# Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill (No. 373 of 2019)

August 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

DSCI
PROMOTING DATA PROTECTION

# Table of Contents

# I. Introduction

Data flows between India and the United States are of unquestionable value to India's modern digital economy and society. According to a 2019 digital trade report[1] from the Hinrich Foundation, digital trade contributed $32.5 billion to India's domestic economy in 2017. The report further notes that this has the potential to grow to $480 billion by 2030. Largely driven by India's rapidly growing AI capabilities, IT and business process outsourcing industries, digital exports represent the largest export sector for India today. With respect to India-US trade specifically, India is the United States' eight largest trading partner and trade in goods and services, including digital trade, between both nations surged from $16 billion in 1999 to $142 billion in 2018.[2]

In addition, a joint study by the Internet and Mobile Association of India (IAMAI) and the Indian Council for Research on International Economic Relations (ICRIER) examining the implications of data localization on India's economy found that there are negative cost implications, including for domestic companies, associated with data localization policies.[3]

Given the economic importance of data flows to both India and the US, it is critical that cross-border data transfers are specifically enabled between the two countries. This is of particular importance in 2020 as India seeks to update its data privacy regime and introduce comprehensive data protection legislation for the first time. India's proposed Personal Data Protection Bill (PDPB) (Bill No. 373 of 2019) was introduced in the Lok Sabha on 11 December 2019 and is currently being reviewed by a Joint Parliamentary Committee.

The Centre for Information Policy Leadership (CIPL)[4] and the Data Security Council of India (DSCI)[5] put forward this joint report to highlight the importance of continued flows of data between India and the US following the passage of the PDPB. This report is intended to inform the Joint Parliamentary Committee's review of the PDPB as well as Indian Government officials working on a potential future trade deal with the US. CIPL has previously provided extensive input on all aspects of the PDPB to the Indian Ministry of Electronics and Information Technology (MeitY) and to the Joint Parliamentary Committee reviewing the PDPB.[6]

Specifically, this report aims to:

- Outline relevant provisions of the PDPB in Chapter VII (Restriction on Transfer of Personal Data Outside India) and section 50 on Codes of Practice that apply to transfers of data from India to the US;

- Evaluate such provisions in light of established mechanisms for cross-border data transfers in other global data protection regimes; and

- Consider available options to govern India-US data flows.

With respect to the last point, this report will:

- **Discuss how India can enable data flows to the US by including certifications and codes of practice as data transfer mechanisms in the PDPB** which could become interoperable with other certification schemes and codes, including the APEC Cross-Border Privacy Rules (CBPR) and EU General Data Protection Regulation (GDPR) certifications and codes of conduct; and

- **Examine how India could facilitate transfers between India and the US through the PDPB's existing provision authorizing adequacy findings for data transfer purposes.** Tools to facilitate such findings, having regard to applicable laws and international agreements, could include an India-US trade agreement specifying a commitment to recognize or elaborate upon relevant transfer mechanisms (e.g. APEC CBPR in which the US is a participant or future Indian certifications or codes of practice) and/or a formally binding cooperation agreement or Memorandum of Understanding (MOU) between the Indian Data Protection Authority (DPA) and the US Federal Trade Commission (FTC).

Each of the above transfer schemes relies on an enforcement mechanism to ensure compliance with its standards. The US FTC is the primary privacy enforcement authority in the US and has vigorously enforced[7] cross-border privacy commitments, including APEC CBPR as well as the EU-US Privacy Shield Framework. With respect to the latter, it is important to note that in July 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield Framework.[8] Privacy forms part of the FTC's jurisdiction over consumer protection matters in the US. Equally, it is important to remember that while the FTC has broad enforcement jurisdiction over broad sectors of the economy, certain aspects of the economy, such as components of health and financial services are regulated by other US government agencies, including on privacy and data protection matters.

Moreover, while this report outlines a number of pathways available to India for enabling data transfers to the US and respectfully suggests certain options, we appreciate that India will conduct its own assessment of the available options in the context of any trade negotiations with its US counterparts.

# II. Provisions in Bill No. 373 of 2019 Relevant to Data Transfers

Chapter VII of the current draft of the PDPB outlines India's proposed approach to regulating transfers of sensitive and critical personal data outside of India. The PDPB does not limit transfers of non-sensitive and non-critical personal data.

### Chapter VII—Restriction on Transfer of Personal Data Outside India

**Section 33** of the PDPB imposes a prohibition on processing sensitive personal data and critical personal data outside of India.

Section 33 specifies that sensitive personal data may be transferred outside of India but must continue to be stored in India. In effect, a local copy of all sensitive personal data must remain within India at all times. Sensitive personal data is defined broadly in section 3(36) of the PDPB and constitutes "personal data, which may, reveal, be related to, or constitute financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation; or any other data categorized as sensitive personal data under section 15". Section 15 of the PDPB permits the Central Government to classify further categories of personal data as "sensitive personal data".

Section 33 further notes that critical personal data may only be processed in India. Coupled with the fact that critical personal data can only be transferred outside of India under two limited circumstances (see below), this effectively creates a data localization requirement for critical personal data in India. In addition, some of the data may not even pertain to Indian data principals, which adds another compliance challenge and does not contribute to any additional security or privacy. Moreover, the PDPB leaves the definition of "critical personal data" to the Central Government. The lack of a definition creates challenging legal uncertainty for domestic and foreign entities that want to transfer data to and from India.

