USINDIA BUSINESS COUNCIL

TEL: 202-463-5679 | FAX: 202-463-3173 | usibc@uschamber.com

September 30, 2018

The Joint Secretary
Ministry of Electronics and Information Technology (MeitY)
Electronics Niketan, 6, CGO Complex, Lodhi Road
New Delhi 110003

Re: USIBC Comments on MeitY Draft Data Protection Bill and Report of the Committee of Experts

Dear Joint Secretary:

The U.S.-India Business Council (USIBC) appreciates the opportunity to provide comments on the Draft Data Protection Bill (Draft Bill) and the accompanying report from the Committee of Experts. We congratulate the Ministry on taking an important step towards achieving this important policy goal by releasing the draft legislation and accompanying report.

Developing a privacy regime requires taking a judicious and thoughtful approach that draws on global best principles and practices that balance privacy, innovation and global interoperability, while designing a regime that is aligned to work within existing legal structures in an effective and efficient manner. The U.S. Chamber of Commerce has developed a set of privacy principles to help achieve a privacy framework that is balanced, flexible, globally interoperable, and protects the free movement of data while protecting consumers:

1. A comprehensive framework of regulation that ensures certainty and consistency
2. Risk-focused and contextual privacy protections
3. Transparency in collection, uses and sharing of consumer data
4. Industry neutrality
5. Flexibility to develop adaptable, consumer-friend privacy programs
6. Harm-focused enforcement
7. Enforcement that promotes efficient and collaborative compliance
8. International leadership that promotes the free flow of data and interoperability between global frameworks
9. Encouragement for privacy innovation
10. Risk-based approaches to data security and breach notification

Creating a privacy framework that is balanced, flexible, globally interoperable, and ensures the free movement of data while protecting consumers is central to India's digital transformation, the promotion of India's global competitiveness, and the *Digital India* vision of the Prime Minister. We are concerned that elements of the draft legislation will hinder India's ability to realize these goals.

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

U.S. CHAMBER OF COMMERCE

In some areas, the draft takes an excessively onerous approach to privacy and data protection regulation that will needlessly impede the free flow of digital commerce without providing meaningful privacy protections to consumers. This approach would burden all participants in India's digital economy, but it would have disproportionate economic impacts on small- and medium-sized enterprises (SMEs) and entrepreneurs.

Also MeitY should assess the very recent Supreme Court ruling on Aadhaar, where the judgment limited access to Aadhaar data by law enforcement even under the aegis of national security. MeitY, therefore, should assess this ruling as it considers law enforcement access to other types of user data based on this new legal standard. The ruling also impacts private sector access to Aadhaar data, and thus could impact privacy related to the program, as well as the privacy related to biometric information more generally.

In this letter, we offer our comments on the draft legislation and accompanying report, and suggest reforms that would bring the draft legislation more into line with international best practices and help the draft succeed in achieving India's goals in the digital economy.

The following represent USIBC's top recommendations for the draft law to ensure a privacy regime that bears in mind the important economic benefits created by flexible approaches to the use of data, and the importance of enabling cross-border data flows:

- ***Remove the data localization requirement and moderate onward transfer restrictions***. At present, the Draft Bill includes an extremely broad data localization provision that will impose significant burdens on all global businesses operating in India.

- ***Expand grounds for data processing***. The current Draft Bill requires data fiduciaries to wait for regulatory approval before they can rely on the "reasonable purpose" ground for processing, which raises significant practical issues, in particular in terms of predictability. In addition, in keeping with the approach adopted by the European Union's General Data Protection Regulation (GDPR) and longstanding data protection laws around the world, India should recognize that processing to fulfill contractual obligations is lawful processing.

- ***Clarify that the law would not apply to foreign national data processing***. The bill should exempt all companies that process data only of foreign nationals. Restricting this exception would undermine the global digital marketplace and India's business process outsourcing industry.

- ***Clarify the definitions of personal data and anonymized data***. Under the Draft Bill's approach, if there is any possibility that data could be used to identify a person—no matter how remote that risk is—that data qualifies as personal data. Current definitions around personal data are too broad and ambiguous. Instead, India should recognize international best practices and approaches to anonymization that permit data fiduciaries to engage in "reasonable efforts" to de-identify data.

- ***Eliminate residency requirement for data protection officer (DPO)***. This requirement imposes substantial and unnecessary costs on foreign companies, who must hire an India-based DPO even if they already employ a DPO in another country.

- ***Reform restrictions on processing data of under-18s***. The Draft Bill defines "child" as anyone under the age of 18, without recognizing the significant distinctions between those aged 17 and those aged 12. We suggest a more reasonable threshold.

- ***Reform excessive penalties***. The Draft Bill's civil penalties, and its provisions holding any executive criminally liable for involvement in any processing of data found to violate its terms, are excessive and will encourage companies to avoid doing business in India. We believe that more emphasis should be put on accountability measures – already acknowledged by the Draft Bill – as a powerful factor to mitigate and minimize privacy risks.

- ***Provide sufficient time for implementation***. The bill does not provide for sufficient time for implementation of the requirements. The data protection authority (DPA) may issue codes of practice on several important matters up to 12 months from the notified date, which leaves only 6 months for data fiduciaries and data processors to implement changes required by these codes of practice.

