Internet and Mobile Association of India

IAMAI Submission on Joint Parliamentary Committee Report on Personal Data Protection Bill 2019

The Internet and Mobile Association of India ("**IAMAI**") is a not-for-profit industry body and we play a key role in ensuring the growth and sustainability of the digital industry. We firmly believe that the digital industry is going to be a major driving force in the economic and social development of the country which includes job creation, innovation, contribution to the GDP, inclusion and empowerment of our citizens, etc.

We write to you in reference to the Joint Parliamentary Committee's (**JPC**) Report (**Report**) on the Personal Data Protection Bill. We understand that the JPC report, which now contains a new version of the data protection law titled the 'Data Protection Bill 2021' (**DP Bill**), has replaced the erstwhile PDP Bill. We appreciate the JPC for efficiently conducting public consultations on the DP Bill. We note that the Report recommends several measures aimed at improving ease of doing business in India and developing India's digital economy. However, the DP Bill is drastically different from the PDP Bill and there is a need for consultation regarding changes that have been carried out to the DP Bill. This will enable all stakeholders to present their concerns and suggestions before the DP Bill is introduced by the Ministry of Electronics and Information Technology (**MeitY**) before the Parliament.

IAMAI on behalf of its members would like to share feedback on DP Bill. We have set out our most pressing concerns along with our suggestions below.

We hope that the government will continue the transparent and consultative ethos under which erstwhile PDP Bill was developed. We believe that due to the changes recommended by the JPC, the original structure of the bill has undergone change and hence the government needs to transparently hold another round of wide stakeholder consultation. IAMAI is confident that through consultation and collaboration, the final version of the law will be inclusive of the feedback provided by a gamut of stakeholders who are invested in and committed to the Indian Digital Ecosystem.

IAMAI Submission:

1. EXPANSION OF THE SCOPE OF THE DP BILL:

Inclusion of non-personal data - We note that the JPC while discussing the nature of data collection has concluded that the distinction between personal data (***PD***) and non-personal data (***NPD***) cannot be made during mass movement of mixed forms of data. Resultantly, the JPC believes that restricting the scope of the law to only PD would not necessarily achieve privacy interests. Thus, the JPC has recommended that NPD be included in the scope of the law and the law be renamed as the "Data Protection Bill".

Data Protection Authority (**DPA**) **-** The JPC in its Report states that having a single regulator to oversee all data (PD and NPD) will make governance simpler and help avoid any "contradiction, confusion and mismanagement". In pursuance of this viewpoint, the JPC has recommended changes to ensure that the same regulator, i.e., the DPA is empowered to regulate both PD and NPD.

Issue / Impact:

- We understand that the JPC seeks to integrate provisions dealing with PD and NPD within a single statutory framework in the interest of data privacy. However, we believe that this step will do more harm than good. Regulatory conflicts and confusion may arise if only selective provisions governing NPD (like Section 92) are added in the DP Bill.
- To illustrate, there are differences in the objectives of any law that governs PD and NPD respectively. A law governing PD will primarily aim to ensure the privacy of individuals and focus on protecting their PD. However, a law that seeks to govern NPD would have different regulatory goals rather than protecting privacy of the individuals and instead would focus on promoting the economic interests of the nation and the ways to achieve them in an increasingly data driven world. Furthermore, even a regulator for PD would primarily concern itself with protecting the interests of data principals, preventing misuse of PD and ensuring adequate data protection, these objectives are different from the expected regulatory framework for NPD. Thus, it is clear that the regulatory objectives for PD and NPD are different. We strongly believe that having a common regulatory framework may not result in an efficient data regulation framework and parallel enforcement will only lead to uncertainty. Given that the policy objectives behind regulation of personal data and NPD are distinct and unique to each, attempting to cover both within a single law will dilute both objectives. Keeping NPD and personal data frameworks separate will also be aligned with the recommendations of the expert committee appointed by MeitY to develop a framework for NPD (**NPD Committee**), which suggested that references pertaining to NPD in the erstwhile PDP Bill must be deleted, and a separate authority must be established to regulate NPD.
- While the DP Bill states that the DPA will specify anonymisation standards at a later date, until such anonymisation standards are prescribed, there is no clarity as to what would qualify as anonymised data for the purpose of this provision. Moreover, the definition of NPD in the DP Bill lacks clarity. It is currently defined as '*data other than personal data*'. 'Data' itself has been defined very broadly as a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing. Clubbing multiple types of data into a single group, without any parameters for classification, could result in the regulation of diverse categories of data types as if it were homogenous.
- The DP Bill empowers the government to seek anonymised data or NPD data from businesses to enable (1) better targeting of delivery of services; or (2) for the formulation of evidence-based policies by the Government. Given this, any upcoming policy or legal framework relating to NPD enacted under the DP Bill will have legislative backing, including any instructions to share anonymised data or NPD. The current language under the DP Bill contemplates a broad right to requisition any anonymized personal data and NPD which will severely impact a data fiduciary / data processor's ability to retain control over its data. Therefore, imposing any obligations around NPD would increase business uncertainty and risk, which would impact the growth of the digital economy.
- The power of the Government to compel data fiduciaries and data processors to provide data is unreasonable. The DP Bill practically empowers the government to direct a business to dedicate additional resources to create anonymised data sets, which may not have been in existence, solely for the use of the Government. A directive of such nature will negatively impact ease of doing business in India. The provision on mandatory data sharing could significantly impact the ability of Indian firms to compete in global markets, especially since global data frameworks do not contain a similar mandate. This may also discourage foreign investment in India, and consequently limit the types of products and services available in the Indian market for consumers.

