Annexure

USISPF Submission

Draft Personal Data Protection Bill 2018

Members of the US-India Strategic Partnership Forum welcome a comprehensive data protection framework that will build consumer trust and confidence in the digital economy while facilitating the needs of business. This legislation will be a critical milestone in the development of India's digital economy as India realizes its aspirations to further its current global status as an IT/ITES leader and extend its leadership into new data-centric industries.

We appreciate the thorough consultations that the Government of India conducted as it prepared the Srikrishna Report and appreciate this opportunity to comment on the draft legislation. Our members offer the following comments to the Draft Personal Data Protection Bill 2018 released by the Expert Committee under Justice Srikrishna in July (the *Bill*). These comments are intended to provide detailed inputs for addressing legal, technical and operational implications of the bill.

CHAPTER I

Applicability

Section 2 of the Bill extends the reach of the law extraterritorially. However, the language of the Bill as it stands gives rise to significant chances of a conflict of laws, especially in jurisdictions where data fiduciaries and data principals have existing agreements subject to the law of the jurisdiction in which the data fiduciary is present. Thus, the Bill must account for the freedom to contract and validity of choice of law provisions.

Recommendations:

We recommend that it be clarified that the Act shall not apply to processing of personal data that a data principal and data fiduciary have contractually agreed to subject to the laws of another jurisdiction.

Definitions

Personal Data

Among the purposes of the Bill is a recognition of privacy as a fundamental right while also "ensuring empowerment, progress and innovation." Application of the law on any particular business will depend on whether the type of data it processes falls within the definition of "Personal Data". The definition of Personal Data was drafted broadly to include not only data that positively identifies an individual directly, but also,

> "indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information."

In practice, a broad definition will do little to enhance consumer privacy while imposing unwarranted costs and hindering companies' ability to conduct business operations, much less innovate. Specifically, the current definition establishes a binary test of identifiability with no regard to the level

of effort necessary to link the data to the individual. As data science advances, more and more data are potentially identifying, but whether someone would expend the resources to attempt identification varies based upon the level of effort as well as the benefit gained by such effort. For example, would a dataset be considered "personal data" if it required one thousand man-hours to identify one person out of a one million record database? And would the answer change if the result of such linking was his/her financial account information versus his/her restaurant ratings on a social network? Moreover, there is no qualification as to how identifiability can be achieved through "combination . . . with any other information". We submit that the "other information" should be legally available to the data fiduciary to qualify.

Recommendations:

Data should only be considered indirectly identifying if it is either the data fiduciary's intent to identify the individual, or if it is reasonable for someone to attempt to identify given the nature and context of the data, the level of effort to identify individuals, and the risk of harm to the individual. Where the level of effort to identify an individual is low and the risk of harm is high, the indirectly identifying information should be categorized as "personal data". On the other hand, if the level of effort is high and the risk of harm is low, the potentially identifiable data should not be considered personal data subject to the regulation. We recommend that the definition of "personal data" be modified as follows:

> "Personal data" means data about or relating to a natural person who is <u>reasonably</u> directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information."

The test of reasonability should be linked to "*objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*". Even countries such as Australia, Hong Kong and the Philippines require the data to be reasonably linked to the identified person for it to qualify as personal data.

We further recommend that business to business contact data may be excluded from the scope of "personal data."

<u>Anonymisation and De-identification</u>

The definition of "anonymisation" refers to the "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority". Further, the Srikrishna Committee and the Bill considers de-identified data (e.g. pseudonymised data) as personal data. These definitions and approaches are of concern because they do not consider a risk-based approach which considers the risk of re-identification. The preferred approach is to focus on taking reasonable steps to make it difficult to re-identify a data principal. These reasonable steps would include taking technical, operational, legal and administrative steps and controls to reduce the risk of re-identification to a minimal level.

Recommendations:

The word "irreversible" should be deleted from the definition of anonymisation.

A concept of reasonableness and risk-management should be incorporated into the definition of anonymisation.

"De-identification" should be considered as anonymisation provided that technological, administrative and legal controls are adopted. In other words, assuming that all reasonable steps are taken to mitigate the risks to the extent possible, de-identified data should be considered as "anonymised data". A standard similar to Recital 26 of the GDPR should be employed, which clarifies that to determine whether a natural person is identifiable, account should be taken of all the means "*reasonably likely to be used*…". The test of reasonability can be linked to "*objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*". The Bill could also take an approach to de-identification that is similar to the Health Insurance Portability and Accountability Act ("HIPAA") of the United States which prescribes two ways of achieving de-identification of data – one, if it has been determined by an expert to have very low risk of identification; two, if certain specific identifiers relating to the individual has been removed from their data (name, contact details, medical records, certificates, license numbers, etc.). When developing codes of practice under Section 61, the DPA could consider notifying the specific identifiers that have to be removed from the data set for it to qualify as de-identified data (and thereafter excluded from the purview of personal data).