**Section 34** of the PDPB outlines the circumstances in which sensitive personal data and critical personal data may be transferred outside of India.

Sensitive personal data may only be transferred outside of India for processing purposes when explicit consent is given by the data principal for the transfer, and the transfer is made (1) pursuant to a contract or intra-group scheme approved by the Indian DPA; or (2) where the Central Government has made an "adequacy" finding with respect to a particular country, entity, class of entity in a country or international organization; or (3) where the DPA has allowed the transfer of any sensitive personal data, or class of such data, necessary for any specific purpose.

With respect to an "adequacy" finding by the Central Government, this must be made on the basis that the transferred sensitive personal data shall be subject to an adequate level of protection, by the country, entity or class of entity or international organization in receipt of the data, having regard to the applicable laws and international agreements. In addition, the transfer must not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction.

Section 34 additionally provides two narrow exceptions to the default ban on processing critical personal data outside of India. Critical personal data may only be transferred outside of India (1) where such transfer is to a person/entity engaged in the provision of health or emergency services where such transfer is necessary for prompt action (note that such transfers must be notified to the DPA within a timeframe to be specified by regulations); or (2) where the Central Government has deemed the transfer to be permissible under a finding of adequacy along the same lines as for transfers of sensitive data outlined above. With respect to the latter exception, there is an additional requirement that such transfer, in the opinion of the Central Government, must not prejudicially affect the security and strategic interest of the State.

### Section 50—Codes of Practice

Section 50 of the PDPB provides that the DPA shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under the PDPB. Under the current text of the Bill, the DPA may approve any code of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government. The PDPB lists specific matters that a code of practice may address, and this includes transfers of personal data outside of India pursuant to section 34 (see section 50(6)(q)). However, it is important to note that the PDPB does not currently list codes of practice as an available transfer mechanism under section 34.

# III. Evaluation of Data Transfer Provisions in Bill No. 373 of 2019 in Light of Established Approaches for Cross-border Data Transfers in Other Global Data Protection Regimes

## A. Chapter VII—Restriction on Transfer of Personal Data Outside India

While some aspects of Chapter VII of the PDPB bear resemblance to data transfer rules found in other data protection laws, for the most part, sections 33 and 34 differ significantly from other common approaches for transferring data across borders. Such differences present significant challenges as detailed below. This section aims to provide an evaluation of the current PDPB rules on cross-border data transfers in light of established approaches for transfers in other global data protection regimes.

For India to continue to flourish as a global center of innovation and trade for both Indian and multinational organizations, it is imperative that the PDPB include interoperable rules on data transfers. There are alternative and less trade-restrictive solutions that can address relevant concerns while avoiding the challenges put forward by the current wording of Chapter VII of the PDPB (see Section IV of this report below).

Sections 33 and 34 of the PDPB present several challenges with respect to sensitive and critical personal data:

### Sensitive Personal Data

1. **Requirement to continually store a local copy of sensitive data in India:** With respect to the transfer of sensitive personal data outside of India, a local storage requirement will severely disrupt the operations of both data fiduciaries and processors in multiple respects. Such a requirement would:

    - **Prohibit the use of technology relying on distribution of data:** A local storage requirement for sensitive data would undermine Indian companies' ability to fully leverage emerging technologies that rely significantly on global and distributed networks, such as cloud computing, data analytics and AI and machine learning applications. This would negatively impact the competitiveness of Indian organizations vis-à-vis their counterparts in other countries that have access to such competitive technologies and data.

- **Impose the creation of redundant storage systems:** The move to the cloud and use of cloud services has only intensified in the COVID-19 world and will continue to do so in the post-COVID world. Such services enable organizations to serve multiple markets without having separate and redundant storage systems within each jurisdiction. Not only does such centralization create economies of scale for organizations but it also streamlines processing operations and ensures relevant types of data are kept together—for example, ensuring that relevant health data is kept with corresponding personal data stored for health insurance purposes outside of India. By requiring organizations to store a local copy of sensitive data in India, the PDPB would impose an obligation to create redundant storage systems that would raise costs, disrupt business processes and create information security risks.

- **Increase costs to prohibitive levels for local and foreign small and medium enterprises:** One of the benefits of permitting data to flow freely between countries is that it ensures the competitiveness of small and medium-sized enterprises (SMEs). Modern day data storage solutions via cloud computing have provided such enterprises with a platform to enter the market and compete with larger organizations. The requirement to create redundant local data storage systems for sensitive data could effectively act as a barrier to market access for SMEs and startups. According to Statista.com, fintech and healthcare startups accounted for almost 14% of all global startups in 2017—businesses which process large volumes of sensitive data on a daily basis.[9] Such organizations may ultimately have no choice but to avoid serving Indian customers due to the prohibitively high costs of creating redundant storage systems, especially when such organizations are just starting out and trying to launch their digital services.

- **Compromise data security:** Creating redundant storage systems for sensitive data may expose such data to greater cybersecurity risks as well as risk of loss from natural disasters. By concentrating such systems in India, organizations would create additional and unnecessary "touch points" of vulnerability susceptible to attack and data loss. It would also prevent the partitioning of sensitive data sets across global servers, which can provide an additional layer of protection against hackers as well as business continuity in the case of natural disasters.