- Due to the novelty of this provision, the risks and corresponding mitigations of such a data sharing requirement are not already identified in privacy law or research. Until those protocols are developed, any requirements to share NPD can raise serious intellectual property (**IP**), privacy and confidentiality concerns. Notably, some information may appear to be non-personal when considered in the context of a single individual, but could reveal private or sensitive information about groups of people. For example, if a service provider were required to share traffic data, they might reveal information about travel patterns in certain neighbourhoods that could create privacy issues for that population. While a single organisation can ensure the integrity of anonymized data, it is harder to protect against re-identifiability when data sets are shared with an external entity that has access to parallel data and an incentive to re-identify individuals. Exposure of anonymized personal data may pose a risk to public security and raise concerns about the privacy and security of groups of individuals. The DP Bill does not currently provide data fiduciaries or processors with any protection or liability for any subsequent harm caused from sharing of NPD, despite the fact that re-identification is a criminal offence under the DP Bill.
- Moreover, the DP Bill lacks any safeguards to ensure that any data collected by the government under this provision is necessary and proportionate to the specified purpose. Further, there are no protections for data businesses from any security breaches, contractual breaches or third party claims that can arise as a result of mandatorily sharing the data to data requesters under this framework. The DP Bill also does not clarify whether the government can direct data fiduciaries and processors to share the data with third parties under these provisions or whether the government itself can share the data with any third parties. There is no provision specifying the government's accountability in respect of the shared NPD it receives under this provision, or any safeguards the government or third party must implement before receiving such data. It also lacks other important provisions clarifying conditions like the payment terms, contractual obligations, technical safeguards, etc. In the absence of any clear guidelines or safeguards on the implementation of this provision, there is ample scope for misuse of this provision, which could impact companies' proprietary rights and also introduce significant privacy risks defeating the core objectives of the DP Bill.
- The DP Bill also fails to address that the anonymised personal data or NPD, which is subject to a forced data sharing requirement, could be proprietary, confidential and critical to business interests. It seems to ignore the fact that substantial effort is required to make data useful and businesses use complex processes to make such data useful, including careful selection, assembly, anonymisation and execution of large data sets. The intellectual property rights regime, both domestic and international, legally protects such works. The proposal for forced disclosure of anonymised data and NPD would be in conflict with the provisions of the Indian Copyright Act, 1957. As per Indian copyright law, the arrangement and selection of certain anonymised data sets would be protected, and exclusive proprietary rights therein would vest with its owner. Further, such anonymised data sets are strictly confidential and proprietary, protectable as trade secrets. However, the DP Bill imposes an unreasonable requirement to forcibly share data upon receipt of a direction from the government. As such, the person who holds rights over such data will be deprived of his/her exclusive rights under the Copyright Act, including common law and statutory principles dealing with trade secrets and confidentiality. Such inconsistencies would create business uncertainty and impact ease of doing business.
- The data processing industry in India may be disproportionately impacted as the DP Bill contemplates that a data sharing direction could be given to data processors which merely process data on the instruction of data fiduciaries. This will require such data processors to bear the onus of sharing anonymized personal data or NPD of its data fiduciaries with the regulators and not in response to instruction from the data fiduciaries. As data processors are subject to contractual