Consequently, the obligations relating to personal data should not be applicable to this data – except for, a) the security measures aimed at keeping the data de-identified, and b) the penalties for re-identification of data.

A clarification should be added to the effect that nothing in the statute should be read to require a data fiduciary or processor to re-identify data that has been de-identified as above.

Sensitive Personal Data

"Sensitive personal data", which may only be processed in limited circumstances (requiring explicit consent in most instances), is broadly defined by the Bill. The inclusion of "passwords", "financial data" and "official identifiers" will frustrate many routine business functions. For example, this will include processing of financial data for debt recovery or employment purposes, or passwords for information security purposes.

It is worth noting that the Srikrishna Committee mentions that consent (let alone explicit consent) is not appropriate for a number of activities (e.g. employment, fraud, information security, etc.), and hence Chapter III of the Bill contains alternative non-consent-based grounds for processing, such as for employment purposes or reasonable purposes.

In addition, because consent may be withdrawn or refused, functions such as password verification, identity checks or fraud detection may be prevented entirely, making the Indian ecosystem less secure. Therefore, it is important not to have an expansive list of sensitive personal data.The Bill also includes "biometric data" within "sensitive personal data" which is defined as facial images, iris scans, fingerprints, etc., resulting from measurements and technical processing operations carried out on the data principal, confirming the unique identification of the data principal. A clarification may be added stating that the scope of "biometric data" is limited to that which is used for the purpose of authentication, and excludes pictures, videos and information derived therefrom.

Additionally, the inclusion of "caste or tribe" as sensitive data is extremely problematic, because such status can often be evident from an individual's name, which, of course, cannot be considered to be sensitive personal data.

Recommendations:

We recommend that passwords, financial data, official identifiers and caste or tribe be removed from the definition of "sensitive personal data" as prescribed in the Bill.

Harm

The Bill defines "harm" in an extremely broad and overarching manner. The present definition includes the following:

> (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
>
> (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled;"

This creates a risk of any evaluative decision that results in the denial of goods, services or benefits of a data subject, being classified as "harm" irrespective of whether the decision was taken in a fair manner.

The definition of harm further includes any restriction on speech, without any exceptions being made for legitimate exercises of censorship (such as by a social media platform for violation of their terms of use).

If the intent of the Bill is to prevent discrimination based on processing of the data principal's personal data, it must define and clarify the parameters and principles that organizations need to consider in evaluating denial or withdrawal of service resulting from evaluative decisions about the data principal. The current language as written would prevent organizations from withdrawing or denying services to data principals who may not meet certain risk or other evaluative criteria before certain services can be offered. Arguably, the provision would also prevent organizations from withdrawing or denying services to data principals that violate company policy or abuse the services offered.

Recommendations:

We propose amendments to these provisions that factor in an unfairness and unreasonability standard respectively.

We recommend rephrasing clause (viii) as "any denial or withdrawal of a service, benefit or good resulting from a discriminatory evaluative decision about the data principal" and clause (ix) as "any unreasonable restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled."

CHAPTER II

Notice

Section 8(1) of the Bill states that "the data fiduciary shall provide the data principal with the following information, no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable". There is a need to incorporate flexibility into the Bill to account for certain practical situations. For example, not all data fiduciaries which process personal data may have a direct relationship with the data principal, and it would be reasonable to expect the data fiduciary to rely on other data fiduciaries to provide the notice to the data principal. There may also be situations where a data fiduciary does not receive the personal data

from the data principal, but from a different entity, for instance where documents or packages are delivered through the postal department, or where authorisations are granted by the primary user of a service in favour of other users. Finally, a notice of the length required under Section 8(1) may not be appropriate for customer call hotlines, and it may be more reasonable to inform the data principal of the availability of a notice on a website.

Section 8(1)(g) requires the notice to mention the "individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared". The requirement to identify individuals imposes a considerable compliance burden on companies (as they would be required to track name changes of suppliers and third party partners). A reasonable approach would be for Section 8(1)(g) to require the listing of "categories" of individuals or entities.

Recommendations:

The Bill should allow data fiduciaries to take reasonable steps to provide the requisite notice, and that these reasonable steps could include contractually requiring another data fiduciary to provide the requisite notice and referring the data principal to an online notice.

Section 8(1)(g) should be revised to only require the listing of categories of individuals or entities.

Data Storage Limitation

Section 10(4) of the Bill prohibits data fiduciaries from retaining the personal data of a principal beyond the period necessary for delivery of the services for which such data was provided. However, given the prominence of Big Data analytics in the business models of most data fiduciaries, this greatly restricts their ability to use aggregated data to improve their quality of service or offer enhancements to their product.

Recommendations:

A balance may be struck between the protection of personal data and the benefits of data analytics for businesses as well as users by requiring that data that is retained after the initial necessary period is adequately de-identified, thereby minimizing privacy risks. Therefore section 10(4) should be amended to allow fiduciaries to retain personal data when such data has been de-identified in such a way that the data principal is no longer identified.