USIBC appreciates the challenge ahead – and indeed the larger global privacy discussions before us. We stand committed to assist you in your efforts. USIBC and our members hope that our comments will be given a timely and sympathetic consideration. We welcome an opportunity to meet you at your convenience, and are happy to provide further information or clarification in relation to the issues in this representation. In the meanwhile, please do not hesitate to contact me or my staff: Jay Gullish, jgullish@usibc.com, in Washington, D.C., and Abhishek Kishore, akishore@usibc.com, in New Delhi. I would like to personally thank you for your leadership, and the Council and its members hope to discuss these recommendations at your convenience.

Sincerely,

Nisha Biswal
President, U.S.-India Business Council
U.S. Chamber of Commerce
1615 H Street, NW
Washington, D.C. 20062
Tel. (202) 463-5612

1. DATA LOCALIZATION

Under the Draft Bill, data fiduciaries must store, on a server or data center located in India, at least one copy of personal data to which this Act applies. In addition, if the government designates a category of personal data as "critical" it must be processed only in a server or data center located in India. The Committee's proposal would authorize the government to exempt "certain categories of personal data" from the data localization requirement "on the grounds of necessity or strategic interests of the State." However, the government cannot exempt sensitive data from this requirement.

Restrictions on the cross-border transfer of personal data in the form of data localization requirements do not advance data protection goals. Instead, they disrupt companies' operations, and make it more costly to provide services in India, even as an unintended consequence.

USIBC urges that this provision be removed. The Committee set out to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." However, the data localization requirement undermines both of those goals in a number of respects:

- *First*, requiring that data fiduciaries store data in an additional location actually amplifies, rather than reduces, security vulnerabilities, as increasing the number of locations in which data is stored makes it the more difficult to protect. Any personal data stored outside India will already be afforded appropriate protections under standard contractual clauses and other protections in Article 41. Effective cybersecurity defenses rely on having timely access to global sources of ongoing threat information and the ability to synthesize the collected information into actionable intelligence for security products and services. The undue restrictions on the flow of data will limit the types of information that can be drawn on for analysis and correlation and leave end users more vulnerable to new attacks that continue to surface on a daily basis. In particular, if global cyber threat analysis centers are unable to evaluate relevant cybersecurity threat activity occurring in India, the visibility and ability to detect and mitigate against emerging cyber threats in India will be severely reduced. With the increasing sophistication of cyber-attacks, any move to interfere with data flows that tend towards increased centralization also may multiply the damage caused by a successful attack.

- *Second*, by forcing companies to build or buy storage space in India, data localization would impose substantial costs on foreign companies that maintain data centers outside of India. Maintaining separate local servers also may not be possible or practical with the network architecture of some global companies. Localization may prompt foreign companies to exit the Indian market and may discourage entrepreneurs from making new investments in India. Such a move will tangibly harm businesses as well as the reputation of India as an innovation hub.

- *Third*, this provision raises the threat of other states employing retaliatory localization measures, could destabilize the Indian information technology (IT) sector, and could result in irreversible harm to Indian

national and economic interests. Data localization would undermine India's $167 billion IT sector, and inhibit the goal of creating a $1 trillion digital economy. India is a global digital leader, and increasingly, Indian companies are investing and exporting digital products and services abroad. Furthermore, India is a net importer of data managed in its outsourcing market, which remains at the core of its expanding digital sector. Data localization could directly result in retaliatory measures, and raise costs for Indian companies conducting digital business abroad.

- *Fourth,* data localization would severely inhibit competition and the choice of technology available in India to end-users and procuring entities, including start-ups and government agencies.

- *Fifth*, if the government's concern is related to ensuring access to Indians' personal data, there are other legal mechanisms that should be used to facilitate the government's access to data stored in other jurisdictions, such as improving the mutual legal assistance treaty (MLAT) system or entering into specific agreements with countries. Australia can serve as an example as to how to handle security and access to personal data for law enforcement purposes. Rather than requiring data localization, the Australian government imposes a data retention requirement and a duty to respond to law enforcement requests.00

In sum, because a broad data localization regulation mandating that "every data fiduciary shall ensure the storage, on a server or data center located in India, of at least one serving copy of personal data" would conflict with India's stated objectives of promoting privacy, data security, and innovation. MeitY should reject this provision. Where localization is necessary to achieve specific security or strategic objectives (e.g. in relation to defense), we encourage the government to specify categories of personal data for which the benefits of localization outweigh the costs to privacy, security, and innovation. USIBC and its members would appreciate the opportunity to participate in an inclusive consultation process for the same.

2. ONWARD TRANSFER

Cross-border transfer restrictions do not significantly enhance data security or privacy, but impose significant burdens on the digital sector. For India to continue to grow its technology and outsourcing sectors in a global marketplace, cross-border data flows are a critical driver which must be encouraged and preserved. For example, according to NASSCOM estimates IT-ITES exports out of India were $126 billion in fiscal year 2017-2018, growing by 7.8% over fiscal year 2016-2017.[1] According to MeitY, this growth resulted, in part, from disruptive 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 grow. McKinsey estimates that cross border data flows have added more than 10% to world gross domestic product (GDP), and the European Centre for International Political Economy (ECIPE) estimates that if India were to

[1] https://www.nasscom.in/sites/default/files/NASSCOM-annual-guidance-fy-2018.pdf

implement economy-wide data localization requirements, India would lose more than U.S. $15 billion in GDP annually.