- **Create complex conflict of laws situations:** A local storage requirement for sensitive data has the potential to create complex conflict of laws situations with other data protection laws globally. For example, holding data longer than necessary or using data for different purposes than for which it was originally collected (including to classify the sensitive data for local storage purposes) could contravene many data protection laws, including the EU GDPR. As the US considers further state privacy laws and potential federal legislation, there is scope for similar conflicts to arise between the PDPB's local storage requirement for sensitive data and US privacy requirements.

**2. Requirement to obtain explicit consent on top of other requirements to transfer sensitive personal data outside of India:**

Contracts, intra-group schemes and adequacy findings are sensible mechanisms to enable cross-border data transfers and are consistent with approaches taken in other modern privacy laws such as the GDPR or Brazil's new privacy law, the LGPD.[10] However, the PDPB's requirement to obtain an individual's consent alongside such transfer mechanisms is an outlier among data protection laws globally. It will seriously impact the ability of organizations to transfer data abroad for legitimate and beneficial purposes.

Indeed, the GDPR only allows for the use of explicit consent as a basis for transfer in cases where a transfer cannot be made pursuant to an adequacy finding or an appropriate safeguard (e.g. binding corporate rules, standard contractual clauses, codes of conduct, or certifications) and the individual has been informed of the possible risks of the transfer. In Canada, the Office of the Privacy Commissioner of Canada (OPC) conducted a public consultation in 2019 on changing its policy position for transfers to require consent for trans-border data flows. At the conclusion of the consultation, the OPC ultimately decided that consent for transfers is not required and that the existing approach based on accountability remains appropriate.

The key concerns associated with requiring additional explicit consent for cross-border transfers of sensitive data in the PDPB are as follows:

- **Consent does not add additional protection to data principals:** Requiring consent for transfers on top of a contract, intra-group scheme or adequacy finding does not necessarily add any additional protection to individuals. This is because contracts and intra-group schemes already impose separate and clear legal obligations to protect the data. In fact, such mechanisms impose more requirements on data recipients and provide more protection than consent as consent simply gives individuals the choice to accept whatever risk they are presented with. Consent in this context is more of a mechanism to protect the businesses rather than the users as it gives the businesses cover once consent is obtained. According to a study from the Consumer Unity & Trust Society Centre for Competition, Investment and Economic Regulation (CUTS C-CIER), only 11% of Indian Internet users read privacy policies.[11] In the digital and data economy, this number will not increase as individuals will not be able to keep up with the sheer volume of consent requests or make informed choices even if they tried. In today's data centric environment, it is unrealistic to expect individuals to protect themselves via consent. Moreover, requiring consent on top of an adequacy finding undermines the Central Government's determination that a country, entity or class of entities in a country, or an international organization provides an adequate level of protection for sensitive data. Adding consent on top of such a determination adds no additional protection to the individual. In fact, no additional protections should be needed, as is illustrated by the fact that

the transfer of sensitive data within India is permitted without consent; yet, in a jurisdiction that is designated as providing a substantially equivalent level of protection when compared to the protections provided under the PDPB, consent is required.

- **Requiring consent sends a confusing and inappropriate message about transfers to data principals:** Asking for consent for all cross-border transfers of sensitive data is confusing to individuals and could mislead people to think that there might be something inherently risky or wrong with such transfers. In the modern global digital economy, transfers are essential to the provision of a wide range of products and services for consumers. Consent requests for every transfer of sensitive data which, in any event, can be made safe through a range of other transfer mechanisms (contracts, intra-group schemes and adequacy findings) may deter individuals from accessing the full range of available products and services, even if they would benefit from using them, for example, to avail themselves of health and wellness Internet of Things (IoT) devices.

- **Requiring consent imposes an unnecessary burden on data principals:** Asking individuals to consent to every transfer of sensitive data would dramatically increase the number of consent requests they receive, overburdening them and having the effect of diluting and undermining the effectiveness of consent in situations where it would be meaningful.

- **Requiring consent imposes an unnecessary burden on data fiduciaries and processors:** In preparing for compliance with the PDPB, organizations would have to implement the mechanisms and procedures associated with obtaining consent for transfers of sensitive data. This could cause substantial costs to new and existing businesses, and disruption to organizations that already have established mechanisms in place for the transfer of data across borders in line with common approaches found in many global data protection laws.

- **Obtaining consent for every transfer of sensitive data is not always feasible:** In some cases, it is impossible to obtain consent for a transfer of sensitive data due to an organization's lack of relationship with, and/or contact information of, an individual whose personal data is being transferred. This is particularly common in the provision of services related to fighting financial crime, where an organization does not have a direct relationship with the individual in question and may be mandated by law to share sensitive data such as financial information.

