SIIA ISSUE BRIEF

DATA FLOW PROMOTION IN INTERNATIONAL AGREEMENTS AND NATIONAL LAWS

DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

TABLE OF CONTENTS

Introduction

This Issue Brief focusses on describing international agreements and national laws that promote cross-border data flows. There is a web of agreements being built up around the world that provide for binding data flow obligations coupled with a respect for data privacy and other public policy issues. There are also countries and economies that have adopted detailed and, in some cases, strict, data privacy and data use, laws and regulations but that still permit cross-border data flows. This Brief describes some of those laws as well. SIIA considers that these agreements and national laws potentially provide templates for policymakers as they consider how to address public policy issues stemming from data-driven innovation, while at the same time maximizing the economic benefits arising from that innovation by not only permitting, but also encouraging, cross-border data flows. The following examples of frameworks for cross-border data flows are discussed in this paper.

- The U.S. Mexico Canada Agreement (USMCA)
- The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
- APEC Cross-Border Privacy Rules (CBPR) System
- The General Data Protection Regulation (GDPR)
- The EU-U.S. Privacy Shield
- Japan Privacy Law
- EU-Japan Free Trade Agreement
- Brazil Privacy Law and Internet Framework Law

THE MEANING OF CROSS-BORDER DATA FLOWS, AND WHY THEY ARE FRAMED BOTH AS A POSITIVE OBLIGATION TO PERMIT FLOWS AND A PROHIBITION ON DATA LOCALIZATION

Cross-border data flows means two things in this context. First, the ability to transfer data (personal or non-personal) across borders. Second, the ability to store and/or process data locally or internationally. Modern digital trade chapters normally describe this provision as an obligation not to mandate the use of local computing facilities. Both of these obligations are needed in trade agreements because a country could permit cross-border data flows but still mandate local data storage and/or processing, thereby effectively reducing the value of permitting cross-border data flows. For example, some countries require that copies of data stay within their nations even though the data is also moved abroad for processing and storage there.

CROSS-BORDER DATA FLOW ECONOMIC CONSIDERATIONS

SIIA's long-standing position has been and continues to be that governments should permit, indeed even encourage cross-border data flows. This is because realizing the full economic potential of data-driven innovation depends, in part, on permitting cross-border data flows. A lot is at stake. For instance, the McKinsey Global Institute estimated that in 2014, global data flows raised global GDP by $2.8 trillion.[1]

With respect to the national downsides of data localization, the European Center for International Political Economy (ECIPE) put out a report in 2014 estimating GDP costs of proposed or enacted data localization laws in Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%), and Vietnam (-1.7%).[2] (Note: ECIPE probably underestimated the costs to India given that country's recently proposed restrictive data privacy law. On the other hand, ECIPE probably overestimated the cost to Brazil given that the county in the end opted to impose less significant cross-border data flow restrictions than originally envisaged.) At the firm level, the Leviathan Security Group has calculated that companies in many countries would be required to pay 30% to 60% more for their computing needs if they operated in nations with data localization laws and/or regulations.[3]

Despite, the well-known costs of data localization, countries around the world are imposing data localization laws and rules. The Information Technology & Innovation Foundation released a report in 2017 with information on data localization barriers around the world.[4] China leads the trend in data localization requirements, but other economies such as India, Indonesia, Nigeria, and Russia are moving in this direction as well. Nonetheless, there are significant countertrends, which this Issue Brief discusses below.

CROSS-BORDER DATA FLOW CYBERSECURITY CONSIDERATIONS

Beyond economics, many countries impose data localization laws ostensibly to improve cybersecurity. However, there is no relationship between cybersecurity and data localization. The Consultative Group to Assist the Poor (CGAP) observes that data security is not a matter of physical location but of security processes; regulatory access to data depends more on system uptime and processing standards, rather than where it is stored; and, data localization can hamper the ability of developing country SMEs from exporting their services.[5]

A number of companies operate a network of data centers designed for a global infrastructure and cannot easily be disaggregated or detached from that global network. For instance, Google explains in a White Paper how its global scale technical infrastructure is designed to provide security through the entire information processing lifecycle.[6]

The company's cloud-based security and risk assessment tools are premised on the ability to share and analyze data on a global basis.[7] A global database enables Google to compare patterns of activity, find anomalies, and detect common vulnerabilities across different geographies and attack vectors. At many points across Google's global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections.[8] When suspicious behavior or vulnerabilities are detected, the firm seeks to respond and patch these vulnerabilities globally.

Google also relies upon distributed storage across a global technical infrastructure to prevent data loss, corruption, and outages, as the company's head of technical infrastructure, Urs Hölzle, has explained.[9] The company breaks up individual data files into smaller pieces and replicates data seamlessly between data centers and across borders in order to protect the integrity of the data and maximize efficiency and security for users.

The global nature of Google's technical infrastructure enables it to automatically and instantly shift platform services and control planes from one facility to another in the event of hardware, software, or network failure. This highly redundant design has allowed Google to achieve an uptime of 99.984% for

services like Gmail with no scheduled downtime. This level of security and reliability is a key market differentiator, and it depends on global and distributed storage and processing solutions. More detail can be found in a security white paper.[10]

Finally, Google certifies its infrastructure against a wide variety of regional and global (ISO) standards.[11] It is possible that the firm's ability to meet these high standards could be compromised if it were inhibited from leveraging its global infrastructure to protect and secure data.

