, cross-border transfers of personal data are not prohibited by default (with limited exceptions) but the Privacy Act empowers the Privacy Commission to prohibit particular transfers where there are specific risks.[51] In Hong Kong, although the text of the Privacy Ordinance contains a provision that would impose cross-border transfer restrictions, this provision did not come into effect with the rest of the ordinance. Data transfers to jurisdictions outside of Hong Kong are permitted with no restriction other than the obligation generally to comply with each of the data protection principles (and the other provisions of the ordinance).[52]

B. Opportunities for International Cooperation in Trade Agreements

The ability to transfer data across borders has become inextricably intertwined with the ability to trade freely. In addition to the data transfer mechanisms discussed in this paper, current trade discussions, such as the U.S. – EU Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA), present opportunities to bridge differences among privacy regimes and developing regional data transfer mechanisms.

1. DATA TRANSFER PROVISIONS IN TRADE AGREEMENTS

Addressing cross-border data transfers through trade agreements is not a novel approach. A number of trade agreements have even acknowledged the significance of cross-border data transfers to the global economy as a fundamental tenet of the agreement. For example, Article 14.5 of the U.S.-Panama Trade Promotion Agreement

50 Ley Federal de Protección de Datos Personales en Posesión de los Particulares [Federal Law on the Protection of Personal Data Held by Private Parties], D.O., July 5, 2010 (Mex.), *available at* http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010 (last visited Apr. 22, 2014).

51 Privacy Act 1993, 1993 S.N.Z. No. 28 (N.Z.).

52 *See* Personal Data (Privacy) Ordinance, (2013) Cap. 486, (H.K.).

highlights the importance of helping small and medium-sized enterprises "overcome obstacles" that impede their participation in electronic commerce and maintaining "cross-border data flows of information as an essential element in fostering a vibrant environment for electronic commerce."[53]

Similarly, Article 15.8 of the United States-Korea Free Trade Agreement (KORUS) recognizes "the importance of the free flow of information in facilitating trade" and pushes the parties to the agreement to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[54]

In addition, the broad outline of the Trans-Pacific Partnership Agreement (TPP) addresses the free flow of information, and the final TPP is likely to include provisions aimed at preventing member countries from adopting national laws that would restrict cross-border transfers of personal data.[55] Despite these positive steps, more needs to be done to embed strong, binding commitments in future agreements.

2. THE TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP

The TTIP represents one of the best opportunities to institute cutting-edge data transfer protections, notwithstanding misplaced concern related to U.S. government surveillance issues. Ideally, the TTIP should address data transfers by including three key features: (1) a commitment to allowing cross-border data transfers; (2) a prohibition on data localization requirements; and (3) a non-exhaustive list of data transfer mechanisms. In conjunction with the third issue, the agreement should also ensure ongoing cooperation between the United States and EU with respect to developing new data transfer mechanisms. The TTIP also must meaningfully limit the transfer prohibitions

53 Trade Promotion Agreement, U.S.-Pan., art. 14.5, June 28, 2007, *available at* http://www.ustr.gov/trade-agreements/free-trade-agreements/panama-tpa/final-text (last visited Apr. 22, 2014).

54 Free Trade Agreement, U.S.-S. Kor., art. 15.8, June 30, 2007, 46 I.L.M. 642. Both the KORUS and the EU – Korea Trade Agreement (KOREU) include provisions specific to financial services, with KOREU stating "each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier." Free Trade Agreement, Eur. Union-S. Kor., art. 7.43, Aug. 20, 2010, 2010/0075 (NLE).

55 U.S. Chamber of Commerce, International Agenda, Trans-Pacific Partnership, *available at* https://www.uschamber.com/trans-pacific-partnership (last visited Apr. 22, 2014).

allowed under the General Agreement in Services (GATS) Article XIV.[56] If the United States and the EU are able to implement strong and ambitious provisions in the TTIP, that agreement may serve as a template and baseline for the TISA negotiations that will affect nearly 70% of the global economy.[57]

VIII. CONCLUSION

Cross-border data transfers are indispensable to the growth of the digitized global economy. In the words of one stakeholder, "cross-border transfer is critical for our business ... [it] is simply unavoidable, even if all of our own IT/business processes could be brought in-house and kept in a single jurisdiction." The global economy simply cannot afford to revert to digital isolationism. The question is whether governments will implement legal regimes to promote a beneficial expansion of the data economy, or if the cumbersome systems currently in place will continue in force, hindering innovation and slowing progress. The path forward must include cooperation between regulators and businesses working together to determine how best to address important concerns about privacy and data security without crippling economic growth.