CHAPTER III

Grounds for Processing: Performance of a Contract

The Bill specifies the grounds on which "personal data" can be processed. It is to be noted that "consent" (which is defined in the Bill with legal requirements going over and above the requirements of contract law) is one of the grounds for processing. Other grounds include processing for functions of the state, compliance with law, purposes necessary for employment, and "reasonable purposes" to be notified.

The key concern is that contractual necessity is not a ground for processing of personal data under the present Bill. Comparable laws such as the GDPR provide exemptions from consent as a ground when processing is "necessary for the performance of a contract" when the data subject is party to such a contract, or in order to take steps at the request of the data subject prior to entering into a contract.

The non-inclusion of contractual necessity as a ground deprives service providers of a globally recognized ground for data processing and adds to the costs of compliance and may be extremely onerous for large and small companies alike to adhere to. It further deprives consumers of the autonomy to enter into contracts on terms whose implications they understand. For contractual necessity to be a ground for data processing, the data principal necessarily consents to the data processing by entering into a contract, or indicating a clear intent to enter into a contract, without which the data fiduciary cannot invoke this ground for undertaking activities involving processing of data. Thus, it is a recognition of user autonomy to consent, which the Bill does not recognize.
This omission is contrary to global best practices, and should be remedied in the interest of smooth functioning of the data economy.

Another issue is that the Bill provides for two levels of consent – for "personal data" under Section 12 and for "sensitive personal data" under Section 18. The dual requirements of consent and explicit consent need to be examined in light of whether they are sufficiently clear.

Recommendations:

An additional ground for processing of data should be added to Chapter III, which may be phrased in the language of the GDPR as follows: "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*."

Section 18 in Chapter IV may be reviewed for additional clarity on the extra steps that are required to be taken for qualifying consent as explicit.

The grounds for processing sensitive personal data should also include contractual necessity.

Grounds for Processing: Compliance with Law or Any Order for any Court of Tribunal

Section 14 provides a ground for processing personal data based on compliance with any law made by Parliament or any State Legislature, or compliance with any order or judgement of any Court or Tribunal in India. The law, however, would apply to multi-national companies that process the personal data of Indians. Such companies would also be subject to the laws of other countries that may require disclosure or other processing of their Indian employees or customers. To avoid the untenable position of requiring companies to choose which country's law they will violate, this ground for processing should be expanded to include compliance with any country's legal requirements.

Recommendations:
Section 14 data processing ground should be expanded to any duly passed law, rule, or regulation of any country or state or any binding order or judgment of any Court or Tribunal of any country or state.

Grounds for Processing: Purposes Related to Employment

Section 16 of the Bill provides for processing in various situations related to the employer/employee relationship. Section 16, sub-part (2), however, limits all of the permitted purposes by allowing them "only where processing on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort . . . " The limitation on the valid employment purpose injected by sub-part 2 creates substantial unwarranted uncertainty on businesses. The draft law is devoid of guidance to businesses on how to conduct the subjective evaluation of the limitations set forth in sub-part 2. As

a result, compliance with this legal ground will have significant variations across businesses. Large risk-adverse companies will likely always seek consent, but the vast majority of employers (and thus the vast number of employees) that do not employ in-house legal counsel or have budget for external legal guidance, will not seek employee consent. A two-tiered system of data protection pivoting upon the nature of Indians' employers should not be an appropriate solution.

More importantly, consent, as set forth in Section 12 as a basis for data processing, should be reserved for situations where the data principal and the data fiduciary have appropriate bargaining power. In the employer/employee context, the employee rarely has the requisite bargaining power to make the consent (as contemplated under Section 12) freely given.

Recommendations:
Remove sub-part (2) in Section 16.

Grounds for Processing: Reasonable Purposes

Section 17 of the Bill provides for processing of personal data for "reasonable purposes". While the introduction of a ground of processing in addition to consent is welcome, the current formulation of the reasonable purposes ground of processing does pose some challenges. These include the need for the Data Protection Authority (DPA) to specify the reasonable purposes (under Section 17(2) of the Bill).

The approach taken in the Bill is very limiting as it requires the DPA to list the activities which are considered as a "reasonable purpose". This introduces potential unnecessary inefficiencies as it relies on a review and listing of activities by the DPA, among all the other matters which the DPA is required to do. The "reasonable purposes" approach should instead rely on the benefit/risk assessments (which are auditable) which are performed by the data fiduciary. This approach allows for flexibility which in turn promotes efficiency and innovation while still ensuring that any negative impacts from the processing are minimized.

Recommendations:
The requirement for the DPA to specify the reasonable purposes under Section 17(2) of the Bill should be removed. In this regard, language based on the GDPR may be considered as a ground: "*processing is necessary for the purposes of the legitimate interests pursued by the data fiduciary, except where such interests are overridden by the interests or fundamental rights and freedoms of the data principal which require protection of personal data.*" We recommend extending this ground to the processing of sensitive personal data.