This issue is much broader than just one company. Again, CGAP recently explained why data localization inhibits modern risk detection and fraud prevention efforts by financial service providers (FSPs):[12]

> *"International cloud and payment systems providers can support local FSPs with far more extensive security accreditations and certifications. Since security is part of cloud providers' core business and value proposition, they can invest more money in security and keep up with ever-changing cyber threats better than small FSPs. Moreover, hackers behave similarly across the world. Leveraging access to a global database of fraud patterns and suspicious transactions can significantly improve fraud risk management and potentially support compliance with international anti-money laundering/combating the financing of terrorism (AML/CFT) rules."*

THE UNITED STATES MEXICO CANADA AGREEMENT (USMCA)

The September 30, 2018 USMCA is the most recent and most ambitious trade agreement with respect to digital trade in general.[13] Chapter 19 is the Digital Trade Chapter. Article 19.11 entitled "Cross-Border Transfer of Information by Electronic Means" says that USMCA countries cannot prohibit or restrict "the cross-border transfer of information, including personal information." Parties are permitted to adopt exceptions to this rule to achieve legitimate public policy objectives. However, this is cabined through standard trade law in that the exceptions may not be arbitrary or discriminatory and the restrictions on information flows may not be greater than necessary to achieve the objective. Article 19.12 prohibits a requirement "to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

The data flow/localization rules described above are robust but cabined with the possibility for exceptions based on standard trade law safeguards. At the same time, like in the Trans-Pacific Partnership (TPP – discussed below), there is also a binding requirement in Article 19.8 entitled "Personal Information Protection" for Parties to have some kind of legal framework for data privacy. There is a reference to international examples of privacy protection such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. This is consistent with the TPP's rules. The USMCA goes further than TPP in that it specifies "key principles" for data collection. They include "limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and, accountability."

Article 19.8 also recognizes the importance of ensuring compliance with data privacy rules while also ensuring that that restrictions on cross-border data flows are necessary and proportionate "to the risks presented." This language is consistent with SIIA's view that domestic privacy laws/regulations should be risk-based. And of course, domestic law/regulation has an impact on what countries can agree to internationally. There is some recognition that "risk" or "harm" should be a component of domestic rules

or, at a minimum, influence the interpretation of the rules. For example, Irish Data Protection Commissioner notes that the General Data Protection Regulation (GDPR) "fails to make it easier for data protection authorities to prioritize complaints based on the severity of the alleged abuse." This is why she argues that "common sense" should guide interpretation of the GDPR.[14] The recognition of risk as a component in determining whether restrictions on cross-border data flows are necessary and proportionate is an important contribution that USMCA makes to global digital trade architecture.

Another important USMCA contribution is that it recognizes that the "APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information." This is significant given that other mechanisms for cross-border data flows such as adequacy determinations, standard contractual clauses, and the EU-US Privacy Shield, while constructive, are also relatively inflexible and sometimes expensive. The APEC system establishes minimum standards for data protection but does not replace national law or require an APEC member to issue adequacy assessments of other APEC economies. Fundamentally, this is why the APEC system is more flexible than other cross-border data flow interoperability mechanisms. It is important to highlight in this context that this is not a "get out of jail card" for participating companies. This is because once a firm is certified under the APEC CBPR system, it becomes enforceable against that company. And again, adherence to the APEC CBPR system for the purpose of data flows between the United States, Mexico, and Canada does not require uniform privacy laws and regulations. But the USMCA's 19.14, appropriately, does contemplate cooperation between the Parties on privacy matters. One suggestion is to establish a "North American Privacy Forum" for regulators and government officials from the United States, Mexico, and Canada. Should a U.S.-Japan FTA be created, such a Forum could be extended to Japan as well.[15]

Importantly, financial data are included in the USMCA's cross-border data flow obligations. The Trans-Pacific Partnership agreement had specifically excluded financial data at the request of the United States. This was because U.S. financial regulators were concerned about having real-time access to data in order to fulfill their regulatory responsibilities. However, USMCA includes financial data through Article 17:19 entitled "Transfer of Information" and Article 17:20 entitled "Location of Computing Facilities."[16] Article 17:19 articulates the basic obligation to permit cross-border flows of financial data, but it allows Parties to adopt or maintain measures to protect personal data "provided that such measures are not used to circumvent the commitments obligations of this Article." Article 17:20 recognizes that financial regulatory authorities need to have "immediate, direct, complete and ongoing access" to financial data. However, as long as regulators have that access, they are not permitted to mandate data localization. Moreover, if the data is not immediately available, "to the extent practicable," companies are to be given a "reasonable opportunity to remediate a lack of access to information" before imposing a data localization requirement. This is a reasonable compromise in that it permits companies to take advantage of the economic benefits of organizing their data processing operations in the most efficient possible way. At the same time though, firms are put on notice that if they do not cooperate in good faith with financial regulators, they could face a data localization requirement.