relationships with data fiduciaries and may have limited control or visibility over the data fiduciary's data, it would be a disproportionate burden on such data processors. For instance, cloud service providers, or entities providing online storage services or outsourcing typically do not have any visibility over their customer's data or the purposes of processing and are subject to stringent confidentiality requirements in their contracts. This has been recognized by MEITY's NPD Committee who recommended that data processors should not be mandated to share data belonging to their clients. If data processors in India are indeed are subject to this provision, it may discourage foreign conglomerates from outsourcing their business processes to India which would be a severe setback to the Indian BPO and cloud services sectors, severely impacting the growth of India's digital economy. Therefore, the reference to 'data processors' should be excluded from Section 92.

- Allowing the DPA to govern NPD breaches is excessive because NPD, by its very definition, does not involve any information concerning an individual. The legislative intent behind reporting of NPD breaches is unclear. Reporting of personal data breaches are done for protecting a person's privacy. However, it is possible that a particular NPD breach will have no relevance to anyone else other than the organization involved. Given how broad the definition of NPD is, the DPA can expect to receive hundreds of thousands of data breach notifications daily, for all types of incidents, even if it the impact is limited and negligible. This would lead to greater risks for security if the DPA misses out on important notifications due to being inundated by numerous notifications. It would also increase the DPA's administrative burden and divert the regulator's manpower from more important regulatory activities (e.g. enforcement or education), towards an activity that does not provide any benefit for privacy or security. Existing regulations under the Information Technology Act, 2000 (**IT Act**), the rules governing the Indian Computer Emergency Response Team (**CERT-In**) and critical information infrastructure already address various cybersecurity-related concerns. While there may be certain forms of NPD which are critical or sensitive and require additional safeguards and regulatory supervision with respect to their storage and protection, such sectors are already under strict breach reporting regimes. For instance, the Reserve Bank of India requires banks to report breaches to the RBI within two to six hours. These regulations sufficiently address the regulatory objectives of reporting NPD breaches.

- Further, if mandatory sharing of NPD under Section 92(2) of the DP Bill is enforced, it will increase the regulatory burden of businesses. This is because such an obligation, which currently lacks safeguards, may amount to unnecessary state intervention in a free market economy. It may also encroach upon the protections provided to intellectual property rights under the Agreement on Trade-Related Aspects of Intellectual Property Rights (**TRIPS**) to which India is a party.

- Section 2(A)(a) of the DP Bill suggests that proposed rules would be applicable to *"processing of personal data where such data has been collected, stored, disclosed, shared or otherwise processed within the territory of India"*. However, there is no similar qualification for NPD and unlike in relation to personal data, the DP Bill does not clarify whether there are any territorial limits to the applicability of its provisions in respect of NPD. As a result, it is currently unclear whether the DP Bill will also apply to processing of NPD outside India, even when it is not originating from India. This significantly widens the scope of the DP Bill where it now seems to also cover personal data of foreign data principles being processed by Indian firms. This broad scope has unintended negative consequences for Indian businesses, without bringing privacy benefits to Indian citizens. If an Indian employee of a global firm may so much as even view foreign personal data — it would trigger obligations under the DP Bill for their company, because access to data is a form of data processing. Given that such data disclosure is only incidental, global

companies under such use cases ought not be expected to comply with obligations under the DP Bill, such as certification of their privacy by design policies by the Government, nor should the Government be burdened with reviewing and certifying the privacy operations of non-Indian firms that happen to use Indian vendors or providers. On the contrary, under the proposed scope of the DP Bill the incentive could favour exclusion of Indian employees from global projects. This is likely to lead to a situation driving global companies to restructure their operations and carve India out so as to ensure that no Indian employee, vendor, or party comes in contact with personal data of foreign principals. This works to a serious disadvantage of India's promising tech startups that otherwise have the potential to become global champions for data processing. An expansive interpretation will result in uncertainty within the industry and impact businesses' ease of operating in India, due to significant compliance burdens for entities who are otherwise compliance with global data protection frameworks.