Regardless of the specific geographic or political context, the following key concepts are critical to ensuring agile cross-border data transfer regimes that will facilitate the global data flows of the future:

- **Recognition that there are many different approaches to regulating cross-border data transfers, and that differing mechanisms can ensure a similar desired level of data protection.** As documented in this report, there are a variety of ways to facilitate the free flow of data while offering meaningful protection from actual privacy harms. Finding alternatives does not have to mean sacrificing safeguards. Ultimately, the areas of convergence on cross-border data transfer restrictions are more significant than the differences we currently see at the national and regional levels. Going forward, the emphasis should be on identifying

56 General Agreement on Trade in Services art. XIV, Apr. 15, 1994, 1869 U.N.T.S. 183, *available at* http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV (last visited Apr. 30, 2014).

57 Office of the U.S. Trade Representative, Notice No. 2013-21836, Participants in Trade in Services Agreement (2013), *available at* http://www.regulations.gov/#!documentDetail;D=USTR_FRDOC_0001-0270 (last visited Apr. 22, 2014).

commonalities and developing interoperable mechanisms to bridge the gaps, moving away from rigid adherence to outdated, byzantine national laws with few material differences. Greater interoperability among different privacy regimes is the most practical way forward for purposes of delivering consistent privacy protections globally.[58] To this end, current initiatives such as the exploration of interoperability between EU BCRs, APEC CBPRs and the EDPS proposed by the European Parliament should be welcomed and encouraged.

- **Movement away from rigid one-size-fits-all regulations toward more outcome-focused regimes.** The future lies in accountability frameworks that focus on actual outcomes, not prescriptive rules that often bear little relationship to practical reality. Accountability frameworks consider actual privacy harms in particular circumstances, rather than seemingly arbitrary lists of adequate and non-adequate jurisdictions that do not take relevant circumstances into account. Importantly, accountability frameworks shift the responsibility and burden of ensuring that particular data transfers are compliant away from overextended regulators. Instead, the entities transferring the data are held responsible for data protection, thereby re-allocating the risk, and the onus, to the party that derives the benefit. In developing future accountability-based frameworks, we can draw on the lessons we have learned from existing and currently proposed frameworks, such as national laws in the U.K. and elsewhere, BCRs, CPBRs, and possibly EDPSs.

- **A clear delineation between the issue of government access to data and the distinct issue of cross-border data transfers in a commercial context.**

- **Assurance that the frameworks we develop today are fit for tomorrow.** One major disadvantage of certain existing transfer regimes and mechanisms is their inability to accommodate rapid technological developments. For example, standard contractual clauses are appropriate for simple transfers from point A to point B, but they struggle to accommodate the web of transfers inherent in cloud computing models.

- **Redirecting responsibility for the protection of personal data to those who use the data.** Rules-based, prescriptive, rote frameworks can encourage "paper" compliance, to the detriment of meaningful compliance in practice.

58 *See, e.g.*, Markus Heyder, *Getting Practical and Thinking Ahead: 'Interoperability' Is Gaining Momentum*, Privacy Perspectives (Apr. 3, 2014), https://www.privacyassociation.org/privacy_perspectives/post/getting_practical_and_thinking_ahead_interoperability_is_gaining_momentum (last visited Apr. 22, 2014).

- **Implementing strong, binding trade agreement commitments that prohibit data localization requirements, support unimpeded data flows, and encourage interoperability among privacy regimes.**

As a global community, we must work toward flexible, customizable data transfer mechanisms that not only promote data protection but also are sufficiently agile to support continuing technological advances and changing business circumstances. Data privacy is not a zero-sum game. Governments, businesses, and consumers should not have to choose between privacy and economic growth when the groundwork already has been laid for a path that leads to both.

ANNEX: OVERVIEW OF DATA TRANSFER RESTRICTIONS IN KEY REGIONS

This Annex provides an overview of key regional and country-specific approaches to the regulation of cross-border data transfers around the world.