THE COMPREHENSIVE AND PROGRESSIVE AGREEMENT FOR TRANS-PACIFIC PARTNERSHIP (CPTPP – ALSO KNOWN AS TPP11 OR TPP-11)

The CPTPP is a trade agreement including Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam. The agreement was signed in Santiago, Chile on March 8, 2018. It will enter into effect when six out of the eleven countries ratify it. As of July 18, 2018, three countries had ratified the CPTPP. The CPTPP was originally the Trans-Pacific Partnership (TPP) when the United

States planned to join. The CPTPP countries decided to adopt the original TPP text with a few exceptions, mostly in the intellectual property and investment areas. However, these provisions were "suspended," not eliminated because many TPP countries hope that the United States will rejoin TPP. So, to understand the CPTPP, it is necessary to review the original TPP text[17], the suspended provisions in CPTPP,[18] and CPTPP side agreements.

Although the side agreement on cybersecurity with Vietnam (see below for detail) is negative from a data flows standpoint, the fact that 10 out of the 11 CPTPP countries chose to apply Chapter 14 in its entirety is highly significant and positive with respect to building a modern global trading system fit for the digital era. This is an underappreciated fact about the CPTPP so it is important to understand what the provisions of Chapter 14 are.[19]

- Article 14.1 provides for definitions.
- Article 14.2 describes the Chapter's scope and general provisions, including that government procurement and government data is not covered. (Note: The USMCA also does not include government procurement. However, with respect to government data, "open government data," is subject to the USMCA's requirements).
- Article 14.3 says that customs duties may not be imposed on data flows, although internal taxes may be charged as long as they are imposed in a manner consistent with the Agreement.
- Article 14.4 provides for non-discriminatory treatment of digital products.
- Article 14.5 obliges Parties to have legal framework governing electronic transactions.
- Article 14.6 lays out rules for accepting electronic authentication and electronic signatures.
- Article 14.7 obliges Parties to adopt or maintain consumer protection laws.
- Article 14.8 obliges Parties to have a legal framework to protect personal information and encourages Parties to adopt interoperability mechanisms to facilitate cross-border data flows. Footnote 6 recognizes that Parties can have general privacy laws [such as the EU's GDPR] or sectoral systems [such as the U.S. system]. The TPP is the first trade agreement to oblige its members to have personal information protection laws.
- Article 14.9 says that Parties should make trade administration documents available electronically and accept electronic trade documents as legally equivalent to paper versions.
- Article 14.10 lays out principles for consumer Internet access.
- Article 14.11 provides for the binding cross-border data flow obligation. Exceptions are permitted subject to standard trade law concepts such as arbitrariness, discrimination, disguised restrictions on trade, and proportionality.
- Article 14.12 says that suppliers seeking international Internet connections should be able to negotiate with suppliers in another Party on a commercial basis.
- Article 14.13 says that Parties cannot require the use or location of computing facilities in their countries. Exceptions are permitted based on standard trade law.
- Article 14.14 lays out requirements for suppliers of unsolicited electronic messages.
- Article 14.15 says that Parties "shall endeavor" to work together to overcome obstacles to e-commerce, especially for SMEs.
- Article 14.16 recognizes the importance of cybersecurity cooperation. (Note: The USMCA adds that risk-based cybersecurity approaches may be more effective than prescriptive ones.)
- Article 14.17 says that Parties may not require that source code be turned over as a condition for use in their territories. However, the obligation does not include software for critical infrastructure, which is not defined. (Note: The USMCA includes algorithms in the commitment and there is no exception for critical infrastructure. However, regulators or courts can get access

to source code or algorithms subject to specific investigations as long as there are safeguards against unauthorized disclosures.)
- Article 14.8 lays out rules for dispute settlement.

From a cross-border data flows standpoint, it is also necessary to review CPTPP side agreements. The relevant side agreement from the standpoint of cross-border data flows and data localization is the side letter that Vietnam signed with the other CPTPP countries to suspend for five years dispute settlement with respect to the TPP's cross-border data flow obligations (14.11) and prohibition on mandatory localization of computing facilities (14.13).[20] The TPP's Article 14.8 had given Vietnam a two-year suspension period. The result of this exception is that Vietnam is mandating data localization and prohibitions on cross-border data flows.

Again though, taken together, the CPTPP's cross-border data flow obligations and prohibitions against data localization (in the sense of either mandating the use of local computing facilities or the construction of local computing facilities as a condition for doing business) are important. Their significance is magnified by the fact that the CPTPP includes large and small high-income economies (Australia, Brunei, Canada, Japan, New Zealand, and Singapore), as well as large and small medium-income economies (Chile, Malaysia, and Peru). Vietnam is on the low end of the middle-income space but is growing quickly and in five years will be subject to the cross-border data flow obligations. For the time being, however, Vietnam is one of the most important breaks on cross-border data flows with a cyber security law coming into effect on January 1, 2019 that mandates local data storage and even opening offices in order to process data.

THE ASIA-PACIFIC ECONOMIC COOPERATION (APEC) CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

The APEC system was established with the intent to facilitate cross-border data flows while creating meaningful privacy protections at the same time. In order for APEC countries and companies to accede to the system, they must adhere to the APEC Privacy Framework.[21] So far, the United States, Mexico, Japan, Canada, Singapore, and Korea have acceded to the CBPR system. It is worthwhile noting that the Framework is associated with all 21 APEC economies, which include Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Vietnam. Some of these countries have domestic policies, which are strongly at variance with the Framework's basic idea, which is to promote "a flexible approach to information privacy protection across APEC member economies, while avoiding the unnecessary creation of unnecessary barriers to information flows." Nonetheless, it is worthwhile noting that APEC Ministers endorsed the Framework in December 2005.[22]

The Framework enumerates information privacy principles. See below for those principles.