The Draft Bill suggests an "entity-led transfer" model, emphasizing model contracts and intra-group schemes as the primary vehicles of cross-border data transfer. However, each of these approaches has limitations. Requiring authority-approved contract clauses may be effective for simple transactions, but will create administrative challenges for more complex international transactions. Consistent with international best practices, transfers should be allowed when the controller proves that the transfer is based on standard contractual clauses recognized under internationally accepted rules or codes of conduct. In addition, the Draft Bill should allow data transfers as pursuant to the recognized codes of practice, seals, and/or certificates outlined in Article 61 that could be certified by the competent authority or a third party.

As for intra-group schemes, based on recent experiences with the GDPR's binding corporate rules (BCR) model, approval under this model is costly and time-intensive for fiduciaries and regulators alike. As of May 2018, the European Union (EU) had fully processed only a short list of BCRs under the GDPR. Due to the burden of this model, many companies may opt to avoid Indian markets rather than incur the added administrative costs and uncertainty.

In addition, the Draft Bill mandates that data principals be required to provide a mandatory consent before their data can be transferred out of India. However, data fiduciaries already need to identify a lawful basis for the type of processing in question—regardless of where the data is transferred. We suggest that this responsibility of data fiduciaries to ensure lawful processing of data should be entirely sufficient to ensure the integrity of the data of Indian data subjects. This approach is used by Canada (a country with EU adequacy), as well as many other countries. Layering on a separate level of empty regulatory burdens will only serve to slow business and impede India's digital progress, while adding nothing of substance to the protection of the personal data of Indians.

The potential harms of restricting cross-border data flows outweigh purported benefits to the security of the information. Not only would the business models of several Indian companies become unviable, but interference with data flows would raise the costs of doing business in India for multinationals, SMEs, and early-stage companies.

3. LAWFUL BASES FOR PROCESSING PERSONAL DATA

First, the Draft Bill appropriately suggests that India's data protection regime provide multiple bases for processing personal data. However, the proposed bill does not include, as a lawful basis, processing to fulfill a contractual obligation. USIBC is concerned that this will create unnecessary barriers for commerce. Assuming that a consumer has provided valid consent to a contract, India's data protection law should not require a second layer of consent. Such an approach does nothing to protect consumers, who will have consented by agreeing to the contract initially, and imposes a new consent that is superfluous (and will confusing to consumers). In

keeping with the approach adopted by GDPR and other data protection regimes, India should adopt contractual obligations as an additional ground for processing.

Second, to avoid any confusion, there should be a range of permissible bases for processing of "sensitive personal data." Similarly, processing of sensitive personal data for employment related purposes such as pre-screening of employees and contingent labor should also be a valid ground of processing. With passwords, financial data, health data classified as sensitive personal data, additional grounds of processing should also be included. Currently "reasonable purpose" cannot be used as a ground for processing sensitive personal data. Requiring express consent for sensitive personal data will make unduly complicate and overwhelm data subjects. If this cannot be reconsidered, then the definition of sensitive personal information should be scaled back.

Without such an enabling provision, it would become, well-nigh impossible, to comply with the Know-Your-Customer (KYC), Anti-Money Laundering (AML) and other fraud prevention obligations of data fiduciaries.

Thirdly, reasonable purposes for data processing should be extended also to third parties, similarly to the legitimate interest provided under Article 6(1)(f) of the GDPR. For example, in addition to self-defense (as data fiduciary), members of USIBC collect and process cyber security threat intelligence to serve the legitimate interest of 'third parties', *viz*. all of their customers and even the broader society rather than limiting to themselves.

Fourth, the Committee specifies that only the DPA—not data fiduciaries—can determine whether the "reasonable purpose" ground applies to a given category of processing. The "reasonable purpose" basis for processing data should not defined as an alternative to be pursued only after "consent" isn't possible. It should be an equal basis for processing so long as it is reasonable and not unduly harmful in the relevant processing content.

By requiring data fiduciaries to wait for regulatory approval before they can rely on the "reasonable purpose" ground, the Draft Bill puts businesses at the mercy of a potentially under-resourced, over-stretched DPA. This approach may result in a narrow residuary ground, forcing businesses and innovators to rely on consent—even when the costs outweigh the benefits. This approach could be better aligned with other data protection regimes around the world, including the GDPR and the just-adopted General Data Protection Law in Brazil, that acknowledge "legitimate interests" for data processing. Retaining such an approach will complicate business, result in consent fatigue for users, and disrupt the online economy. We recommend the removal of the requirement for the DPA to specify the list of activities under the reasonable purpose ground.

Similarly, in cases where exceptions to lawful grounds are the basis for processing, for instance under the exception for research purposes, requiring the DPA to approve every single instance of research before processing is allowed will lead to delays and lags in research that could be in the public benefit. Therefore, we recommend that the requirement for the DPA to approve every instance of the research exception be removed.

Should MeitY decide to retain the requirement for the DPA to specify certain activities that will qualify for the "reasonable purpose" ground for processing personal data, at a minimum, some of the activities currently listed under Section 17(2) (such as "prevention and detection of any unlawful activity including fraud"; "network and information security"; "credit scoring" and "processing of publicly available personal data") should be removed and instead be allowed as *per se* reasonable grounds.

Purposes of preventing and detecting fraud as well as ensuring network and information security of the data fiduciaries serve the legitimate interest of the data principals in particular and the society at large, without exposing the data principals' rights to extremely high risks. Considering that almost all crimes entail some element of cyberspace, there should be a general permission and ability of data processing by any data fiduciary or processor to process personal data for the legitimate interest and purpose of cyber security as a measure of self-defense and/or as a commercial service.