CHAPTER V

Processing of Child Data

The Bill does not recognise the varying maturity levels of children at different age groups. While parental/guardian approval makes sense for certain types of collection and use of personal data from children below the age of 13 years, young adults between the ages of 13 and 18 years should be permitted and empowered to make decisions about their data. We agree there are certain types of data use and targeting that rightfully create concerns for parents and should be subject to a consent regime. But just as the Bill should expand its definition of personal data processing for "reasonable purposes" rather than requiring DPA approval for all such purposes, businesses can and should be permitted to use certain types of personal data collected from children for legitimate, pro-consumer,

and benign purposes (such as recommending content) without obtaining parental consent as long as they limit the use of such personal data to those purposes. Requiring parental consent for any and all personal data collected from a child may in practice work to the detriment of children, as it would discourage businesses from offering beneficial content, products, and experiences for children due to the costs, complexities, and uncertainties attendant to compliance. For example, a prohibition on contextual ad serving would have a direct impact on businesses' ability to create and offer free ad-supported content appropriate for children. This would result in the exclusion of children from large parts of the Internet including valuable sources of information, learning, and communication.

Moreover, when combined with the apparent scope of the Bill, overbroad parental consent requirements could have unintended, harmful effects beyond the Internet, including in educational or other offline enrichment contexts. In a country such as India that is faced with challenges around adverse teacher-student ratio and capacity building of teachers, online courses and educational content provide a cost effective medium for bridging the educational gap for children. Creating restrictions for children in accessing educational content may lead to unwarranted obstacles and further increase this gap for the country.

In light of the Bill's broad definition of "profiling" section 23(5)'s outright prohibition of certain types of activities directed at children would appear to preclude businesses from engaging in certain beneficial activities altogether – with or without parental consent. Instead of banning a broad swath of activites outright, the Bill should identify a certain set of activities that trigger heightened concerns (such as online behavioural advertising) and require parental consent for such activities.

Recommendations:
The Bill should lower the age range requiring parental consent to children under the age of 13, and narrow the scope of activities that would trigger the need for parental consent for such children. Activities that are of concern should be subject to parental consent, not banned altogether.

CHAPTER VI

Data Principal Rights: Right to Portability

The Bill provides an elaborate set of rights to data principals, in order to balance the power deficit between data fiduciaries and principals. The Bill provides the Right to Portability [Section 26], stating that data principals have the right to receive their personal data that has been generated during provision of services or use of goods by the data fiduciary, or which forms part of any profile on the data principal.

From a plain reading, this provision seems to include processed or derived data in its ambit. This potentially means that the data acquired by the data fiduciary after running proprietary processing software and algorithms, which forms a part of the data fiduciary's intellectual property, may have to be shared with the data principal. This provision, thus, gives rise to concerns regarding the intellectual property rights of data fiduciaries, and requires necessary modification.

A right to portability which requires the transfers of data relating to fraud prevention and information security may negatively impact the effectiveness of fraud prevention and security systems.

Recommendations:

Derived data should be excluded from the ambit of the personal data that data principals have a right to receive from data fiduciaries. Further, the exception relating to trade secrets needs to be broadened to include details of proprietary or confidential technology used by the data fiduciary to generate any data about the data principal.

Similar to the CCPA (California Data Protection Law), the right should only be allowed to be exercised twice in a 12-month period. This would reduce the regulatory load on the DPA and be commercially reasonable for the data fiduciary.

CHAPTER VII

Transparency

Section 30 sets forth certain transparency obligations on data fiduciaries. Sub-part (1) requires disclosures of certain data types "as may be specified" and sub-part (2) obligates "periodic notifications" "in such manner as may be specified". Our concerns are two-fold: First, it is not clear how Section 30, Transparency, is related to Section 8, Notice. Both sections share the goal of empowering data principals with information about the data processing of the data fiduciary. It is therefore unclear as to the need for both overlapping sections. Second, the process of who and how the obligations under both sub-sections will be "specified" deserves clarification. To the extent that it will be the DPA that is making such specifications, we suggest that it is improper to vest in a non-legislative branch the power to both draft significant portions of the law as well as enforce the law.

Recommendations:

Section 30(1) and Section 8 have significant overlaps, with the key difference being that the latter is formal and more definitive and presecriptive. Section 30(1) should be reconsidered in its entirety.

Section 30(2) is overly broad, leaving a lot to the determination of the data fiduciary and therefore increasing the risk of non-compliance.

To the extent that Section 30 is retained, the specifications required should be decided by the DPA in a manner that allows public consultation and participation.

Data Breach Notification

The current threshold for breach notifications under Section 32(1) of the Bill is too low. It currently requires notification to the DPA of "any personal data breach… where such breach is likely to cause harm to any data principal" regardless of the nature or degree of the harm. "Harm" is defined broadly in Section 3(21) to include subjective evaluations such as "loss of reputation, or humiliation". Without a qualifier as to the degree of harm necessary to trigger the notice obligation, any slight or trivial infraction of the inherently subjective reputation or humiliation would trigger the notice. Notification for personal data breaches should be required where this would result in serious harm to the individual, otherwise, this would only result in unnecessary notifications, and unnecessary compliance burden on companies and the data protection officer.