- *Preventing Harm*. The idea is that privacy protection should be designed to prevent harm to individuals and should be proportionate to the potential harm in question. This is the most important principle in the Framework. Moreover, it can be applied in ways possibly not foreseen in the Framework. For instance, a potential criticism of the APEC Privacy Framework is that it does not include rules on data breach. However, the harm principle can and should be applied to data breach law and regulation. In practical terms that could mean, for example, limiting notifications to situations were persons could suffer discernible harm stemming from a data breach.

- *Notice*. This principle is consistent with privacy laws around the world in that it calls for "clear and easily accessible statements" with respect to personal information. Importantly, it diverges somewhat from the General Data Protection Regulation (GDPR) and the proposed California Data Privacy Act (CDPA) in that it says: "It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information." This is constructive in that the use of publicly available information is often needed for companies to be able to provide, for example, know-your-customer (KYC), anti-money laundering, anti-corruption, anti-terrorism finance, and other important services.
- *Collection Limitation*. Limits collection and says that information should be obtained by lawful and "fair means," which provides flexibility for member economies to determine collection rules.
- *Uses of Personal Information*. This is consistent with rules around the world which limit use to the purposes at the time of collection, although uses can be expanded if companies obtain consent.
- *Choice*. Individuals should be provided with "clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information." Importantly, and correctly in in SIIA's view, the APEC Privacy Framework notes that these mechanisms may not be appropriate with respect to the collection of publicly available information.
- *Integrity of Personal Information*. The idea here is that a personal information controller is obliged to maintain the accuracy and completeness of records to the extent necessary for the purposes of the use of the data.
- *Security Safeguards*. The principle recognizes the responsibility that personal information controllers have to secure the data. Importantly, the principle notes that the safeguards should be "proportional to likelihood and severity of the harm threatened."
- *Access and Correction*. This is one of the most interesting principles in that it articulates rights that individuals should have, including the ability to "challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted."
- *Accountability*. This sets out the important principle that personal information controllers should be accountable for following the principles and that consent is needed if information is transferred domestically or internationally. Without specifying like the GDPR does that a contract is needed, the principles specify that information controllers should "take reasonable steps to ensure" that the personal data recipients protect the personal data consistently with the principles.

As mentioned above, six countries have acceded to the CBPR system. The APEC CBPR system is voluntary both for countries and companies. However, if a firm obtains a CBPR seal from an accountability agent, the commitments it undertakes are enforceable against it. Individuals can complain to the accountability agent that has certified a company to verify that it is living up to its commitments. There is also the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement (CPEA).[23] The CPEA creates a framework for regional cooperation in the enforcement of privacy laws. Most importantly, it aims to "provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of Privacy law."[24] The CPEA Administrators are the U.S. Federal Trade Commission and the Personal Information Protection Commission of Japan. In addition, there are 27 participating CPEA participants.

Currently, there are 23 companies that are APEC CBPR certified.[25] This is a relatively small number of companies, which reflects the arguably weak value proposition for becoming certified. After all,

certification does not eliminate the obligation to comply with local privacy laws; certification has no effect for the same company in distinct APEC economies; certification does not per se authorize cross-border data flows; and, while adopting the CBPR system gets a company partially towards EU interoperability, it does not get a firm all the way.[26] The "referential" with the EU is a useful tool demonstrating where the CBPR system overlaps with EU Binding Corporate Rules (BCRs), but the referential itself does not allow for cross-border data flows. However, as more economies participate in the system, that should incentivize more companies to participate in the system, thereby raising privacy protection standards throughout the APEC region and providing regulators with a common tool they can hold participating companies accountable for.

Although not conducted specifically for APEC, it is worthwhile noting that, recently, the non-governmental Asian Business Law Institute issued 14 Asian country reports on the regulation of cross-border data flows and data localization in Australia, China, Hong Kong SAR, India, Indonesia, South Korea, Macau SAR, Malaysia, New Zealand, the Philippines, Singapore, Thailand, and Vietnam.[27] While a number of these jurisdictions, notably China, Indonesia, and Vietnam, are, in reality, restrictive when it comes to data flows, it is still noteworthy that these nations (even through non-government legal associations with some not so independent from their governments) participated in a project where the ultimate goal is to build "a shared legal ecosystem for cross-border data transfers in Asia."[28] Some of the countries in this group, for instance Australia, South Korea, and Singapore, have committed to cross-border data flows and prohibitions against data localization so they potentially constitute a pro cross-border data flows sub-group of legal scholars attempting to develop an Asian shared ecosystem for data transfers.

THE GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is an umbrella privacy law[29] directly applicable in all the EU's 28 member states (the UK will apply the GDPR even after it departs the EU). While SIIA questions whether the law will stimulate the degree of innovation its proponents assert it will, the GDPR is indisputably one of the world's most influential privacy laws. SIIA's suggestions for how the GDPR could be made better were laid out in a May 24, 2018 article.[30] SIIA member companies are committed to complying with the law. SIIA itself is subject to the GDPR and changed privacy policies upon entry-into-force of the law.