- Additionally, an avoidable adverse impact of this wide scope could be on the Indian outsourcing industry. In the normal course, one of the advantages to date of India's outsourcing industry has been its ability to offer services to foreign clients subject to those foreign client's legislative requirements, rather than subjecting them to domestic Indian regulatory regime as well and making them subject to double regulatory requirements. Global firms that currently outsource their IT and data operations to India's talent, may be disincentivized to continue their Business to Business (**B2B**) partnerships if the burden of complying with double rules outweighs India's competitive cost and workforce advantages.

- We understand and appreciate that a strong data security regime is important to maintain India's attractiveness as an IT and data outsourcing destination. However, to avoid unintended adverse consequences, we suggest that along the lines of the European Union General Data Protection Regulation that the scope provision be grounded in domestic data collection activities as well as targeting of users in India. When asked a question whether a foreign business partnering with a European data processor would become subject to the GDPR, the European Data Protection Board's Guidelines on the territorial scope of GDPR, Example 7 at p. 12 clarified that it would not, unless such data controller was processing personal data of Europeans or otherwise targeting them in the context of European business activities.[1] This aspect of the European approach is sensible so as to maintain competitiveness of domestic industries.

IAMAI Suggestions:

- **Inclusion of non-personal data within the DP Bill is premature and contrary to the recommendations of the NPD Committee. We strongly believe that any proposed framework to govern NPD should not be included within the scope of the DP Bill. Any proposed framework for anonymised data or NPD should be considered only after (i) the DP Bill has been passed; (ii) the DPA has issued appropriate standards, rules and regulations on anonymisation and (iii) the NPD Committee has concluded its deliberations and published its recommendations after inviting comments from all relevant stakeholders, including from the public.**
- **The main objective of the DP Bill is the protection of the privacy of individuals within India, as the rights of the foreign individuals whose personal data is processed within India as part of the outsourcing activities are already covered by extensive legislation applicable in their countries of "origin". It should be clarified that the scope of DP Bill applies to personal data of data principles in India.**
- **Section 92 of the DP Bill, relating to forced sharing of anonymised data and non-personal data should be removed in its entirety.**

- **As an alternative model, firms are already making large data sets available, which helps empower other organisations to innovate and develop programs that produce socio-economic value, which should be encouraged and incentivised. The government should promote voluntary data sharing mechanisms separately (e.g. via data marketplaces and data exchanges), with adequate intellectual property protections, privacy protections, fiscal incentives and legal immunity in case of liability emanating from such sharing. Such mechanisms should only be introduced after the NPD Committee's revised report has been published and comprehensive consultations have taken place.**
- **If at all Section 92 is retained, the DP Bill should include safeguards and restrictions on the use by the Government of any data it receives under Section 92.**
- **Safeguards should be put in place to ensure that companies are not compelled to share proprietary and business-critical information that would adversely affect their proprietary interests or competitive advantage**
- **Section 25(6) of the DP Bill allowing the DPA to take action in case of an NPD breach must be deleted. The DP Bill should also not impose any requirement on data fiduciaries for the notification of non-personal data breaches, as it does not serve any additional purpose.**
- **Data processors, such as cloud service providers, should be exempted from sharing any NPD to the government because they are not ultimate owners of this data and are merely processing the data on behalf of data principals/data fiduciaries.**
- **We also urge the government to defer any proposed regulation of anonymised or non-personal data until appropriate anonymisation standards are notified.**

2. ADDITIONAL DATA LOCALISATION REQUIREMENTS AND LIMITATIONS ON CROSS-BORDER TRANSFERS[1]:

Data Localisation Requirements – JPC has recommended more stringent data localization requirements. Report recommends that recommends that India move towards complete data localisation. The DP Bill mandates data localisation for sensitive PD (**SPD**) and critical PD (**CPD**) and imposes rigorous compliances. All SPD is to be stored in India, though it may be transferred outside India (after obtaining explicit consent in addition with other conditions; such as transfer being subject to a scheme/contract approved by the DPA, transfer to only certain permissible countries, or if the transfer is approved for a specific purpose), and all CPD is to be processed only in India under Section 33. Further, cross-border transfer of SPD for processing purposes is allowed only when the conditions under Section 34 are satisfied.

Cross Border Transfer - The DP Bill on the recommendation of JPC has added the words *'in consultation with the Central Government*' at the end of Section 34(1)(a) which enlists the conditions for transfer of SPD and CPD. By virtue of this, the DP Bill now mandates that the DPA has to consult the Central Government for all SPD related cross-border transfer decisions.