A. Europe, the Middle East and Africa

The EU Directive and each of the national implementing laws of the EU Member States contain similar, though not identical, data protection requirements. European data protection law reflects a heightened sensitivity to privacy concerns rooted in the region's experiences during World War II and its aftermath, when certain regimes persecuted citizens based on secret government dossiers. Against this backdrop, the protection of personal data came to be considered a fundamental human right that today is enshrined – separate from the right to privacy – in the EU Charter of Fundamental Rights.[59] Data protection in Europe is about more than mere rules to govern the use of personal data; it is a fundamental right that is fiercely protected and rigorously upheld. Implemented as a single market measure aimed at facilitating the free flow of information *within* the European Union, the EU Directive was not designed to enable the transfer of personal data *outside* the EU.

The EU Directive prohibits the transfer of personal data from the EU to any country outside of the European Economic Area (EEA[60]) unless (1) the European Commission has made an adequacy finding with respect to a particular country or otherwise covering the transfer (including the U.S-EU Safe Harbor framework); (2) a derogation applies, including the unambiguous consent of the individual; or (3) the data exporter in the EU can demonstrate that adequate safeguards are in place, including through the use of Commission-approved standard contractual clauses or binding corporates rules. Transparency obligations generally require data exporters to provide prior notice to individuals of intended data transfers.

Many European countries outside the EU have national data protection laws that mimic

59 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ENG (last visited Apr. 22, 2014).

60 The EEA includes the European Union Member states except Croatia, plus Iceland, Liechtenstein and Norway.

the EU Directive and contain similar data transfer restrictions.[61] European laws have heavily influenced national data protection laws across the Middle East and Africa. For example, comparisons can be drawn between Portugal's data protection law and the laws of Angola, a former Portuguese colony. Transfers of personal data outside of Angola to countries that are not considered to provide an adequate level of data protection are prohibited, subject to exemptions similar to those found in EU law, including (1) with the individual's consent; (2) to protect important public interests; and (3) where the recipient can ensure an adequate level of protection.

Other regimes across the region have their own frameworks, including the following:

- ***Azerbaijan:*** Both domestic and international data transfers require the individual's written consent, and transfers of personal data outside of Azerbaijan are prohibited where the recipient country does not provide an equivalent level of data protection as that provided by Azerbaijani law, or where the transfer would pose a threat to national security.

- ***Dubai International Financial Centre:*** Transfers outside the Dubai International Financial Centre are prohibited unless the recipient country has been deemed by the Commissioner of Data Protection to provide an adequate level of data protection. Transfers to non-adequate countries are permitted in limited circumstances, including with the individual's written consent or with a permit granted by the Commissioner.

- ***Israel:*** Transfers are prohibited except (1) to EU Member States; (2) from an Israeli company to its foreign subsidiaries; (3) with the individual's consent; or (4) where the data importer enters into a written agreement requiring it to substantially comply with Israeli data protection law.

- ***Russia:*** Transfers of personal data outside of Russia require the consent of the individual. For transfers to jurisdictions deemed adequate (including the signatories to the Council of Europe Convention 108), written consent is not required. For transfers to jurisdictions that are not deemed adequate, the individual's consent must be in writing.

61 For example, data transfer restrictions under Ukrainian law strongly resemble EU restrictions. Transfers of personal data outside of Ukraine are permitted only where (1) the recipient country provides an adequate level of data protection (which includes all EEA countries and all countries that are signatories to the Council of Europe Convention 108), or (2) a derogation applies, including where the individual consents to the transfer, where the transfer is necessary to protect the vital interests of the individual or the public interest, or to establish or support legal claims.

South Africa: In 2013, the South African Parliament passed the Protection of Personal Information Act (the POPIA). Under the POPIA, an organization cannot transfer personal data outside of South Africa unless (1) the recipient is subject to a law, binding code of conduct or contract that imposes principles substantially similar to those contained in the POPIA and includes a requirement to impose the same transfer restrictions in the case of onward transfers; (2) a derogation applies (e.g., consent of the individual); or (3) the transfer is necessary to enter into a contract with the individual or for the individual's benefit.

B. The Americas

Privacy laws across the Americas fall into two broad groups: EU-style omnibus privacy laws in Latin America and Canada and a patchwork of sectoral laws in the United States.

In the United States, privacy laws do not contain cross-border data transfer restrictions. Unlike in the EU, the United States has no privacy law and no overarching scheme regarding the transfer of personal data outside of the country. Federal and state privacy laws in the United States generally focus on specific types of information (e.g., credit reporting data[62] or children's personal information[63]) or apply to specific industries (e.g., financial services[64] or health care[65]). Privacy laws in the United States are neutral as to the geography of the data recipient. Certain rules, however, impose significant restrictions (and protections) on the disclosure of personal data.[66] For entities doing business in the United States, restrictions placed on the transfer of personal data from the United States to other jurisdictions generally are a matter of contract.