The GDPR's rules with respect to cross-border data flows are in the GDPR's Chapter 5 entitled: "Transfers of personal data to third countries or international organisations."[31] The key thing to understand is that while the GDPR imposes strict requirements on companies, the Regulation does permit cross-border transfers of personal data subject to certain safeguards. Derogations from those safeguards allowing for cross-border data flows, including consent, are also possible. **So, it should be emphasized that the GDPR actually provides for a menu of options to make cross-border data flows possible. And, in fact, the GDPR itself acknowledges the economic desirability of cross-border data flows.**

Article 44 entitled "General principle for transfers" notes that transfers are possible only if the conditions in Chapter 5 are complied with by the controller and processor. Recital 101 recognizes that flows of personal data are "necessary for the expansion of international trade and international cooperation," but notes that transfers must conducted in compliance with the Regulation. Recital 102 notes that the Regulation does not affect international agreements concluded by the EU and third

countries regulating personal data transfers. (Note: For example, the EU-US Privacy Shield's rules with respect to data transfers are valid.)

Article 45 entitled "Transfers on the basis of an adequacy decision" notes that the Commission has the authority to determine whether a "third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection" to permit cross-border data flows. The Article lays out criteria that the Commission must take into account when making an adequacy determination. Recitals 103-107 provide additional information with respect to this possibility.

Article 46 entitled "Transfers subject to appropriate safeguards" notes that in the absence of an adequacy determination, transfers can still take place as long as the controller or processor provides appropriate safeguards. There are a variety of options, including enforceable instruments between public authorities; binding corporate rules; standard data protection clauses; approved codes of conduct; and/or approved certification mechanisms. Recitals 108-109 provide additional information on these possibilities.

Article 47 entitled "Binding corporate rules" (BCRs) lays out how companies can obtain such rules. BCRs are approved by Data Protection Authorities (DPAs) and are for cross-border data flows within multinational companies. BCRs must be "legally binding" and "expressly confer enforceable rights on data subjects with regard to the processing of their personal data."

Article 48 entitled "Transfers or disclosures not authorized by Union law" says that courts or administrative bodies in third countries can only require transfers of EU PII data subject to an international agreement such as a mutual legal assistance treaty. Recital 115 says that third country "laws, regulations and other legal acts" requiring transfers of personal data could be extraterritorial. The Recital says that transfers should only be allowed "where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject."

Article 49 entitled "Derogations for specific situations" permits cross-border data flows in certain circumstances even when the safeguards described above are not in place. These conditions include explicit consent; the transfer is necessary for the performance of a contract; public interest; the transfer is needed to establish legal claims; the transfer is needed to protect the vital interests of the data subject; and, the transfer is made from a register which according to Union or Member State law is intended to provide information to the public. (Note: The last exception demonstrates the importance the EU attaches to the ability to use public records.) Recitals 111-115 provide additional information on how derogations work.

Article 50 entitled "International cooperation for the protection of personal data" directs the Commission and Data Protection Authorities to work internationally to protect personal data. Recital 116 provides more explanation for why Data Protection Authorities should cooperate internationally.

THE EU-U.S. PRIVACY SHIELD

The Privacy Shield is the world's most important cross-border data flow agreement in terms of the number of participating companies by far. There are currently 3838 companies that participate in the Shield. Most participating companies are U.S.-based and use the Shield to transfer data legally

from the EU to the United States. There are also some Europe-based firms that use the Shield to transfer data. The European Commission adopted an adequacy decision on July 12, 2016 regarding the Shield.[32] The U.S. Department of Commerce administers the program and the U.S. Federal Trade Commission enforces the Shield.[33]

The Privacy Shield is called a "Framework" and that is accurate because it is really a series of agreements and commitments between the United States and the European Union. The Shield is composed of the following elements.[34]

- EU-U.S. Privacy Shield Principles
- EU-U.S. Privacy Shield Supplemental Principles
- EU-U.S. Annex I (Binding Arbitration)
- Letter from Secretary of Commerce, Penny Pritzker, transmitting the Privacy Shield Package
- Letter from the Commerce Department International Trade Administration describing its administration and oversight of the Privacy Shield
- Letter and accompanying attachment from the Federal Trade Commission describing its enforcement of the Privacy Shield
- Letter from the Department of Transportation describing its enforcement of the Privacy Shield
- Letter from the Department of State and accompanying memorandum describing a new Privacy Shield Ombudsperson for submission of inquiries regarding U.S. signals intelligence practices
- Letters prepared by the U.S. Office of the Director of National Intelligence regarding safeguards and limitations applicable to U.S. national security authorities
- Letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes

The Framework is a first in global cross-border data flow governance because besides the obligations of companies that self-certify under the Shield, the U.S. government also provided explanations regarding its surveillance practices. Moreover, the Ombudsperson mechanism provides for a mechanism available to EU citizens in the event that they have questions regarding U.S. surveillance practices.

Passage in 2015 of the Judicial Redress Act[35], legislation that SIIA advocated for, which gave the U.S. government the authority to permit citizens from designated countries or regional economic integration organizations such as the EU to enjoy the same redress rights under the Privacy Act as U.S. citizens, solidified EU political support for the Privacy Shield. On January 17, 2017, the U.S. Attorney General designated 26 countries and the EU as "covered countries" so citizens from those nations do, in fact, enjoy redress options enjoyed by U.S. citizens under the Privacy Act.[36]

American companies find the Privacy Shield advantageous because it is relatively inexpensive to join, administered by the Commerce Department, and enforced by the FTC. But Privacy Shield firms do undertake significant commitments which are encapsulated in the Principles and Supplemental Principles briefly mentioned below.