Further, even in situations where cross border transfer of SPD is approved upon an adequacy decision being made on a foreign jurisdiction, the Central Government is empowered to approve further sharing of SPD within such a jurisdiction.

Issue / Impact:

[1] **Our members Reliance Jio and Paytm have divergent views on data localisation and cross-border data flows**

- We note that the JPC in the Report states that with the evolution and growth of information technology, the world has become a "global village" wherein there is a seamless flow of people, goods and data. We agree with this statement and strongly believe that robust cross-border data flows will play a crucial role in helping India achieve the goal of a 'Digital India'.

- Enforcing the strict requirement of local storage of SPD is at odds with the global standards and would only lead to compliance problems, as its well-known that companies often have data-sets comprising of CPD, SPD and NPD and separating them can be impossible. This may force companies to opt for complete localisation of such data-sets. This will inevitably increase compliance costs, which will be particularly harmful for start-ups.

- We recognise the concerns that Government has regarding digital privacy and security and are fully committed to improving privacy and security safeguards for users. However, restrictive data localization doesn't solve these problems. Effective security and privacy don't depend on the location of data or the territory where data is processed, but rather in the security and privacy controls applied to such data, irrespective of where the systems are physically located. In fact, data localisation could exacerbate security threats, for example by limiting pattern analysis helpful in detecting fraud. Storing data in one location could make it a more attractive target. Rather, globally distributed networks better protect against loss of data or interruption of service as a result of a technical failure or natural disaster. Forced data localization also harms consumers as it limits their choice of service providers, and the increase in compliance costs for businesses may be passed down to consumers.

- Localisation requirements may lead to increased privacy concerns due to lack of clarity on exactly what SPD should be localised under the DP Bill. If the localisation requirement also extends to SPD that is voluntarily generated on a data fiduciary's platform, in addition to the SPD collected by a data fiduciary, data fiduciaries may have to closely monitor every activity of their users to comply with the DP Bill.

- We believe that since the transfer of SPD is otherwise strictly regulated, the government can meet its sovereign objectives (for e.g. consumer protection) without having to mandate any local storage requirements. Additionally, most providers will not already have systems in place that isolate SPD from other, general account data. Requiring specialised types of processing for different types of data categories often stored in the same account could actually create privacy risks by requiring companies to sort and identify the data that fall into this category in order to meet these additional requirements. Mirroring requirements may also increase the likelihood of errors in datasets.

- Another pressing concern is that the exact scope of SPD is not clearly laid down because the Central Government is empowered to notify further classes of SPD, etc. Even the meaning of CPD is yet to be clearly provided. At present the DP Bill lacks clarity in the scope CPD as: (i) it does not provide any definition of CPD; (ii) it does not specify any parameters or criteria for classification of CPD; and (iii) the government can notify categories of CPD, without consulting either the DPA, or industry, who will be significantly impacted. Without prejudice to the above, our initial assessment is that it creates a heavy compliance burden and imposes restrictions on how companies can develop their products and services. This could result in companies delaying or even stopping the launch of certain consumer offerings in India, or launching a version with limited features. Further, in the absence of any guidance on CPD, data fiduciaries will not be able to

anticipate the infrastructural changes required to comply with this rule, which creates business uncertainty and heavy compliance costs should the timeline for compliance be insufficient. This may even have an adverse impact on small and medium sized enterprises as it will significantly increase their operational costs. Such uncertainty could also impact FDI flows into India and lower India's ranking in the 'Ease of Doing Business' index.

- It is common knowledge that data localisation requires significant planning and investments from companies. Accordingly, there should be clarity on the exact types of data that have to be localised.

- We are concerned with the recommendation mandating mirror copies of SPD and CPD that are already in possession of foreign entities to be brought back to India. Such retrospective effect is prone to scrutiny by courts as it is not in consonance with established legal norms that require all obligations to generally be applicable prospectively.

- Additionally, to mandate explicit consent for every cross-border SPD transfer and to place the burden on individuals to make an informed decision about whether to consent to each transfer may prove to be redundant. This is because when countless notices about SPD cross-border transfers are presented to an individual, they may encounter consent fatigue.