In addition to these practical reasons against requiring consent for cross-border transfers of sensitive data, there is an important policy consideration that the Joint Parliamentary Committee should take into account as it reviews the PDPB's requirements for transferring data outside of India:

- **The definition of sensitive data may expand:** As previously mentioned, section 15 of the PDPB permits the Central Government to classify further categories of personal data as "sensitive personal data" in addition to those expressly outlined in section 3(36) of the Bill. This flexibility will create perpetual uncertainty for both Indian and global organizations that may be required at a moment's notice to obtain consent for the transfer of additional categories of data that are deemed "sensitive". To ensure an attractive Indian digital market for all organizations, the Joint Parliamentary Committee should ensure predictability of the rules by clarifying how further categories of sensitive personal data may be classified outside of the PDPB. For example, regulatory guidance on sensitive categories of data that can be rebutted through appropriate risk assessments may provide flexibility for new risks that arise while ensuring more certainty for organizations.

### Critical Personal Data

1. **Critical personal data is not currently defined:** The absence of a definition of critical personal data in the PDPB will create considerable uncertainty for organizations as they prepare to implement its rules. Providing open ended flexibility for the Central Government to decide which categories of data are considered "critical" also impacts data transfers as any data classified as critical can only be transferred outside of India under extremely narrow circumstances.

2. **Critical personal data can be transferred across borders only in extremely limited circumstances:** As noted previously, critical personal data may only be transferred outside of India to persons/entities engaged in the provision of health or emergency services and where the transfer is necessary for prompt action. It may also be transferred under an adequacy finding where such a transfer would not prejudicially affect the security and strategic interest of the State. CIPL and DSCI understand that such a requirement may be motivated around concerns to secure access to data in cross-border investigations of serious crimes. However, there are other less trade-restrictive methods for achieving such access which avoid the negative economic impacts that a localization requirement imposes on digital trade. For example, India could seek to negotiate bilateral instruments such as Mutual Legal Assistance Treaties (MLAT), new mutual legal assistance mechanisms,[12] agreements under the US CLOUD Act[13] or under specific trade agreements.[14]

## B. Section 50—Codes of Practice

Codes of practice are an important tool for ensuring compliance, organizational accountability and responsible data use. The term codes of practice could describe both "codes of conduct" (the term used in the GDPR) as well as data protection certifications, seals and marks (which the GDPR lists as a separate mechanism from codes of conduct). However, it is not clear from the PDPB whether the term "codes of practice" intends to capture both codes of conduct and certification schemes. Each of these schemes play an increasingly important role in creating global interoperability between different privacy regimes as well as cross-border transfer mechanisms. CIPL and DSCI recommend that the Joint Parliamentary Committee consider amending section 50 of the PDPB to expressly include certifications.

In addition, the Joint Parliamentary Committee should recommend adding certifications and codes of practice to the list of existing mechanisms available to transfer sensitive data under section 34(1)(a). An increasing number of countries allow transfers of personal data across borders pursuant to such mechanisms, including the US. The US currently participates in the APEC CBPR system. The US also participates in the EU-US Privacy Shield and the Swiss-US Privacy Shield self-certification frameworks—although, as previously noted, the EU-US Privacy Shield has been invalidated as a transfer mechanism by the Court of Justice of the European Union. The Swiss-US Privacy Shield remains valid pending further analysis by the Swiss Federal Data Protection and Information Commissioner and the US Department of Commerce has stated that it will continue to administer the EU-US Privacy Shield. Both the US Department of Commerce and the FTC have made clear that the CJEU's decision does not relieve organizations of their ongoing obligations with respect to data transferred under the terms of the Privacy Shield.[15] Modern data protection legislation also incorporates the concept of certifications (e.g. the GDPR and Brazil's LGPD).[16]

# IV. Available Options to Govern India-US Data Flows

It is clear from the above discussion that the current draft of the PDPB raises significant challenges with respect to flows of personal data outside of India that might seriously impair India's ambitions to grow its economy and advance its SMEs, especially those in the technology field. CIPL and DSCI believe that there are alternative options that India can pursue to facilitate responsible data transfers to the US while ensuring the protection of personal information in line with the PDPB.

## A. Facilitating India-US Data Transfers: Enabling Certifications and Codes of Practice as Transfer Mechanisms under the PDPB

One approach to facilitating responsible data flows from India to the US involves enabling certifications and codes of practice as transfer mechanisms in the PDPB. CIPL has previously made this recommendation to MeitY and the Joint Parliamentary Committee reviewing the PDPB.[17] Such certifications and codes of practice should be designed in ways that are interoperable with certification schemes of third countries. Achieving such interoperability could involve considering the APEC CBPR, GDPR certifications and codes of conduct, or certain elements of the now defunct EU-US Privacy Shield Framework in building India's own certifications.

Privacy certifications are of great value to the Indian market. A recent study by CISCO examined the value of privacy certifications in the buying process when selecting a vendor or product. 95% of Indian companies agreed that privacy certifications are an important factor. In fact, out of the 13 countries surveyed in that study, Indian companies placed the highest in terms of assigning importance to privacy certifications.[18]

There are several ways India can introduce certifications for cross-border data transfers in the PDPB:

- Add certifications and codes of practice to the list of existing mechanisms available to transfer sensitive data (i.e. contracts and intra-group schemes) under section 34(1)(a).
- On top of this, expand section 50 of the PDPB, dealing with codes of practice, to explicitly include certifications. This would directly link the PDPB with certifications that deal with the transfer of personal data outside India under section 50(6)(q).