<u>EU-U.S. Privacy Shield Principles</u>

- Notice
- Choice
- Accountability for Onward Transfer

- Security
- Data Integrity and Purpose Limitation
- Recourse, Enforcement and Liability

EU-U.S. Privacy Shield Supplemental Principles

- Sensitive Data
- Journalistic Exceptions
- Secondary Liability
- Performing Due Diligence and Conducting Audits
- The Role of the Data Protection Authorities
- Self-Certification
- Verification
- Access
- Human Resources Data
- Obligatory Contracts for Onward Transfers
- Dispute Resolution and Enforcement
- Choice – Timing of Opt-Out
- Travel Information
- Pharmaceutical and Medical Products
- Public Record and Publicly Available Information
- Access Requests by Public Authorities

The Commerce Department has summarized key new requirements for companies in its Fact Sheet document.[37] There are rules regarding informing individuals about data processing. Firms have to provide free and accessible dispute resolution. Privacy Shield companies have to respond promptly to Commerce Department inquiries. Companies have data integrity and purpose limitation obligations. Privacy Shield members have to ensure accountability for data transferred to third parties. Firms must make public relevant Privacy Shield sections of FTC enforcement reports should they become subject to an FTC or court order based on non-compliance with the Shield. The Privacy Shield commitments continue for companies even if they depart the Shield if they receive data under the Privacy Shield Framework.

JAPAN PRIVACY LAW

The Amended Act on the Protection of Personal Information (APPI) came into effect on May 30, 2017.[38] The Act's Article 24 lays out options for permitting cross-border data flows. Kensaku Takase articulates these rules in the following way.[39]

The APPI provides that Personal Data may not be transferred to a foreign country unless:

(i) *the data subject has given specific advance consent to the transfer of the data subject's Personal Data to the entity in a foreign country:*

(ii) *the country in which the recipient is located has a legal system that is deemed equivalent to the Japanese personal data protection system, designated by the Japanese data protection authority; or,*

(iii) *the recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Japanese data protection authority.*

Perhaps the most interesting aspect of the Japanese system for cross-border data flows is the legitimacy it affords the APEC CBPR system as a transfer mechanism.

Japanese officials told Bloomberg BNA on September 27, 2017 that companies "transferring data from Japan to the U.S. should continue to rely" on the CBPR system because Japan "doesn't plan to give a blanket designation that the U.S. provides adequate data protection."[40] Japan's commitment to the APEC CBPR system is also clear because besides, TrustE, the Japanese company, JIPDEC, is the only other accountability agent in the APEC CBPR Framework.[41] Accountability agents are given the authority to certify companies as CBPR-compliant.

THE EU-JAPAN ECONOMIC PARTNERSHIP AGREEMENT

The EU and Japan signed the EU-Japan Economic Partnership Agreement on July 17, 2018.[42] On that day, the EU and Japan concluded their talks on reciprocal adequacy with respect to data flows between the EU and Japan. The European Commission describes the decision as creating the "world's largest area of safe data flows." [43] The mechanism the two sides agreed[44] upon to establish to make this happen was a mutual adequacy decision, meaning the EU will issue an adequacy decision and so will Japan.

The Commission announced on September 5, 2018 that it (and Japan) is going through its internal procedure to issue an adequacy decision with respect to data flows to Japan.[45] The Commission says that Japan has made the following commitments, which will enable the EU to make an adequacy decision.

- *A set of rules providing individuals in the EU whose personal data are transferred to Japan, with additional safeguards that will bridge several differences between the two data protection systems. These additional safeguards will strengthen, for example, the protection of sensitive data, the conditions under which EU data can be further transferred from Japan to another third country, the exercise of individual rights to access and rectification. These rules will be binding on Japanese companies importing data from the EU and enforceable by the Japanese independent data protection authority (PPC) and courts.*
- *The Japanese government also gave assurances to the Commission regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms.*
- *A complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority.*

The Commission has released a draft adequacy decision.[46] Japan's Personal Information Protection Commission is also preparing an adequacy decision. The law firm, Debevoise & Plimpton, summarizes advantages to firms transferring data from the EU to Japan as including more flexibility in data storage locations; smoother communications between EU and Japanese affiliates, potentially facilitating post-acquisition or post-merger integration; and, simplified due diligence – for example, transfers of personal data between the EU and Japan will not require verification of consent.[47]

BRAZIL PRIVACY LAW AND INTERNET FRAMEWORK LAW

President Michel Temer signed the Brazilian General Data Privacy Law (Lei Geral de Protecao de Dados Pessois or LGPD)[48] on August 14, 2018. Generally, commentators have emphasized the similarity between the Brazilian law and the GDPR.[49] There are, in fact, numerous similarities. Perhaps the most notable convergence given that Brazilian policymakers have, in the past, considered extensive data localization laws and/or regulations, is that the law does permit cross-border data flows. (Note: Brazil still has data localization laws, but they are less sweeping than originally contemplated. Government agencies including the Secretary of Information Technology of the Ministry of Planning, Development, and Management, have included forced data localization as a requirement for public procurement contracts involving cloud computing services.[50])

The LGPD's Chapter V entitled "International Transfer of Data" covers cross-border data flows. Article 33 permits transfers under the following circumstances.