- At present, it is unclear how the cross-border transfer conditions in the DP Bill will be interpreted in light of sectoral regulations. For example, under RBI's directive, payments data must be stored only in India, but can be processed on foreign servers, provided the data is deleted within 24 hours. The DP Bill should clarify that SPD can be stored outside India as long as necessary for processing that is legally permissible. Although the DP Bill provides for consultations between regulators, the lack of clarity before passage of the DP Bill creates business uncertainty and risk, and would inhibit the ability of companies to innovate using such data. This could impact growth in key sectors of the digital economy such as fintech and healthcare.

- The additional obligations would also make it difficult for start-ups to compete in global markets. For example, the lack of clarity would make it difficult for Indian fintech companies to gain access to innovative technologies like big data analytics, AI/ML tools, etc. which depend on data flows. They may also lose access to cost-efficient cloud services in the global market. Therefore, we recommend that sectoral regulators work with the DPA to ensure that regulatory uncertainty and conflicts are eliminated to promote business predictability.

- Restrictions on cross-border data flows harm India's economic growth prospects. These restrictions will have an adverse impact on the operational costs of businesses, burdening local companies with 30-60% additional computing costs. IAMAI-ICRIER report shows that if cross-border data flows were to decline by 1 percent, India's total trade could be negatively impacted by US$ 696.71 million[2]. The processing of big data is inhibited by imposing limits on data aggregation due to increased costs, complexity and eroding the informational value that can be gained from cross-jurisdictional transfers. Enabling the free flow of data across borders is crucial for India to meet its strategic economic policy goals of becoming a USD 5 trillion economy by 2025 as evidenced in the 2020 data localization report by CUTS International which notes that depending on the restrictiveness of the measures imposed and their outcomes, India could witness a shortfall of USD 9 -17 billion in achieving this goal.

[2] Economic_Implications_of_Cross-Border_Data_Flows.pdf (icrier.org)

- The JPC states that it is necessary to restrict countries from sharing SPD of Indians to any third country and the government can only grant adequacy to a country if it finds that SPD will not be shared with any foreign government . While the Report suggests that this is to restrict onward transfers to third countries, the changes to the text of the DP Bill suggests this is a pre-condition for adequacy. The restrictive conditions relating to adequacy may also result in very few countries being granted adequacy status. These restrictions may also fail certain threshold criteria such as objectivity and reasonableness that India is obligated to follow the introduction of these restrictions can also lead to retaliatory measures in other jurisdictions, which can have a significant impact on the outsourcing industry in India, especially in the IT sector. Free flow of data to enable market access is also endorsed by India's major trade partners in the Asia Pacific region, such as Japan and Singapore. With the DP Bill, India may be prematurely foreclosing its ability to participate in free trade agreements with these nations.

- The DP Bill vests many obligations and discretionary powers with the DPA and the government in relation to data transfers, which impose a heavier compliance burden. Data fiduciaries will have to obtain approval from the DPA for contracts or intra-group schemes involving cross-border data transfers, even after having obtained explicit consent of data principals for the transfer of SPD. The DP Bill requires that transfers of SPD in pursuance of a contract or intra-group scheme, must be approved by the DPA, "in consultation with the Central Government" and can be denied if it is against 'public policy' or 'state policy'. Public policy as a ground for denial of transfer may lead to unpredictability of interpretation, and in its current form it allows undue discretion to the DPA or Central Government to block cross-border data transfers. It is also likely that the DPA will not have the capacity and resources to approve each and every contract/scheme in a timely way, especially since the DPA is required to do so in consultation with the Central Government. These changes will create additional bureaucratic hurdles for companies that rely on free flow of data across borders. Further, the DP Bill contemplates a case-to-case analysis of the contracts or intra-group schemes and which will cause huge delays. There is inadequate state capacity to ensure such a review and approval process, which is bound to impact business in India. Most data protection laws allow for onward data transfers. For instance, when the EU was assessing Japan's Act on the Protection of Personal Information (**APPI**) for adequacy, it noted that Japan allows onward transfers to a third country if it ensures a similar level of data protection as the APPI and other Japanese laws. Such provisions allow for data to be shared in a responsible manner and would build trust between India and other countries. The DP Bill should be aligned with such international practices to aid in smooth running of businesses across borders. Under these provisions, the option to transfer information is available not only where the data principal has provided explicit consent, but also when the transfer is necessary for performance of a contract in the interests of the data principal, to protect the data principal's interests or for defense of legal claims, etc.