Recommendations:

The requirement to notify the DPA of any personal data breach should only apply where such breach is likely to cause "serious harm" to any affected data principal. For example, the GDPR mandates notification of a data breach to the data subject only in a situation where there is "high risk" to the subject. Such notifications may not be required when the data controller has implemented appropriate technical and organisational protection measures, or has taken subsequent measures which ensure that the high risk is no longer likely to materialise, or it would involve disproportionate effort. The Bill should adopt a similar approach.

Data Protection Impact Assessments (DPIAs)

Section 33(4) of the Bill requires that all DPIAs must be submitted to the DPA. This requirement only serves to impose considerable administrative burden on data fiduciaries in submitting the DPIAs, without any evident benefit for the data principal. In any event, the DPA may exercise its information gathering powers to obtain DPIAs on a request basis. Further this may also lead to unwarranted delays in enabling business operations in case of a capacity constraint at the DPA level.

Recommendations:

Remove the requirement under Section 33(4) to submit all DPIAs to the DPA.

Data Audits

Section 35 requires data fiduciaries to have their policies and processes audited annually by an independent auditor and directs the DPA to designate certain institutions as appropriate auditors. It will be challenging for an auditor to conduct a review of organizations' systems located outside of India. In addition, setting up a program of approved auditors and administering a program whereby the DPA oversees the auditors and ensures consistency will be challenging and unnecessarily bureaucratic. Further, the value of the trust score is questionable and it's unclear what the DPA will do with the assigned "rating in the form of a data trust score" and whether that rating will be made public.

Recommendations:

Adopt a self-certification approach for data fiduciaries, which is subject to audit. Modify the trust score concept to be a voluntary program.

Significant Data Fiduciaries

Section 38 of the Bill states that the statutory authority will notify "significant" data fiduciaries, who would have additional obligations under the law, such as data protection impact assessment, record keeping, data audits and appointing a data protection officer.

Our key concerns are:

(i) Vesting the power in the DPA to designate certain companies and/or industries as "significant" data fiduciaries with only minimal guidelines will likely lead to significant uncertainty and undue risk of inconsistent and arbitrary decision-making. Open questions include: What is the process for the DPA's designations? Will the public and the relevant companies and/or industries have an opportunity for comment? Will companies/industries have an opportunity to appeal the decisions? Once designated, what is the time-frame for companies to comply with the substantially enhanced obligations? We submit that any enhanced privacy protections are questions for the legislature in open and public debate, not questions for the DPA charged with enforcement of the law.

(ii) The factors to be taken into account to determine who constitutes "significant" data fiduciaries include turnover and use of new technologies. These criteria, in addition to being arbitrary in the sense of having no nexus with data protection violation risks, also have the result of discouraging use of new technology. One of the stated aims of the government's Digital India mission is to make India a hub of digital innovation, which is entirely at odds with a legal provision in the Bill that explicitly discourages innovation.

Recommendations:

(i) There should not be two categories of data fiduciaries based on the criteria that have been specified in the Bill. Instead, we recommend a harm-based approach where additional

responsibilities, if any, are imposed based on whether there is a significant potential for harm based upon criteria set forth in the law (such as processing of sensitive personal data, or sensitive uses such as credit evaluations).

(ii) In the alternate, the categories of turnover and use of new technologies should be removed, as these categories are irrelevant to an assessment of harm in the context of data protection.

(iii) The requirements applicable on significant data fiduciaries, if the category is retained, should be reconsidered and rationalized in line with global standards. For example, a residency requirement for Data Protection Officer ("DPO") is out of line with global practices and should not be mandated. Futher, data trust scores are highly subjective and should not be mandated by law.

CHAPTER VIII

Data Localisation

It is well-recognised that the ease with which cross-border data transfers occur has been a significant contributor to the success of modern globalised economies. This becomes especially pertinent in relation to economies such as India where outsourcing and the export of services are among the largest contributors to GDP. For India to continue to grow its IT, ITeS, and outsourcing sectors, and expand into new data-intensive industries serving global markets, cross-border data flows are a critical driver, which must be encouraged and preserved.

The Ministry of Electronics and Information Technology ("MeitY") estimates that India's IT-ITES exports were U.S. $117 billion in fiscal year 2016-2017, growing by 8.5% over fiscal year 2015-2016. According to MeitY, this growth resulted, in part, from technologies such as social media, mobility, analytics, cloud services, artificial intelligence, and embedded systems. All of these technologies rely on the international flow of information in order to function and to grow. McKinsey estimates that cross border data flows have added more than 10% to world GDP, and the European Centre for International Political Economy ("ECIPE") estimates that if India were to implement economy-wide data localisation requirements, India would lose more than U.S. $15 billion in GDP annually.