In Canada, although the federal private-sector privacy law (the Personal Information Protection and Electronic Documents Act, or PIPEDA) does not generally restrict cross-border exports of personal data, organizations remain responsible for the protection of personal data in their control even after a transfer outside of the jurisdiction. Certain Canadian provincial statutes contain explicit data transfer restrictions. For example,

62 *See* Fair Credit Reporting Act, 15 U.S.C.A. § 1681(a)-(b) (West 2007 & Supp. 2009).

63 *See* Children's Online Privacy Protection Act, 15 U.S.C.A. §§ 6501–6508 (2001).

64 *See* Gramm-Leach-Bliley Act (GLBA), 115 U.S.C.A. §§ 6801–6809 (West Supp. 2009).

65 *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, 110 Stat. 1936 (1996).

66 Two examples of such rules are the HIPAA Privacy Rule and the GLBA Privacy Rule. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164); Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (May 24, 2000) (codified at 16 C.F.R. pt. 313).

Alberta's Personal Information Protection Act requires data exporters in Alberta to provide specific notice to individuals of the use of foreign-based service providers, and Quebec's Privacy Act generally requires data exporters in Quebec to take steps to ensure that personal data are not processed by foreign-based service providers other than as directed by the data exporter, or disclosed to third parties without the consent of the individual.

In Latin America, EU-style laws often contain requirements that are similar to, or even stricter than, those found in the EU Directive. Examples are as follows:

- ***Argentina:*** The Argentinian Personal Data Protection Act prohibits the transfer of personal data to countries or international entities that do not provide an adequate level of data protection. There are limited exceptions, including (1) transfers required for international judicial cooperation or between law enforcement or intelligence agencies; (2) the exchange of medical information necessary for treatment; (3) stock exchange or banking transfers; and (4) transfers made pursuant to international treaties.

- ***Brazil:*** In 2011, the Brazilian Congress introduced the Marco Civil da Internet, a draft bill to establish the country's first set of Internet regulations, including provisions regarding personal data protection. Following the 2013 revelations regarding U.S. government surveillance, the Brazilian government introduced new amendments to the bill, including a requirement that companies store any type of Brazilian data on servers physically located in Brazil. This provision generated significant controversy and opposition, and ultimately the localization requirements were removed from the bill.

- ***Colombia:*** Cross-border transfers generally require the individual's consent, with limited exceptions, such as transfers (1) to protect the public interest; (2) to protect health and public hygiene; and (3) of financial information made in connection with banking operations and in accordance with applicable legislation.

- ***Mexico:*** Mexico has adopted an accountability model containing multiple exceptions to the requirement to obtain consent for cross-border transfers of personal data, including where the transfer (1) is made between entities within the same corporate group, operating under common internal policies and procedures; (2) is necessary under a contract executed, or to be executed, in the interests of the individual; or (3) is necessary to maintain or fulfill a legal relationship between the individual and the data exporter (e.g., in the employment context). Specific

regulations governing processing in the cloud context permit data exporters to transfer personal data outside of Mexico to cloud computing service providers subject to specific safeguards, including a requirement that the relevant cloud provider has policies and procedures similar to those contemplated by Mexican data protection law and is required to maintain the confidentiality of the personal data. Further, the data exporter must provide notice of the fact that it uses third parties to process the personal data.

Peru: Cross-border transfers are permitted only where the recipient country provides an adequate level of data protection or the recipient entity otherwise guarantees that the personal data will be processed in accordance with the requirements of Peruvian data protection law.

Asia-Pacific

Data transfer restrictions across the Asia-Pacific region vary, reflecting the different legal and cultural traditions of each individual jurisdiction. A number of former European colonies, for example, have implemented EU-style transfer restrictions:

- ***India:*** cross-border transfers are permitted where (1) the recipient jurisdiction provides an equivalent level of data protection to that contained in India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules; (2) the transfer is necessary for the performance of a contract between the data recipient and the individual; or (3) the transfer is made with the individual's consent. Prior written consent is required to transfer sensitive personal data.