- In the absence of explicitly including certifications in section 50, India could interpret the meaning of "codes of practice" to implicitly include certifications. As noted above, it is arguable that codes of practice already encompass certification schemes. Codes of practice are defined in the PDPB as "a code of practice issued by the Authority under section 50". Section 50 notes that the Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under the PDPB—certifications, by their very nature, achieve such goals (i.e. promotion of responsible data practices and compliance with applicable law).

Enabling certifications and codes of practice in this way would also put the Indian DPA in a position to recognize the certifications of third countries as valid certifications under the PDPB to the extent they are in line with its own certifications for data transfers or substantially align with the privacy protections in the PDPB. Where foreign certifications are not substantially in line with Indian requirements, India could negotiate add-on protections to close any material gaps. As an example, this might include approving the APEC CBPR as an equivalent certification (plus any necessary add-on protections), thereby permitting data flows between Indian organizations and CBPR certified entities generally or to US CBPR certified organizations specifically. In June 2020, the Singapore Personal Data Protection Commission (PDPC) took similar action by amending its Personal Data Protection Regulations relating to "Transfer of Personal Data outside Singapore" to recognize APEC CBPR and its corollary system, the APEC Privacy Recognition for Processors (PRP) as transfer mechanisms in their own right. This allows Singaporean organizations to transfer personal data to an overseas recipient that is CBPR- or PRP-certified.[19] Similarly, Japan's Personal Information Protection Commission (PPC) recognized, in guidelines relating to the 2015 Amendment of the Japanese Act on the Protection of Personal Information (APPI), the CBPR as an international framework on the handling of personal information for data transfer purposes under the APPI.[20]

Additionally, in enabling certifications and codes of practice as transfer mechanisms under the PDPB, India should consider the enforceability of such certifications. For transfers to the US, appropriate enforcement could be facilitated via an enforcement cooperation agreement with the FTC, along the lines of a bilateral enforcement cooperation agreement or MOU:

- **Bilateral enforcement cooperation agreement:** To ensure appropriate oversight and robust enforcement of India-US data transfers, the Indian DPA could enter into a binding enforcement cooperation agreement with the US FTC relating to privacy and data protection enforcement. The FTC has the legal authority under the US SAFE WEB Act of 2006[21] to enter into binding agreements if the law of the foreign country requires it. This Act, amending the FTC Act, provides the FTC with a number of tools to improve enforcement regarding consumer protection matters, particularly those with an international dimension, including increased cooperation with foreign law enforcement authorities through confidential

information sharing and provision of investigative assistance. The Act also allows enhanced staff exchanges and other international cooperative efforts. Historically, the FTC has rarely entered into such agreements given the complex interagency process involved.

- **Memorandum of Understanding:** More commonly, the FTC has entered into non-binding enforcement cooperation arrangements (known as "Memorandums of Understanding" or MOUs) with counterpart authorities. According to the FTC website, all cooperation agreements can be classified as either US interagency agreements or international agreements, though these "international agreements", as stated, more often take the form of MOUs.[22] The US Department of Justice and the FTC have an MOU with the Government of India's Ministry of Corporate Affairs and the Competition Commission of India on antitrust cooperation.[23]

## B. Facilitating India-US Data Transfers: Adequacy Findings under the PDPB

Under section 34(1)(b) of the PDPB, the Central Government has the authority, in consultation with the DPA, to make an adequacy finding with respect to the level of protection of a third country, entity or class of entity or international organization for data transfer purposes. Such a finding must be made on the basis that the sensitive data being transferred shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements. There are numerous forms of international agreements that India could pursue with the US to facilitate such a finding which are detailed further below.

It is important to note that it is highly unlikely that the US will enter or accept further bilateral data transfer arrangements with other countries as it did with the European Union under the EU-US Privacy Shield or the Swiss-US Privacy Shield. Instead, the US has been signaling that, going forward, it will focus on multilateral solutions to data flows via the CBPR system rather than on bilateral solutions. For example, in September 2019, a statement from the White House Press Secretary released shortly before the Privacy Shield's third annual review noted "[t]he Administration will continue to expand the benefits of the CBPR System to more of our trading partners within and beyond the APEC region, while reinforcing its close partnership with the European Union to ensure the success of the Privacy Shield Framework"[24] (emphasis added). This has been widely interpreted as a clear indication that the US will not entertain the idea of additional bilateral data transfer agreements along the lines of a Privacy Shield like arrangement but will seek multilateral solutions to global cross-border data flows, specifically via the CBPR. This makes sense considering that global interoperability for data flows is key to sustained growth. Creating multiple unrelated data transfer agreements between multiple countries leads to higher costs of doing business, increased bureaucracy for both governments and businesses, and economic inefficiencies. Multilateral solutions avoid such issues while enabling data

flows to the largest possible number of countries and ensuring appropriate levels of protection and responsible data use by organizations. Furthermore, as noted above, in July 2020 the Court of Justice of the European Union invalidated the EU-US Privacy Shield Framework[25] which only further calls into question whether the US would enter into similar arrangements with other countries.

To facilitate India-US transfers in light of this, India could consider the following:

- A specific India-US trade agreement that may articulate a commitment by both parties to collaborate on a cross-border transfer framework coupled with a privacy enforcement cooperation arrangement. A promising and feasible transfer framework in this regard is the APEC CBPR system[26] for the reasons explained above.

- A binding bilateral enforcement cooperation agreement between the Indian DPA and the US FTC under the US SAFE WEB Act of 2006.