Our concerns are:

(i) Section 40(1) of the Bill mandates storage of at least one "serving" copy of all personal data within India. The term "serving copy" is not defined in the Bill, but the Srikrishna Committee Report refers to it as a "live" copy.

Though the stated aim of the Bill is to address data protection, it proposes to add rules that would mandate localisation without any evidence of corresponding benefits in terms of protecting personal data. As one of the dissenting notes to the Srikrishna Committee Report states: "*The requirement that every data fiduciary should store one live, serving copy of personal data in India is against the basic philosophy of the Internet and imposes additional costs on data fiduciaries without a proportional benefit in advancing the cause of data protection*." The dissenting notes also state that: "*the inclusion of such restrictions in a bill that should focus primarily on empowering Indians with rights and remedies to uphold their right to privacy, seems out of place*."

(ii) Section 40 (2) of the Bill completely restricts the cross-border flow of categories of data which would be notified by the Central Government as "critical personal data." Despite the potentially enormous economic impact of such a hard localisation policy, the text of the Bill contains no guidelines as to what would constitute "critical personal data." This may raise

concerns regarding excessive delegation by the legislature. The Supreme Court in this regard has clearly held that "*where a statute confers a power on an authority to decide matters of moment without laying down any guidelines or principles or norms the power has to be struck down as being violative of Article 14 [of the Indian Constitution]*."[1]

(iii) TRAI in its recent "*Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector*" released in July 2018 took note of various advantages and disadvantages of a localization policy. Some of the disadvantages noted were as follows: creating very high costs for service providers, discouraging investment, functioning as a trade barrier which may induce other countries to take similar steps, and leading to inferior quality of service due to interplay of various platforms. It also noted the impact that such a provision may have on delaying innovation and undermining competitiveness. Based on this assessment, it did not see any of the benefits of data localization outweighing the costs. Hence it refrained from recommending restrictions on cross border data flows.

(iv) The Srikrishna Committee Report's justification for the localization measure, namely, easier access to data for law enforcement purposes does not necessarily hold under law as:

- In the case of foreign companies required to retain a serving copy in India, the existence of the copy of data may not automatically allow them to be accessed by Indian authorities without due procedure. The mere presence of data within the territory of India may not lead to easier access to data for law enforcement, and the costs to consumers may be potentially much higher than the limited and uncertain benefits that may arise in this regard. In fact, in this context, it is important to note that the recent Supreme Court judgement[2] on the Aadhaar (Targeted Delivery of Financial Benefits and Other Subsidies, Benefits, and Services) Act, 2016 ("Aadhaar Act, 2016"), has ensured that unfettered access to citizens data under Section 33(2) is no longer automatically permited even if data is sought for national security purposes. In striking this provision down in its entirety, the Supreme Court has delieneated a clear and high standard of needing due process safeguards, such as judicial review, when it comes to accessing an individual's data even if it is for national security purposes.
- In the case of Indian companies seeking to store their data abroad instead of in India, they can be compelled to produce data by following the procedures under existing criminal law and company law, without the requirement for localization.

Thus, mandating localisation does not automatically create access for law enforcement and that such access has to be subject to due process safeguards to meet the highest standard.

Recommendations:

(i) In Section 40(1), the term "serving" should be deleted as this does not have a definition in the Bill and could lead to needless ambiguities.

(ii) Instead of mandating the storage of one copy of personal data in all cases, there should be a case-specific determination of the same based on requirements arising in particular situations. The criteria for these should be stated in the Bill through an addition to Section 40(1). These conditions should be very specific towards those areas which impact national security and / or other sensitive information which may be detrimental to the nation's security.

(iii) There should be no requirement of hard localization under Section 40(2), as this imposes prohibitive costs on service providers as well as consumers. In the event that this is necessary

[1] *AIR India vs. Nergesh Meerza and Ors.* AIR 1981 SC 1829 (Para 118)
[2] *Justice K.S. Puttaswamy (Retd.) and Ors. Versus Union Of India And Ors*. (W.P.(C) 494/2012)

for specific national security purposes, the same should be clearly defined within the Bill, should not be left to the unfettered discretion of the Central Government and should be subject to the stringent due process requirements that includes judicial scrutiny. We note the recent judgement of the Supreme Court where it struck down Section 33(2) of the Aadhaar Act, 2016, a provision which used "national security" as a justification for personal data disclosure. This provision was struck down given the absence of judicial oversight over the process in which law enforcement gains access to data.

(iv) The Bill should also provide that hard localization cannot be imposed for any reasons other than the national security interests specified therein, in order to avoid the use of such a provision for protectionist purposes.

Data Transfer

The Bill empowers the Central Government to notify categories of personal data that may be processed *only* in India.