- ***Malaysia:*** Cross-border transfers are prohibited unless (1) the recipient jurisdiction has been approved by the Minister; (2) the individual provides consent; or (3) another exemption applies, including where the data exporter has taken reasonable steps to ensure that the personal data will not be processed in a manner that violates Malaysia's Personal Data Protection Act.

- ***Singapore:*** Pursuant to Singapore's new data protection law (which will become effective on July 2, 2014), cross-border transfers generally are prohibited unless they are conducted in compliance with rules that have not yet been adopted. The rules would seek to ensure that the transferred data would be subject to a standard of protection that is comparable to that provided under the new Singaporean law. The rules are intended to be flexible to accommodate technological, legal, and commercial developments.

Some Asian jurisdictions have adopted restrictive, consent-based models. For example:

- ***Indonesia:*** Indonesia does not have an omnibus privacy law imposing data transfer restrictions. Law No. 11 of 2008 and Regulation No. 82 of 2012 (which regulate organizations collecting, processing, analyzing, storing or disclosing electronic data), however, require providers of services to the public to maintain their data centers and recovery centers within Indonesia.

- ***Japan:*** Although there are no specific restrictions on the transfer of personal data outside of Japan, the Personal Information Protection Act does restrict data disclosures generally (whether domestic or cross-border). These restrictions generally require the individual's consent to disclose his or her personal data unless certain exemptions apply, such as where (1) the disclosure is required by law or is necessary to protect an individual's life, or (2) the individual has been provided detailed information about the transfer and has been given the option to stop the transfer.

- ***South Korea:*** Pursuant to the Data Protection Act of Korea, transfers of personal data outside of South Korea are permitted only with the informed consent of the individual, who must be provided with detailed notice of the intended transfer, including the personal data that will be transferred, the recipient country, the date of the transfer, the name of the recipient organization, and the method and purpose of the transfer. Under the Protection and Use of Credit Information Law, foreign companies operating in South Korea are prohibited from transferring any credit information outside of the jurisdiction, including intra-group transfers to affiliated entities.

In Far East Asian countries, where cultural traditions historically have emphasized social cohesion over individual privacy, there often are no restrictions, or only limited restrictions, on cross-border transfers of personal data:

- ***People's Republic of China:*** Cross-border data transfers generally are not prohibited, although sector-specific restrictions prohibit the transfer of personal financial and credit reference information outside of the jurisdiction.

- ***Hong Kong:*** Although the text of the local privacy ordinance contains a provision that would impose a cross-border transfer restriction, this provision did not come into effect with the rest of the ordinance. Data transfers to jurisdictions outside of Hong Kong are permitted with no restriction other than the obligation to

comply with each of the data protection principles (and the other provisions of the ordinance) generally.

- ***Taiwan:*** Transfers generally are not prohibited, but central government authorities are empowered to restrict certain transfers for specific reasons, including where the purpose of the transfer is to evade restrictions imposed by the Personal Data Protection Act or where the transfer would involve material national interests. Since 2012, a blanket order prohibits the transfer of telecommunications subscribers' communications data from Taiwan to the People's Republic of China.

Australia, New Zealand, and the Philippines have adopted accountability models in shaping their data protection regimes, as follows:

- ***Australia:*** Organizations transferring personal data abroad must take reasonable steps to ensure that the overseas recipient does not violate the Australian Privacy Principles (APPs). The data exporter remains responsible for violations by the recipient entity unless an exemption applies, including if (1) the data exporter reasonably believes the recipient is subject to a law or binding scheme that provides a similar level of protection as the APPS and enables individuals to enforce that law or binding scheme, or (2) the disclosure is required or authorized by Australian law or court order.

- ***New Zealand:*** Transfers generally are not prohibited, but the Privacy Commissioner is empowered to prohibit a cross-border transfer if the Commissioner determines that: (1) the information is received in New Zealand from another country and is likely to be transferred to a third country where it will not be subject to a law providing safeguards comparable to those contained in the Privacy Act, and (2) the transfer likely would violate the basic principles of the Organization for Economic Cooperation and Development (OECD) Guidelines.

- ***Philippines:*** The Data Privacy Act 2012 does not impose any specific restrictions on cross-border data transfers. Instead, data exporter entities are responsible for complying with the Act's requirements, including ensuring that third-party processors, whether domestic or foreign, provide a comparable level of protection as required under the Act.

U.S. CHAMBER OF COMMERCE

1615 H Street, NW | Washington, DC 20062-2000
www.uschamber.com