- A Memorandum of Understanding (MOU) between the Indian DPA and the US FTC.

### 1. An India-US Trade Agreement that Specifically Incorporates CBPR

India could negotiate a trade agreement with the US that specifically incorporates the CBPR. The Central Government could recognize CBPR certified companies as providing an adequate level of protection for purposes of data transfer under the PDPB, having regard to such an international agreement. The CBPR comprise a set of 50 robust program requirements that operationalize nine Privacy Principles of the APEC Privacy Framework[27] (which are also reflected in the PDPB and which draw upon principles in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013)) and are enforceable under the laws of participating APEC economies. However, if India deems the CBPR requirements as insufficient when compared to India's privacy law, it could require CBPR certified companies to adhere to additional key requirements in order to meet its standard for adequacy.

There is precedent for such country specific arrangements. For example, in order for Japan to receive its finding of adequacy from the European Union it had to adopt supplementary rules to augment the protections of its Act on the Protection of Personal Information. One such rule relates to the onward transfer of data received from the EU.[28] Similarly, Canada received an adequacy determination from the EU only with respect to transfers to commercial organizations regulated by Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). The adequacy decision does not cover transfers to organizations regulated by Canada's Federal Privacy Act or those that are regulated by the public sector at a provincial level.[29] As such, India could consider a tailored adequacy finding with the US, using the APEC CBPR as the basis.

APEC economies participating in the CBPR are currently exploring options for expanding the reach of the CBPR beyond APEC given the interest among industry and other stakeholders to have a global rather than regional solution for cross-border data transfers. Options under consideration include (1) that non-APEC economies adopt similar certifications that are interoperable with the CBPR; and (2) that the CBPR be expanded beyond APEC and opened up to allow participation by non-APEC countries. Moreover, the CBPR requirements are in the process of being updated and, particularly if option (2) materializes, all participating countries, including potentially India, will be able to shape these updates. One key advantage for India in pursuing a tailored adequacy finding with the US on the basis of the CBPR is that it could potentially play a more active role in ensuring key requirements of the PDPB are met by the CBPR. Another advantage is that it would also set India up to formally join the system if and when it is opened up to non-APEC countries.[30] In that case, India could also join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), which is an enforcement cooperation arrangement all privacy enforcement authorities responsible for enforcing the CBPR in the participating countries must join.[31]

Incorporating the CBPR in an India-US trade agreement could be done along the same lines as the United States-Mexico-Canada Agreement (USMCA)[32] (formerly known as the North American Free Trade Agreement (NAFTA)) or the US-Japan Digital Trade Agreement.[33] Such an approach is timely as trade negotiations are currently ongoing between India and the US.

Article 19.8 in the USMCA's chapter on Digital Trade (Chapter 19) requires the US, Mexico and Canada to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade", and that in developing this legal framework they "should take into account principles and guidelines of relevant international bodies, 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 (2013)".[34] It also encourages each country to develop "mechanisms to promote compatibility" between their different legal regimes for protecting personal information. Importantly, it states that "[t]he Parties recognize that the APEC Cross-Border Privacy Rules (CBPR) system is a valid mechanism to facilitate cross-border information transfers while protecting personal information".[35] In addition to recognizing the CBPR, this language strongly supports recognizing the broader concept of accountability tools such as certifications in a legal framework for the protection of personal information of users of digital trade.

On 1 January 2020, the Agreement Between the United States of America and Japan Concerning Digital Trade entered into force. Article 15 of the agreement deals with personal information protection. Article 15(1) requires each party adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. Article 15(3) encourages the

development of mechanisms to promote interoperability between the countries different privacy regimes, recognizing that the parties may take different legal approaches to protecting personal information. A Fact Sheet produced by the Office of the United States Trade Representative (USTR)[36] which details key outcomes of the agreement notes that the agreement contains rules for "[g]uaranteeing enforceable consumer protections, including for privacy and unsolicited communication, that apply to the digital marketplace, and promoting the interoperability of enforcement regimes, such as the APEC Cross-Border Privacy Rules system (CBPR)". Of course, both the US and Japan participate in the CBPR system and have operationalized this system between themselves and other participating APEC economies already. There is nothing to stop the Indian and the US governments from doing the same between their countries.

India and the US could negotiate a digital trade deal containing similar provisions to the USMCA and/or the US-Japan Digital Trade Agreement. According to the USTR, the US-Japan Digital Trade Agreement "parallels the USMCA as the most comprehensive and high-standard trade agreement addressing digital trade barriers ever negotiated".[37] Accordingly, such agreements may provide inspiration and guidance for a similar India-US trade agreement. Of course, it will be up to India and the US to work out the exact parameters of such a deal. It is important to note that even with relying on the CBPR for India-US data transfers, any protections of the PDPB that are not provided by the CBPR must also follow the data to the US. Thus, consistent with the CBPR system generally, under the CBPR the protection of the data may not fall below the standard required by the country in which the data was collected—here India, and that feature could be explicitly restated between India and the US. A digital trade deal could also address issues of enforcement, for example by committing to encourage the relevant privacy enforcement authorities (the Indian DPA and the US FTC) to enter into an appropriate enforcement cooperation arrangement (see discussion in section A above generally).