> ***Art. 33.*** *International transfer of personal data is only allowed in the following cases:*
> *I – to countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of this Law;*
> *II – when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in this Law, in the form of:*
> *a) specific contractual clauses for a given transfer;*
> *b) standard contractual clauses;*
> *c) global corporate rules;*
> *d) regularly issued stamps, certificates and codes of conduct;*
> *III – when the transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies, in accordance with the instruments of international law;*
> *IV – when the transfer is necessary to protect the life or physical safety of the data subject or of a third party;*
> *V – when the national authority authorizes the transfer;*
> *VI – when the transfer results in a commitment undertaken through international cooperation;*
> *VII – when the transfer is necessary for the execution of a public policy or legal attribution of public service, which shall be publicized pursuant to Item I of the lead sentence of Art. 23 of this Law;*
> *VIII – when the data subject has given her/his specific consent and distinct for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; or*
> *IX – when it is necessary to satisfy the situations provided in Items II, V and VI of Art. 7 of this Law.*

So, the Brazilian law provides for a menu of options allowing for cross-border data flows and does not mandate data localization.

The Marco Civil da Internet, sometimes translated as the "Internet Framework Law" and occasionally as the "Brazilian Internet Bill of Rights," is an even more interesting example of how Brazil has handled the question of cross-border data flows.[51] Prior to the law being enacted in 2014, Brazil considered data localization requirements. Those obligations were, however, ultimately eliminated from proposed versions of the bill. Nonetheless, the law makes clear that Internet application providers must respect Brazilian law, including privacy laws, if they offer services to Brazilian citizens. Chapter III, Section 1, Article

11 3. says that "internet application providers must provide, as set forth by regulation, information that allows verification concerning its compliance with Brazilian legislation regarding the collection, storage, retention and treating of data, as well as, in regard to the respect of privacy and of confidentiality of communications." So, companies have obligations to respect Brazilian law, including with respect to storage, but the law does not require that data be stored in Brazil. The law seems to have struck a reasonable compromise in line with the spirit of the principle articulated in Chapter I, Article 3 that there should be "freedom of business models promoted on the Internet, provided that they do not conflict with the other principles set out in this Law."

CONCLUSION

As countries consider new trade agreements and possible new domestic legislation, especially privacy legislation, the examples discussed above can help shape thinking on developing optimal outcomes with respect to the promotion of cross-border data flows and, at the same time, the effective protection of, for instance, privacy. With respect to government or regulatory access to data, the USMCA Chapter 17 Financial Services Chapter illustrates how trade negotiators can promote an economically optimal outcome and at the same provide regulators the assurances that they require to obtain access to data, including in real-time if needed. While adequacy based cross-border data flow legal regimes are not ideal, such regimes, for instance the GDPR, can be reconciled with meaningful cross-border data flow commitments. Finally, with the United States, Canada, and Mexico committed through USMCA to recognizing the APEC CBPR system as a valid cross-bsorder data transfer mechanism, plus Japan's commitment to the APEC CBPR system, the APEC rules could become a more important data transfer mechanism in the future.

[1] McKinsey&Company, McKinsey Global Institute, "Digital Globalization: The New Era of Global Flows," March 2016, page 20
https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx
[2] ECIPE Occasional Paper No. 3/2014, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," 2014
http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[3] Leviathan Security Group, "Quantifying the Cost of Forced Localization," June 24, 2015, page 3
https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization
[4] Information Technology & Innovation Foundation (ITIF), "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Nigel Cory, May 2017
https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost
[5] CGAP, "3Myths About Data Localization," Silvia Baur-Yazbeck, August 21, 2018
http://www.cgap.org/blog/3-myths-about-data-localization
[6] Google Cloud, "Google Infrastructure Security Design Overview," Google Cloud White Paper, January 2017
https://cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf
[7] Google Products and Capabilities
https://cloud.google.com/security/products/
[8] Google Security White Paper
https://cloud.google.com/security/overview/whitepaper
[9] Google Cloud, "Freedom of data movement in the cloud era," Urs Holzle, Senior Vice President, Technical Infrastructure, February 22, 2018
https://www.blog.google/products/google-cloud/freedom-data-movement-cloud-era/
[10] Google Security White Paper
https://cloud.google.com/security/overview/whitepaper
[11] Google Standards, Regulations & Certifications
https://cloud.google.com/security/compliance/
[12] CGAP, "3 Myths About Data Localization," Silvia Baur-Yazbeck, August 21, 2018
http://www.cgap.org/blog/3-myths-about-data-localization