4. SCOPE, KEY TERMS AND DEFINITIONS

The overall scope of applicability within the Draft Bill is too wide. It should be limited to entities established in India as opposed to any entity which has collected, shared or disclosed data within India. We recommend that Art 1.(a) be deleted. In addition, clarification should be provided in relation to the extra-territorial effect, in particular in respect of the "any business carried on in India…." to ensure it does not capture business-to-business (B2B) arrangements. The focus should be offering of services to data principals within India.

Sensitive Personal Data. The Draft Bill's definition of "sensitive personal data" is expansive, and permits additional categories to be added by the regulator, creating uncertainty for organizations. Given that processing of data in this category requires "explicit consent" and cannot be processed under other legal bases, it is essential that this category be carefully delineated so that the application of the explicit consent requirement can be predictable.

The scope of the term "sensitive personal data" is broader than other comparable privacy regimes, such as the GDPR, and covers passwords, official identification data, and financial data. Combined with the Draft Bill's restrictions on the transfer of sensitive personal data outside of India, this broad definition could potentially have a significant operational impact on legitimate business operations and established data security practices – such as the transfer of passwords to central databases located outside of India.

We recommend that the definition of "sensitive personal data" be scaled back by removing the references to financial data and passwords. In particular, definitions should be consistent with other laws such as the GDPR and exclude passwords, official identifiers and financial data. For example, financial data should not be considered sensitive personal data as this is inconsistent with other data protection laws in other jurisdictions and will lead to challenges in implementation as most organizations operate globally. Financial data is already

heavily regulated by industry specific laws and regulations and so adding financial data to sensitive personal data would be cumbersome and unnecessary.

In addition, lawful bases other than explicit consent (such as performance of a contract) should be considered for the processing of sensitive personal data (e.g., reasonable purposes, employment purposes, performance of a contract). For example, insurers need to process health data in order to provide a number of types of insurance. The data is needed to carry out a number of functions, such as to price and underwrite according to the level of risk presented, and to process claims. Both the United Kingdom (UK) and Dutch government have exempted this processing from obtaining explicit consent in relation to GDPR.

Finally, sensitive personal data should not be an open list subject to additional categories to be included by the Authority as this may undermine the principle of the legal certainty of the proposed act.

Anonymization. Under the definition of "personal data" used in the Draft Bill, if there is *any* possibility that data could be used to identify a person — no matter how remote that risk is — that data qualifies as personal data. By treating data that is unlikely ever to be linked with an individual as personal data, this broad definition amplifies compliance costs without a corresponding reduction in privacy and security risks. Moreover, it may actually discourage companies from taking the protective step of anonymizing data by making the anonymization process seem useless — in other words, if anonymized data will be seen as "personal data" even if there is only a very minor chance it could be re-identified, why would companies go to the extra effort to anonymize data? Several existing data protection regimes showcase a more balanced and workable approach, which nonetheless protects consumer privacy. For example, many countries have adopted definitions of personal data that include a "reasonable linking" requirement. This definition excludes data for which identification is theoretically possible, but cost-prohibitive.

Likewise, the Committee's proposed definition of anonymized data is overly narrow. The proposal defines anonymization as an "irreversible process of transforming. . . personal data to a form in which a data principal cannot be identified." Accordingly, for the anonymization exception to apply, the Draft Bill insists that anonymization must be "irrevocable." Under this standard, data fiduciaries could almost never be certain that a given data set qualifies as "anonymized." The narrow definition of anonymization may discourage data fiduciaries from attempting to de-identify data. The bill's definition of de-identified data also seems to correspond to pseudonymized data. Moreover, it erects a barrier to entry for small companies and start-ups that lack the resources and technical know-how to achieve "irrevocable" anonymization.

As an alternative, India should recognize international anonymization practices and best approaches that permit data fiduciaries to engage in "reasonable efforts" to de-identify data. Expanding the definition of anonymization would encourage businesses to anonymize data in more situations, reducing the privacy and security risks facing Indian data principals.

Biometric Data. The definition of biometric data under the Bill is overly broad. The current definition would include nearly every type of data collected as a result of observing a data subject, as this can be deemed to be processing carried out on the 'behavioral characteristics of the data principal.' As this would also unduly expand the scope of sensitive personal data, the definition of biometric data must be restricted to only include data used for the purpose of confirming unique identification of a natural person. Moreover, the definition as it stands could be interpreted to apply to mere photographs of individuals, severely restricting common, non-sensitive processing. Thus, an explicit exclusion of photographs is required.

Business information. Finally, business contact information (e.g., names of representatives at vendors, retailers, etc.) should be removed from the definition of "personal data." Many companies handle business contact data in their everyday work to move business-to-business communications along and use this data solely for contacting representatives among their partners and customers. Collecting and storing business contact information typically poses little risk to data principals. At the same time, treating business contact information as personal data may impose disproportionately high costs on small and medium-sized enterprises.

Harm. The definition of harm under the Draft Bill 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 out for legitimate exercises of censorship (such as by a social media platform for violation of their terms of use). The definition is particularly important to breach notification and the assessment of penalties. A narrower definition, or one that more generally references economic, physical, or reputational harm, would be preferable.