### 2. A binding bilateral enforcement cooperation agreement under the US SAFE WEB Act of 2006

With respect to bilateral enforcement agreements, we have mentioned that historically the FTC has rarely entered into such agreements. However, the FTC may be more willing to enter into such an agreement if Indian law requires it under section 34(1)(b) of the PDPB (i.e. if it is required by virtue of the term "international agreement").

### 3. A Memorandum of Understanding (MOU) between the Indian DPA and the US FTC

With respect to an MOU, depending on the parameters of the reference to "an international agreement" under section 34(1)(b) of the PDPB (i.e. whether such an agreement can be non-binding), there is scope for the FTC to enter into an MOU on data protection enforcement cooperation with the Indian DPA.

As mentioned earlier in this report, the FTC has enforcement jurisdiction over broad sectors of the economy. However, certain aspects of the economy, such as components of health and financial services are regulated by other US government agencies, including on privacy and data protection matters. While a large portion of sensitive data transfers from India to the US likely would be between organizations covered by the US FTC's jurisdiction, some of it may not and, therefore, similar cooperation arrangements would have to be explored with other relevant sectoral regulators.

Moreover, only US organizations within the FTC's jurisdiction can currently certify to the CBPR—at least until additional US sectoral regulators join the CBPR system as backstop privacy enforcement authorities, which is a possibility. In fact, India's recognition of US CBPR certified companies as adequate might create demand in the US and impetus for certain sectoral regulators to join the CBPR thereby increasing the range of the CBPR-based solution proposed by this report for India-US data flows.

These sector-specific issues and options require further exploration that is beyond the scope of this report.[38]

# V. Conclusion

Given that the PDPB is still under consideration, India has a real opportunity to shape the data flows landscape it wants to participate in for many years ahead. This report has provided an analysis of current challenges to transferring data outside of India under the current text of the PDPB. To ensure the continued and responsible flow of data from India to the US, India should enable certifications and codes of practice as transfer mechanisms within the PDPB and ensure that they are designed with interoperability in mind. Furthermore, India should facilitate India-US data transfers by recognizing the US as providing an adequate level of protection. A promising and feasible way of doing this is by recognizing the APEC CBPR as adequate for transfers by having regard to international agreements such as an India-US trade agreement or different forms of enforcement cooperation agreements between the US FTC and the Indian DPA.

With this in mind, it is imperative that the Joint Parliamentary Committee, the Indian government and other key stakeholders in India's privacy debate act to prevent unnecessary barriers to data transfers that can hurt the Indian economy and digital transformation. Hundreds of billions of dollars in digital trade growth could depend on the difference between immediate action and delay, and immediate action as described herein would only improve, not undermine, effective data protection for Indians.

If you would like to discuss this report or require additional information, please contact Markus Heyder, mheyder@HuntonAK.com or Sam Grogan, sgrogan@HuntonAK.com at CIPL or Vinayak Godse, vinayak.godse@dsci.in; Rama Vedashree, rama@dsci.in or Anand Krishnan, anand.krishnan@dsci.in at DSCI.

[1] See "The Data Revolution: Capturing the Digital Trade Opportunity at Home and Abroad", Hinrich Foundation, July 2019, available at https://s3-ap-southeast-1.amazonaws.com/hinrichfoundation-images/wp-content/uploads/2019/10/HF-Digital-Trade-Countries-D4-Red1.pdf at page 16.

[2] See "A Field Guide to U.S.-India Trade Tensions", Council on Foreign Relations, 13 February 2020, available at https://www.cfr.org/article/field-guide-us-india-trade-tensions.

[3] Kathuria, R., Kedia, M., Varma, G., and Bagchi, K., "Economic Implications of Cross-Border Data Flows", IAMAI and ICRIER, November 2019, available at http://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.

[4] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/.

[5] DSCI is a not-for-profit, industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities.

[6] See CIPL Comments on the Indian Ministry of Electronics and Information Technology's Draft Data Protection Bill 2018, 26 September 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_indian_ministry_of_electronics_and_information_technology%E2%80%99s_draft_data_protection_bill_2018.pdf and CIPL Response to the Indian Joint Parliamentary Committee on the Personal Data Protection Bill 2019, 21 February 2020 available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_indian_joint_parliamentary_committee_on_the_personal_data_protection_bill_2019__21_february_2020_.pdf.

[7] For a list of FTC enforcement actions relating to APEC CBPR, please see https://www.ftc.gov/terms/asia-pacific-economic-cooperation-apec. For a list of FTC enforcement actions relating to the now defunct EU-US Privacy Shield Framework, please see https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=8013.

[8] See Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, 16 July 2020, available at http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=9710274.

[9] Duffin, E., Distribution of startups worldwide in 2017, by industry, 27 May 2019, available at https://www.statista.com/statistics/882615/startups-worldwide-by-industry/.

[10] See Article 33 of Brazil's Data Protection Law (Lei Geral de Proteção de Dados Pessoais (LGPD)), available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[11] 60% online users fear unauthorised data collection, only 11% users read privacy policies: Survey, Consumer Unity & Trust Society Centre for Competition, Investment and Economic Regulation (CUTS C-CIER), 11 March 2019, available at https://cuts-ccier.org/60-online-users-fear-unauthorised-data-collection-only-11-users-read-privacy-policies-survey/.