(i) There are significant implications to the combination of the territorial jurisdiction and scope of the Bill. For example, many organisations use their Indian operations to support processing for both internal clients (e.g. employees) and external clients (e.g. customers) for a range of reasons including for back-office or customer support and internal reporting and analytics. This could be done via remotely accessing datasets which are located overseas and would be considered as "processing" under the Bill. The implication of this is that the overseas dataset would fall under the scope of the Bill and hence be subject to the requirements under Section 40(1) and (2) of the Bill. There is also considerable uncertainty as to whether Section 40(1) and (2) of the Bill would include data of foreign citizens which is processed by data fiduciaries in India. Any requirement to process foreign citizen data only in India would prevent companies from meeting their own legal auditing and regulatory reporting obligations in the other countries in which they operate.

(ii) The conditions for cross-border transfer of personal data under Section 41 are onerous. One of the potential grounds for transfer is that standard contractual clauses or intra group schemes have been approved by the statutory authority. In the alternative, another possible condition is that the Central Government, after consultation with the DPA, may prescribe that transfers to a certain country or within a sector, etc. are permissible. As a practical matter, this would likely cause significant logistical issues for the Central Government and DPA, as the DPA would have to be equipped to deal with a deluge of approvals. A mere stumble or delay by the DPA could lead to severe delays which would be fatal to most industries that rely on quick and smooth data transfers and processing.

(iii) The Bill states that data can be transferred abroad if the data principal has consented to the same, in addition to (a) transfer being made pursuant to pre-approved clauses; or (b) transfers to a particular country or sector being permitted by the Central Government. This makes the role of consent quite unclear and seemingly irrelevant.

In practice and in modern data protection regulatory frameworks (e.g. Article 49 of the GDPR), consent is a separate and alternative cross-border data transfer mechanism. In many situations, companies will rely on intra-group schemes (e.g. binding corporate rules) to engage in cross-border data transfers for the processing of employee data (e.g. for processing of benefits, career development and performance reviews). Companies may also rely on the reasonable purposes ground under Section 17 of the Bill to process personal data (e.g. for internal investigations, information security purposes). In these situations, consent is not

appropriate, and should therefore not be required under Section 41(d) or (e) of the Bill. Thus, we recommend that consent or explicit consent (depending on the nature of data) should be a separate ground for transfer of data and should be delinked from the standard contractual clauses requirement.

Recommendations:

(i) The conditions for transfer of data abroad should be suitably modified to remove the ambiguity in the present draft. Section 41 (c) should be appropriately modified to state that *" a particular transfer or set of transfers is permissible due to necessity or when intrinsic to the business".*

(ii) The words "in addition to clause (a) or (b) being satisfied" in Sections 41 (d) and (e) should be removed so as to make consent or explicit consent a separate ground for data transfer, delinked from any of the other requirements.

CHAPTER IX

Exemptions: Research Purposes

There is a requirement for approval from the DPA even for processing personal data for research, archiving or statistical purposes. It is important that a research exemption should not be limited to what is permitted by the DPA, and that the researcher should be in a position to determine the same, subject to investigative powers of the DPA.

Recommendations:

Remove the term "as the Authority may specify" from Section 45(1).

CHAPTER X

Data Protection Authority (DPA)

The Bill establishes the DPA, and envisages it in the roles of a regulatory body, an enforcement agency, a certifying authority, a standard setting body, as well as an adjudicatory authority. The Bill provides for the appointment of a chairperson and six members. In light of its manifold responsibilities and functions, the DPA's composition, technical ability and autonomy are vital for the success of an effective data protection framework. The Bill accords vast powers and discretion to this body, which is concerning for the following reasons:

i. Composition:

- The Bill provides only skeletal qualifications for the chairperson and members of the DPA, primarily requiring at least ten years of professional experience in relevant areas. Further, it is entirely silent on the necessary qualifications for the officers, employees, consultants and experts.
- The Bill grants a crucial role to Adjudicating Officers, who are responsible for conducting inquiry and adjudication. The qualification for these officers is also limited to specifying seven years of professional experience in certain relevant areas. It is apparent that the present version of the Bill does not prioritize these details adequately and must give statutory status to other important eligibility criteria.

ii. Designation Powers: The DPA has the power to specify categories of sensitive personal data. Such designations will have significant implications for data fiduciaries that process sensitive personal data. The DPA should be required to consult with stakeholders and data fiduciaries prior to issuing these notifications and specifications.

iii. Search and Seizure Powers: The DPA has been granted wide search and seizure powers by the Bill, allowing it to search and seize a business's property on the basis of 'reasonable grounds' to believe that a business has or is likely to violate the law. This is a draconian power that may be exercised without any judicial oversight and would lead to a high level of government intrusion. Such powers must be made subject to oversight similar to other regulators who exercise search and seizure powers, for instance the Competition Commission of India, which must make an application before the Metropolitan Magistrate before proceeding. Moreover, the 'reasonable grounds' standard should be changed to a 'probable cause' standard to ensure that arbitrary search and seizure isn't a threat to businesses.

Recommendations:

(i) The qualifications for the members and other staff of the DPA, including the Adjudicating Officers and all other employees, consultants and experts must be included in the law to ensure adequate technical competence.