5. DATA PROTECTION OFFICER

The Committee recommends that India require certain data fiduciaries to hire a DPO to promoted advice on compliance with the data protection regime. For foreign companies whose processing activities fall within the scope of the proposed bill, the DPO must be based in India.

The DPO residency requirement imposes substantial and unnecessary costs on foreign companies, particular innovators, entrepreneurs, start-ups, and investment corporations, who must hire an India-based DPO even if they already employ a DPO in another country. These types of companies will forgo investments in India and/or delay the introduction of advanced technology by raising the costs and risk for early-stage market entry. The requirement that a DPO reside in India, in the context of a global enterprise, may mean that the DPO will be further away from the essential decisions being made by the enterprise on new potential proposals that may involve personal data. We believe that this requirement is unnecessary and unwise, because DPOs who are not based in India can become proficient in understanding and applying Indian law.

6. CHILDREN'S DATA

In its present form, the Draft Bill proposes one standard for all children under the age of 18. This approach does not recognize the varying maturity levels of children at various age groups. We agree that parental or guardian approval makes sense for certain types of collection and use of personal data from children below the age of 13 years. However, young adults between the ages of 13 and 18 years should be permitted and empowered to make decisions about their data. For example, teenagers should be able to sign up to receive information about and products that interest them and to have access to educational materials online.

Our sense is that the Draft Bill has been overly deferential to a more general law that does not square with the overall purpose of the Draft Bill, a conclusion that the Committee itself notes in its report. The definition of "child" as a person below 18 years is drawn from the Indian Contract Act, 1872 read with the Indian Majority Act, 1875. But the Committee acknowledges that "from the perspective of the full, autonomous development of the child, the age of 18 may appear too high" (Report at 44). As the Delhi High Court acknowledged in the case *K.N. Govindacharya v. Union of India* [W.P. (C) 3672/2012], the general practice has been to consider 13 years of age as the right threshold in the case of social media.

The approach in the Draft Bill also is not in line with international best practices. The GDPR provides for a default age of under 16 for parental consent, but permits member states to choose 13, 14 or 15 as the appropriate age. So far, Member States that have enacted legislation lowering the age for parental consent include France (15), Italy (14) Denmark (13), Sweden (13) and the UK (13); Portugal also has pending legislation to set the age at 13.[2]

In addition, mandating age-verification by itself is an insufficient solution. Given the onerous nature of implementing such solutions, many businesses will choose to stop serving children or any users suspected to be children under a specific age to avoid inadvertently running afoul of these requirements. This would exclude large parts of the internet for use by children – including valuable sources of information, learning, and communication.

Instead, the Draft Bill should adopt an approach that recognizes that age-verification mechanisms can be implemented through 'reasonable steps' by data fiduciaries. Entities that take reasonable steps to ascertain age should be exempt from liability for the processing of child data. At the same time, where an entity has actual knowledge that a user is underage, it may be obligated to obtain parental consent or discontinue serving such user if the personal data collected is of a sensitive nature.

[2] *See* I. Milkaite and E. Lievens, University of Ghent, *GDPR: Updated State of Play of the Age of Consent across the EU, June 2018*, Better Internet for Kids, 28 June 2016, *available at* https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.

With these concerns in mind, we urge the Ministry to lower the age range requiring parental consent to children under the age of 13.

7. POWERS OF THE DATA PROTECTION AUTHORITY

The move towards establishing a dedicated Data Protection Authority is important to ensure citizens' protection and predictable implementation. However, we have concerns with the current structure and tasks of the DPA, do not seem to align with light of international practices.

The DPA is a powerful body and has many responsibilities, including setting standards for anonymization, preparing the codes of practice, approving intra-group transfer schemes, as well as others. There is a risk that the DPA may be over-burdened and unable to respond to the many requests and questions regarding data processing. This may impede the ability of businesses and commerce to process data in a predictable and timely manner.

Delegation of Legislative Powers to DPA. The DPA also is empowered to determine some aspects of data protection regulation that are generally defined by legislators rather than by regulators. For example, the DPA is empowered to craft new categories of sensitive data, which generally is a task reserved for the legislature. It will be empowered to define the "reasonable purpose" residuary ground for lawful data processing, rather than the legislature. These requirements would impede efficient operation of a new data protection regime. Resolving them in the Draft Bill, rather than leaving them for the regulator to determine, would be consistent with GDPR and other data protection regimes, and would permit businesses to structure appropriate compliance programs and meet their legal obligations from the outset.

Significant Data Fiduciaries. We are particularly concerned that the DPA would be empowered under the Draft Bill to decide which entities are "significant" data fiduciaries, a designation that imposes substantial new regulatory obligations. These obligations include data protection impact assessments (DPIA), enhanced record-keeping obligations, and audit requirements. Such an important classification, if it is to be used, should be determined by the legislature in the statute rather than left to the discretion of a regulator. If the task is to be left to the DPA, however, the criteria must be stated with specificity. The Draft Bill suggests that the DPA consider factors such as volume and sensitivity of personal data processed, turnover, use of new technologies and similar factors. If the imposition of these substantial obligations is to be left to the regulator, the criteria under which the DPA will make those determinations must be set out with specificity and clarity, and companies should have a clear path to challenge the decision of the DPA.