[12] See, as an example, Swire, P., and Desai, D., "A 'Qualified SPOC' Approach for India and Mutual Legal Assistance", Lawfare, 2 March 2017, available at https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance.

[13] Public Law 115-141: Clarifying Lawful Overseas Use of Data (CLOUD) Act, available at https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm.

[14] See, for example, Article 17.18(2) of the United States-Mexico-Canada Agreement, available at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between which does not require financial institutions to store data locally as long as relevant authorities are able to access the information they require.

[15] See "FAQs – Swiss-U.S. Privacy Shield", US Department of Commerce, available at https://www.privacyshield.gov/article?id=Swiss-U-S-Privacy-Shield-FAQs and Federal Data Protection and Information Commissioner (FDPIC) Statement on "CJEU ruling on European standard contractual clauses and the EU-US Privacy Shield", available at https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#2131377919. See also "FAQs – EU-U.S. Privacy Shield Program Update", US Department of Commerce, available at https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

[16] See Article 42 GDPR and Article 33 LGPD.

[17] See CIPL Comments on the Indian Ministry of Electronics and Information Technology's Draft Data Protection Bill 2018, 26 September 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_indian_ministry_of_electronics_and_information_technology%E2%80%99s_draft_data_protection_bill_2018.pdf at page 44 and CIPL Response to the Indian Joint Parliamentary Committee on the Personal Data Protection Bill 2019, 21 February 2020 available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_indian_joint_parliamentary_committee_on_the_personal_data_protection_bill_2019__21_february_2020_.pdf at pages 10-11.

[18] "From Privacy to Profit: Achieving Positive Returns on Privacy Investments", CISCO Data Privacy Benchmark Study, January 2020, available at https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf at page 12.

[19] See "Welcome Address by Commissioner, Mr Tan Kiat How, at 53rd Asia Pacific Privacy Authorities Forum", 2 June 2020, available at https://www.pdpc.gov.sg/news-and-events/press-room/2020/06/welcome-by-commr-at-53rd-asia-pacific-privacy-authorities-forum-on-2-june-2020.

[20] The 2015 Amendments to the APPI entered into force in 2017. Under the Amended APPI, overseas transfers of data are permitted if the third party recipient of the data has a system of data protection that meets the standards prescribed by the PPC Ordinance, including whether the recipient has been certified under an international framework, recognized by the PPC, regarding its system of handling personal information. The PPC has recognized the APEC CBPR as such an international framework. See "Guidelines on the law concerning the protection of personal information (Provision to third parties in foreign countries)", available at https://www.ppc.go.jp/files/pdf/190123_guidelines02.pdf (in Japanese).

[21] Public Law 109-455: Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders (US SAFE WEB) Act of 2006, available at http://uscode.house.gov/statutes/pl/109/455.pdf.

[22] Cooperation Agreements, FTC, available at https://www.ftc.gov/policy/cooperation-agreements.

[23] Memorandum of Understanding on Antitrust Cooperation Between the United States Department of Justice and the United States Federal Trade Commission and the Ministry of Corporate Affairs (Government of India) and the Competition Commission of India, 27 September 2012, available at https://www.ftc.gov/system/files/1209indiamou.pdf.

[24] See Statement from the Press Secretary on the European Union–United States Privacy Shield Framework, 11 September 2019, available at https://www.whitehouse.gov/briefings-statements/statement-press-secretary-european-union-united-states-privacy-shield-framework/.

[25] *Supra* note 8.

[26] For a detailed explanation of the CBPR system, please see CIPL CBPR and PRP Q&A, 19 March 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf.

[27] See APEC Privacy Framework, available at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[28] See Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN and Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, available at https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf.

[29] See 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=en.

[30] India has previously expressed interest in joining APEC and its membership has come under repeated discussion within the Forum. India presently holds "observer" status within APEC. In 2011, the Obama administration invited India to participate as an observer, for the first time, in the annual APEC forum. See M. Lee "Clinton urges India to expand influence" Associated Press, 20 July 2011, available at https://web.archive.org/web/20150224145655/http://news.yahoo.com/clinton-urges-india-expand-influence-093840435.html (original link no longer available).

[31] APEC Cross-Border Privacy Enforcement Arrangement (CPEA), available at https://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement#:~:text=The%20APEC%20Cross%2Dborder%20Privacy,Authorities%20that%20enforce%20Privacy%20Laws).

[32] United States-Mexico-Canada Agreement, available at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[33] Agreement between the United States of America and Japan Concerning Digital Trade, effective 1 January 2020, available at https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

[34] *Supra* note 32, Article 19.8.

[35] *Id*.

[36] FACT SHEET on U.S.-Japan Digital Trade Agreement, October 2019, available at https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement.

[37] *Id*.

[38] Additionally, the United States is currently exploring a potential Federal privacy standard and numerous draft Bills are being put forward in the US Congress. As of the time of writing this report, it is not clear what direction a Federal privacy standard will take or if such a standard will leave sectoral laws in place.

# About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at **http://www.informationpolicycentre.com/.**

# About the Data Security Council of India

DSCI is a not-for-profit, industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities. For more information, please see DSCI's website at **https://www.dsci.in/**

CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

DSCI
PROMOTING DATA PROTECTION