[13] See the United States Trade Representative (USTR) website for the text of the agreement, including Chapter 19 on Digital Trade
https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/united-states-mexico
https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pdf
[14] Foreign Affairs, "World War Web: The Fight for the Internet's Future," September/October 2018, "Regulate to Liberate: Can Europe Save the Internet," Helen Dixon, page 31
https://www.foreignaffairs.com/articles/2018-08-14/world-war-web
[15] IAPP, "Why CBPR recognition in the USMCA is a significant development for privacy," Joshua Harris, October 10, 2018
https://iapp.org/news/a/why-cbpr-recognition-in-the-usmca-is-a-significant-development-for-privacy/
[16] See the USTR website for the USMCA Text, specifically Chapter 17.
https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/17%20Financial%20Services.pdf
[17] See the USTR website for the TPP Text.
https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text
[18] The text is only 9 pages long because it incorporates most of the TPP text. See the document below from the New Zealand Ministry of Foreign Affairs&Trade website.
https://www.mfat.govt.nz/assets/CPTPP/Comprehensive-and-Progressive-Agreement-for-Trans-Pacific-Partnership-CPTPP-English.pdf
[19] See the USTR website for the text of Chapter 14 entitled: "Electronic Commerce."
https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf
[20] March 8, 2018 Letter from Vietnamese Minister of Industry and Trade Tran Tuan Anh to New Zealand Minister for Trade and Economic Growth Hon David Parker.
https://www.mfat.govt.nz/assets/CPTPP/Viet-Nam-New-Zealand-Cyber-Security.pdf
[21] The APEC Privacy Framework is available on the APEC website.
file:///C:/Users/cschonander/Downloads/05_ecsg_privacyframewk.pdf
[22] See the APEC Website.
https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
[23] See the APEC website.
https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx
[24] See link in footnote 15.
[25] Click on compliance directory upon clicking on the link below.
http://www.cbprs.org/Consumers/ConsumerDetails.aspx
[26] "Challenges to APEC-CBPR credibility," Professor Greenleaf AM, Panel 8 – Mapping APEC CBPRs onto EU BCRS – Mauritius, 15-16 October 2014
http://www2.austlii.edu.au/~graham/publications/2014/IDPPCC_APEC.pptx.pdf
[27] See below for the Asian Business Law Institute website.
http://abli.asia/UploadPDF/DP_Compendium_May_2018.pdf
[28] See below for the analysis of the 14 reports prepared by the Asian Business Law Institute website.
http://abli.asia/Portals/0/Privacy%20Laws%20and%20Business%20International%20Review%20-%20June%202018.pdf?ver=2018-06-18-145254-893
[29] See this Intersoft Consulting website for "the text of the GDPR neatly arranged."
https://gdpr-info.eu/
[30] See the SIIA website. "General Data Protection Regulation (GDPR) Entry-into-Force: Ten Suggestions from SIIA." Carl Schonander. May 24, 2018
https://www.siia.net/blog/index/Post/76033/General-Data-Protection-Regulation-GDPR-Entry-Into-Force-Ten-Suggestions-From-SIIA
[31] See the Intersoft Consulting website.
https://gdpr-info.eu/chapter-5/
[32] See the European Commission website below for the text of the Commission's adequacy decision with respect to the Shield plus the text of the Shield itself and accompanying annexes.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A207%3AFULL
[33] See the U.S. Commerce Department website below for information about the Shield.
https://www.privacyshield.gov/welcome
See below also for a relatively short but very useful Commerce Department Fact Sheet on the Shield.
https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf
[34] See the below Commerce Department website, which contains links to the EU-U.S. Privacy Shield elements described in this paragraph.

https://www.privacyshield.gov/EU-US-Framework
[35] See the below Government Printing Office published text of the Judicial Redress Act.
https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf
[36] See below for U.S. Department of Justice information on Attorney General Order No. 3824-2017, "Judicial Redress Act of 2015, Attorney General Designations," 82 Fed. Reg. 7860 (Jan. 23, 2017)
https://www.justice.gov/opcl/judicial-redress-act-2015
[37] See the below for the link to the document.
https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf
[38] See this non-official translation from Japanese into English of the Amended Act, which is available on the Japanese Data Protection Authority website.
https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf
The Personal Information Protection Commission of Japan contains links to a number of relevant documents in English.
https://www.ppc.go.jp/en/
[39] Privacy Tracker, "GDPR matchup: Japan's Act on the Protection of Personal Information," Kensaku Takase, August 29, 2017
https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/
[40] Bloomberg Law: Privacy & Data Security, "Moving Data Between Japan, U.S.? Use Asia Privacy Rules System," Stephen Gardner, September 27, 2017
https://www.bna.com/moving-data-japan-n73014470193/
[41] See the APEC website for information about accountability agents.
http://www.cbprs.org/Agents/AgentDetails.aspx
[42] Text of agreement in the below Government of Japan website.
https://www.mofa.go.jp/policy/economy/page6e_000013.html
Text of agreement in the below European Commission website.
http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684
[43] See this European Commission press release.
http://europa.eu/rapid/press-release_IP-18-4501_en.htm
[44] See below for the July 17, 2018 "Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Vera Jourova, Commissioner for Justice, Consumers and Gender Equality of the European Commission
https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf
[45] See this European Commission press release.
http://europa.eu/rapid/press-release_IP-18-5433_en.htm
[46] See below for the text of the draft adequacy decision.
https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf
[47] See below for Debevoise Update, "The EU and Japan Announce Data Protection Deal," August 13, 2018
https://www.debevoise.com/~/media/files/insights/publications/2018/08/20180813_eu_and_japan_announce_data_protection_deal.pdf
[48] See below for a translation of the law by the law firm of Pereira Neto Macedo
https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf
[49] See below, for instance, for a Covington comment entitled: "Brazil's New General Data Privacy Law Follows GDPR Provisions," Melanie Ramey, August 20, 2018
https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/
[50] Information Technology & Innovation Foundation, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost," Nigel Cory, May 2017
http://www2.itif.org/2017-cross-border-data-flows.pdf
[51] See below for an unofficial side-by-side translation of the law prepared by Carolina Rossini.
https://sflc.in/sites/default/files/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014.pdf