Qualifications of Members. The Draft Bill provides that the members of the DPA have specialized knowledge of, and at least ten years of professional experience in the relevant areas. The Bill does not provide similar requirements for the appointment of its officers, employees, consultants and experts. In addition, there are no specialized qualifications for the chair of the DPA. Ensuring that such officers also will possess the requisite

expertise will ensure that the DPA makes reasoned decisions based on a sound understanding of all relevant technical factors.

Search and Seizure Powers. The Draft Bill grants the DPA the power to search and seize the property of any business for up to 6 months on the basis of 'reasonable grounds' to believe that a contravention of the Act has been or is likely to be committed. This is a draconian power without any judicial oversight, making it a departure from how regulators such as the Competition Commission of India (CCI) usually exercise these powers. In order to ensure that businesses are not adversely impacted, the basis to proceed with search and seizure should be changed from a 'reasonable grounds' standard to a 'probable cause' standard, and judicial approval should be required to exercise these powers.

In view of the above, we urge the Ministry to consider changes that will allow the DPA to work efficiently and with sufficient expertise.

Timeline. According to the draft, the establishment of the DPA takes place within 3 months after the notified date; the DPA notifies grounds for processing and issue codes of practices on several issues no later than 12 months from the same date. The Act would come into force 18 months after the notified date, leaving 6 months to organizations to define in detail all internal processes and build a consistent compliance program. This timeframe seems too short and the number of provisions that will be defined by the Government or the DPA after the enactment too broad. We encourage the lawmakers to review this timeline in order to ensure a clearer and more predictable enforcement.

8. PENALTIES & OFFENCES

USIBC has concerns regarding the severity of the proposed penalties outlined in the legislation. In particular, the criminal penalties are out of step with international data protection regulations. Imprisoning individuals for violating data protection regulations is excessive in light of alternative punishment approaches that are available, particularly if they only meet a "recklessness" criterion. The potential for actual imprisonment for data protection violations will result in many companies avoiding India as a potential market, a result that would be contrary to India's interests.

We are opposed to criminal penalties. If there is further consideration of criminal liability, it should only be triggered in extreme/limited situations involving criminal (including fraudulent) intent (e.g., illegal sale of personal data to third party for profit without consent) or where there is a direct and serious violation of explicit direction issued by the DPAI to a particular data fiduciary. However, it would be desirable to invoke the extant legislative provisions to deal with such offences rather than under the data protection legislation.

Accordingly, Chapter XIII dealing with the criminal offences should be omitted altogether. Adopting an approach in line with the EU, Canada, or the United States in opting for financial penalties would be the most effective, and fair, alternative.

The civil penalties proposed are excessive as well. Basing penalties on total worldwide turnover risks bankrupting companies for a single global incident, given the GDPR's analogous approach. A more appropriate and fair approach would base penalties on the amount of turnover within India, an approach that would be scaled to the actual activities of the enterprise in India. Although penalties should serve as a deterrent, they should not be so extreme as to severely restrict economic activity and growth in the digital economy. Many businesses may choose to avoid doing business in India altogether, given the risk of incurring such severe penalties. Furthermore, such high penalties create a perverse incentive to avoid working proactively with regulators to address problems as they emerge. On the contrary, more emphasis should be given to accountability measures adopted by organizations to minimize privacy risks – as already acknowledged in Section 73 – when determining penalties.

In the interest of fairness and justice, we believe that the scope of corporate liability should be restricted to the persons found to be involved and responsible for the offence and that MeitY consider more reasonable civil penalties that will deter illegal behavior.

In addition, we recommend that the DPA is assigned sole authority to bring data protection and privacy enforcement actions. This will avoid potentially overlapping and differing enforcement of the law across India.

9. JURISDICTION

The proposed jurisdiction provisions allow substantial extraterritorial reach. The Committee's proposed data protection regulation would apply to all companies incorporated outside of India that offer goods or services in India. Adopting such an expansive regulation will deter companies from offering services in India and overburden them with excessive regulations from India and the EU. The costs may prove prohibitive, particularly for SMEs.

The text of the Draft Bill is similar to that of the GDPR, but importantly the Draft Bill does not include the significant limitations on those provisions stated in the GDPR's recitals and years of European common law. As a result, the Draft Bill's approach is actually significantly more extensive than the GDPR and would purport to bring a far wider range of companies under the law's ambit. This approach would result in many companies restricting access to global goods or services from being provided in India. For example, some 1,000 U.S. publications now have been restricted by their publishers from being made available in EU Member States because of the onerous jurisdiction provisions of the GDPR.[3] We could expect a similar result here, particularly given that the Draft Bill's penalties also are more onerous than the GDPR. This result would be contrary to India's interests.

[3] *See* J. South, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect*, Nieman Foundation at Harvard, 7 August 2018, *available at* http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

In particular, the "profiling" requirement is much broader than the parallel requirement in the GDPR, and could apply to any "profiling" of data subjects regardless of whether it concerns their activities in India. We suggest that the "profiling" basis for jurisdiction be limited as in the GDPR (not only text, but the accompanying recital), and apply specifically only to data subjects' activities in India.

USIBC supports the proposed exception for organizations processing data only of foreign nationals. However, it is unclear whether a branch or subsidiary of a foreign-incorporated company processing the data of only foreign nationals in India is exempted. USIBC encourages MeitY to clarify that this exception applies to all entities in India, not just Indian companies. Restricting this exception only to Indian companies would undermine the global digital marketplace and India's business process outsourcing industry.