(ii) The vast delegated legislative powers of the DPA should have set limits to prevent executive over-reach and conserve the spirit of the law.

(iii) The DPA should be obliged to consult stakeholders and data fiduciaries prior to exercising its powers of designating categories of sensitive personal data.

(iv) The search and seizure powers of the DPA must be subjected to judicial oversight, through a provision mirroring Section 41 of the Competition Act, which requires an application to be made to the Metropolitan Magistrate. Moreover, the 'reasonable grounds' standard should be moved to a stricter 'probable cause' standard.

CHAPTER XI

Penalties

The Bill adopts an unreasonable and arbitrary approach to penalties for violations under the proposed regime. Notably, penalties may extend to as high as 4% of worldwide turnover of an entity in default in addition to criminal liability for certain offences. By linking penal sanctions to 'worldwide' revenue, the Bill also adopts an irrelevant consideration in place of the actual harm that any non-compliance may have caused an entity. For this reason, the current approach may also fall short of constitutional safeguards which require penalties to be 'proportionate' and linked to the extent of the guilty conduct.

As the Supreme Court of India has, for example, stated in the Competition Act context:

> *"…It should be noted that any penal law imposing punishment is made for general good of the society. As a part of equitable consideration,* ***we should strive to only punish those who deserve it and to the extent of their guilt.*** *Further it is well established by this Court that the principle of proportionality requires the* ***fine imposed must not exceed what is appropriate and necessary for attaining the object pursued****…."*[3]

[3] Civil Appeal No. 2480 of 2014 (Decided on May 08, 2017; Supreme Court of India)

The Bill also prescribes criminal penalties in addition to civil penalties and compensation. This is likely to cause unease amongst businesses, and may lead to a situation where there might be a reluctance or delay in disclosing any breaches for fear of such criminal liability.

Recommendations:

The Bill should contain a fixed cap on penalties that may be levied and the same should be computed based on the articulated harm caused to an entity arising from such non-compliance. Such an approach would provide sufficient deterrent value for organisations while, at the same time, ensuring that entities are only penalised based on relevant considerations.

CHAPTER XIII

Offenses by Companies

The Bill (Section 95) considers the scenario when a company is in violation of the provisions of the Bill. It holds that when a company contravenes any provision, every person who was in charge and had responsibility for the company will be deemed to be guilty of the offence. Further, the Bill places the burden of proving innocence on the person instead of on the prosecution. This provision is unduly harsh and exposes persons who are innocent and uninvolved in the matter to legal proceedings, thereby causing not just distress but also threat of monetary and legal harm.

Recommendations:
We recommend removing from Chapter XIII the principle under which individuals would be held liable or responsible and potentially face imprisonment and move towards a framework of reasonable and proportional fines and compounding. This is an approach being adopted by the Government of India today in the context of the Indian corporate governance framework, the Companies Act. This would also automatically mean that the burden of proof will not be on the person in charge.

CHAPTER XIV

Transitional Provisions

The Bill does not provide sufficient time for data fiduciaries and data processors to comply with the requirements. The Bill provides for a 12-month period from a notified date for the DPA to issue essential codes of practice and specify the list of activities that qualify as reasonable purposes under Section 17. This gives data fiduciaries and data processors 6 months to make changes to comply with the requirements set out in the codes of practice which would set out the detailed standards expected by the DPA.

In order to provide data fiduciaries and data processors with sufficient time to comply with the requirements of the Bill (e.g. implement technology, operational, legal and administrative changes), the effective date of the Bill should be at least 3 years from the notified date.

Recommendations:

The effective date of the Bill should be at least 3 years from the notified date of the Bill.

CONCLUSION

As the government works to finalize the law, we encourage incorporating the concept of self-regulation and consultative rule-making into the Bill**.** It's important to consider the evolution of

technology and consumer preferences still to come in a new privacy framework. Trying to determine and codify the broadest set of rules from the outset can put this evolution at risk. This approach also discounts the value of future rule-making procedures that can be consultative with broad groups of stakeholders and more responsive to changes in technology, society, and the economy.

The broad scope and impact of the current draft law does not strike an effective balance with the necessary self-regulatory practices that will need to be part of every privacy regime. A revised bill that makes more space for self-regulation and places a greater emphasis on industry codes of conduct will result in more innovative and effective solutions for protecting consumers.

A more flexible approach that makes room for self-regulation and adaptations through future proceedings can facilitate improved transparency, better control mechanisms for consumers, more effective audit and enforcement approaches, and a much greater potential for innovation that benefits consumers.

While the Bill is a welcome step and we are committed to its stated aims, we encourage the Government to engage in meaningful discussions with industry prior to adopting any regulatory reform. We want to ensure that we can work together with the Government of India to address the above concerns in the Bill. We recommend that any draft bill be harmonized with international best practices in order to protect the data of its citizens, promote investment and facilitate ease of doing business.