10. TRUST SCORE

The Draft Bill provides for the assignation of trust scores by data auditors to data fiduciaries. The criteria for this score are to be specified by the DPA. The Draft Bill mentions some factors that must be considered by the DPA while setting the criteria, for instance the clarity and effectiveness of notices, instances of personal data breach, and similar grounds. However, the criteria themselves are not mentioned in the Bill, thereby making the DPA the only authority on the subject without any guidance on how its discretion is to be exercised. It is our view that at least the fundamental criteria of determining trust scores must be specified by the Draft Bill itself. We also suggest the DPA also not participate in the scoring process.

This proposal for data trust score based on ratings proposed within the Section 35 seems overtly burdensome obligation, especially considering that such rating would itself be based on the criteria specified by the DPA. It would not be out of place to mention that such a construct would be predicated on a myriad of factors and would likely vary across sectors and business context. Accordingly, the data trust score mechanism should not be part of the data protection legislation and the Authority should not be burdened with such additional tasks. Instead, we recommend that instead the DPA's role be restricted to create a facilitative environment where sectoral regulators or industry bodies are able to formulate guidance on trust-scoring on voluntary basis.

11. DATA PROTECTION IMPACT ASSESSMENT

The proposed regulation requires that significant data fiduciaries submit data protection impact assessments, or DPIAs, to the DPA for review in all instances before it may process data. As drafted the Article presumes that any new technology requires a DPIA which is disproportionate. There needs to be a link between the processing activity and the risk of harm to the data principles. Such a requirement would be a significant impediment to the ability of digital businesses to be nimble and innovative, and would slow, rather than accelerate, India's digital economy. This requirement goes far beyond the analogous provision in GDPR, which requires submission only for processing activities that are most likely to harm data principals. In particular, making this mandatory for all kind of new technologies might impinge on the innovation environment in India. We recommend the removal of the requirement to submit DPIAs to the DPA for review.

Essentially, the DPIA should be limited to those data fiduciaries that process data with high risk such as the critical information infrastructure and dealing with sensitive personal information. However, these again need to be evaluated within a particular context at any given point in time. For example, a social networking site serving a few hundred students on a college campus need not be subject to DPIA but if it grows to hundreds of millions of users, it may be subject to the same. Otherwise the Authority will be unnecessarily inundated with DPIAs. This approach is consistent with the GDPR.

The Draft Bill also is ambiguous regarding whether processing may commence prior to the DPA's review, and lacks timelines during which the regulator must respond. If this structure is to be retained, deadlines are critical for reducing business disruption from pending DPIA reviews. The structure may be workable if a short deadline is set, after which the DPIA is considered approved; otherwise, we recommend that the GDPR approach be considered rather than the approach set out in the Draft Bill.

12. CLEAR REQUIREMENTS FOR CONSENT

The Draft Bill and report are inconsistent and ambiguous on the forms of consent that will be considered permissible under the law. For example, the Draft Bill states that consent may be implied so long as there is "an affirmative action that is meaningful in a given context." Likewise, the report speculates that website monitoring of user behavior may not require opt-in consent. By contrast, a different part of the report declares that pre-ticked boxes or silence cannot provide valid consent. Given that the Committee's proposal treats consent as the preferred ground for processing, it is essential to provide consistent guidance on the conditions for consent.

13. PRIVACY BY DESIGN

Under the Draft Bill, data fiduciaries are required to implement policies and measures to ensure "privacy by design." The privacy by design obligations in the Bill involve designing managerial, organizational, business practices and technical systems in a manner to anticipate, identify and avoid harm to the data principal, and ensuring that these practices are embedded in the business practices of the regulated entity at every stage of processing of personal data. Unlike the GDPR, however, the Draft Bill creates an absolute obligation in this regard, regardless of the size of the enterprise or the nature of its data processing. The GDPR, for example, allows the controller to take into account the costs of implementation and allows the controller to determine measures that are "appropriate" in the relevant circumstances. We believe these elements of flexibility will be important for SMEs and early-stage businesses to be able to effectively comply with the "privacy by design" obligations that are most relevant to their data processing, and suggest that similar flexibility be provided in the Draft Bill.

14. DATA BREACH NOTIFICATION

The Draft Bill crafts a data-breach notification approach that does not mandate a specific time limit similar to that of the GDPR, which we believe is an important step forward and a reflection of the reality that a reasonable

time period should be permitted for data fiduciaries to determine the true scope of a breach. However, it imposes an obligation on data fiduciaries to notify the DPA (and, in some cases, the data principal) in the case of any personal data breach that is "likely to cause harm." This threshold is lower than the threshold adopted in the GDPR and that of many data-breach notification statutes around the world. All data breaches are not equal. For example, a data breach of medical history may prove significantly more damaging for an individual than his or her addresses being compromised.

The use of the light "likely to cause harm" standard means that many data breaches that would, in effect, carry no risk of serious harm to the data subject will nonetheless be notified, causing notification fatigue on the part of data subjects. When too many notifications are issued, the important notifications of breaches that are, in fact, serious may be obscured to the data subject. In addition, the large number of notifications to the DPA would entail substantial administrative costs for organizations and excessive workload for the DPA.

Accordingly, the Section 32 (1) should be revised as suggested below:

"The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause significant risk of impact or harm to the affected data principals."

It also would be helpful for the Draft Bill to clarify that only data fiduciaries, and not processors, bear the obligation of notification. Processors, such as cloud service providers, often do not have sufficient information to determine which data subjects should be notified because full information on data subjects is held solely by data fiduciaries. As with the GDPR, the data fiduciary's obligations should be triggered by "actual knowledge," an appropriate standard. As a matter of good practice, the Draft Bill should make these distinctions explicit.

In some circumstances, data fiduciaries may also be required to communicate a personal data breach to data principals. However, to incentivize companies to proactively adopt good data protection practices, we suggest the following exemptions to the reporting requirements:

- the breach is unlikely to result in a high risk for the rights and freedoms of data principals;
- appropriate technical and organizational protection measures were in place at the time of the incident; for example, where data is strongly encrypted or otherwise rendered unintelligible to a person without legitimate access to the same even as there should be an obligation to keep internal records to prove compliance and demonstrate the effectiveness of the encryption applied; or,
- if such reporting requirement would trigger disproportionate efforts; as an alternative, a public information campaign could be relied on so that affected individuals can be effectively informed).

In certain circumstances, disclosing that the breach has occurred may necessarily involve the disclosure of personal data and other information. While there would usually be a confidentiality exception in the contract with the customer for disclosure required by law, it would be helpful if the framework made it clear that data

fiduciaries are legally obliged to notify the DPAI (or other regulators) of such data breach even if it entails the disclosure of personal data and other information, thereby protecting data fiduciaries from undue liability claims pursuant to such disclosures.

15. DATA FIDUCIARIES

The Draft Bill treats what are generally recognized as data controllers as data fiduciaries and imputes a fiduciary relationship with data principals. Accordingly, they are required to uphold trust and loyalty and process data in a fair and reasonable manner that respects the privacy of the data principal and ensures a duty of care. This requirement is novel and overarching. Hence the term data fiduciary should be changed to "data controller".

The Draft Bill puts a lot of obligations on significant data fiduciaries. All these requirements/obligations will put unnecessary burden on companies without providing any additional benefit. Hence this concept should be entirely removed. Even if India decides to proceed with it, the authorities should define the significant data fiduciaries upfront (vs. notifying it later). Secondly "volume of personal data processed, turnover of the data fiduciary & new technologies used for data processing" should not be considered as a relevant factor for deciding whether a data fiduciary is significant or not.

The proposal to allow engagement of a sub-processor by a data processor only with the prior authorization of the data fiduciary as provided in Section 37 (2), is neither necessary nor desirable nor even pragmatic.

It would be desirable to have a parallel here again with the GDPR. Accordingly, the *data processor should be able to obtain prior general consent of the data fiduciary, with an obligation to inform the latter before engaging a new sub-processor.* This would provide the requisite flexibility to the data processor while proffering reasonable opportunity for data fiduciary to object, paving the path to resolution by way of mutual discussions and negotiations.

In addition, the Draft Bill requires the data fiduciary to provide the data principal with information on the individuals or entities including other data fiduciaries or data processors, with whom the principal's personal data may be shared, if applicable. It is almost impossible to maintain such information in a privacy notice as suppliers may change regularly. Hence the requirement to share information on individual and entities should be changed to "categories of entities." In addition, the Draft Bill requires the data fiduciary to provide the data principal with any other information as may be specified by the Authority. Again, such changes to data privacy notices make compliance onerous. Hence, we recommend that the notice requirements be laid out in the Draft Bill and not left to the discretion of the DPA.

17. DATA STORAGE LIMITATION

The Draft Bill restricts data fiduciaries from retaining personal data beyond the period necessary for delivery of services. This greatly reduces the ability of businesses to use aggregated data for analytics and other processes that can be used to enhance products and services. In order to strike a balance between protection of privacy of individuals and the ability of businesses to harness data, it is recommended that fiduciaries be allowed to retain personal data once it has been sufficiently de-identified in a manner where the data principal is no longer identified. We request an explicit reference that excludes de-identified data from the storage limitations outlined in Section 10.

18. TRANSPARENCY

The Draft Bill requires data fiduciaries to notify data principals of important operations periodically with regards to processing of personal data. However, neither the term 'important operation' nor 'periodically' has been defined, leading to a lack of clarity. In order for meaningful compliance, it is recommended that these terms be specifically clarified.

19. PROHIBITION ON REIDENTIFICATION

The Draft Bill virtually prohibits non-consensual re-identification of personal data, which is an imperative protection. In order to ensure that incentives within the law support privacy-protecting actions taken by data fiduciaries, and that the legislation does not lead to unintended consequences, it is recommended that a clarifying provision be added to state that compliance with any provision of the Act will not be interpreted to require a data fiduciary to re-identify personal data relating to a natural person that has been de-identified.

20. COMMENCEMENT DATE

The Act will come into force 18 months from the notified date. As the DPA will be established within 3 months of the notified date, and will have a period of 12 months from the notified date to issue codes of practice and specify the list of activities that fall under the reasonable purpose ground of processing, there will not be sufficient time for data fiduciaries and data processors to make the necessary changes especially if the codes of practice are not consistent with international privacy and data protection norms. A more realistic commencement date for the Act would be a period of 24 months from 12 months from the notified date, which would take into account the detailed guidance in the codes of practice and the list of reasonable purposes specified by the DPA, and the consequential changes required for internal processes, organizational structure, contractual arrangements, and operations and technology. Considering that organisations had a period of two years to implement the GDPR, which by some accounts was not sufficient, a period of 24 months from 12 months from the notified date would be reasonable.