- We note the JPC's recommendations for cross-border SPD transfers are not in consonance with the established global practices and international businesses will need to completely change their existing storage practices for India specifically.

IAMAI Suggestions:

- **Imposing strict data localisation provisions will lead to difficulties in compliance and will be harmful for global and domestic companies alike. India should avoid data localisation requirements, which are ill-suited to protecting privacy and security, and which are inconsistent**

with trade commitments and modern data protection standards. Privacy and security protections are not based on the location of data.

- **Instead, the DP Bill should focus on establishing baseline standards for personal data that are consistent with global norms. This can include acknowledging tools and policy instruments designed to enable transfer between legal jurisdictions.**

- **The MeitY should set narrow limits as to what may constitute CPD and provide an exhaustive list of the types of data that will be considered SPD. The DP Bill should clearly specify the categories of 'critical personal data' and/or specify a principle based criteria for classification, e.g. based on the risk of harm to the data subject. The DPA, industry bodies and other stakeholders should be consulted before categories of CPD are notified by the government.**

- **We further urge the MeitY to the reconsider the JPC's retrospective recommendations on localisation, as foreign entities should not be subjected to restrictions that were not in force at the time of collecting data. This recommendation should be revisited to enable companies to store mirror copies of SPD outside India. This is a necessary measure for promoting ease of business in India.**

- **The requirement to continuously store sensitive personal data (SPD) in India should be removed since its transfer outside India is separately regulated under the DP Bill (for eg. through contracts approved by the regulator, i.e. DPA).**

- **If the local storage requirement for SPD is retained, we suggest that at a minimum it should be clarified that any such data can also be stored outside India as long as is necessary for processing, including storage, and is legally permissible.**

- **We submit that placing restrictions on cross-border flows may create circumstances that lead to higher business failure rates, barriers on growth of start-ups and increased costs for companies. It will also inevitably have a drastic impact on the ability of Indian consumers to access a truly global internet. In light of the concerns discussed above, we urge the MeitY to reconsider the extent of involvement of the Central Government in cross-border transfer decisions, as well as the requirement of seeking explicit consent from individuals. The DP Bill should expand the conditions for cross border transfer of data, by allowing for transfer of SPD outside India if explicit consent has been obtained. Exceptions should be provided for certain categories of data, contracts or schemes based on the DPA's one-time assessment.**

- **The DP Bill should allow for cross-border transfers on the basis of standard contractual clauses and binding corporate rules that are approved once off and not on a case-by-case basis. These mechanisms provide users assurances that a DPA approved level of privacy and security standards are being upheld, while creating a reasonable path for businesses to transfer data overseas as necessary to provide products and services. Specifically, we recommend that transfers outside India should also be allowed if any of the other transfer conditions have been met. Specifically, for cross border transfers:**

    - **The DP Bill should also allow for cross-border transfers on the basis of standard contractual clauses and binding corporate rules that are approved once off and not on a case by case basis.**

- **Instead of explicit consent AND meeting conditions of adequacy principle/approved contracts/specific purpose, the conditions for cross border transfer could be explicit consent OR meeting conditions of adequacy principle/approved contracts/specific purpose. That is, the DP Bill should allow businesses to transfer data outside India, so long as explicit consent has been obtained (for e.g. through contracts).**

- **Further, the DP Bill should enable bilateral and multilateral/regional mutual recognition frameworks and certification regimes, (e.g. modelling a light-touch US-India data transfer agreement after the EU-Japan mutual recognition of adequacy). This would help promote the secure and free flow of data and support cross-border privacy protections that are compatible with the borderless nature of trade and digital flows.**

- **Data fiduciaries should not be required to obtain the DPA's approval before each instance of transferring data outside India. Instead, alternative practices to ensure that privacy of Indian users is protected should be developed, such as, empowering DPA to independently approve model contractual clauses that govern companies' data protection practices, employing an independent third-party certifier for ensuring that SPD is transferred in accordance with high privacy standards, setting out minimum protections (e.g. Singapore PDPC's guidance) which should be in the scope of every contract governing overseas data transfer. Alternatively, the DPA can consider publishing one or more sets of approved standard contractual clauses which can be used by companies 'off the shelf', as the European Commission has done.**

- **The requirement for Central Government permission for sharing of SPD with a foreign government should be deleted.**

- **The government must avoid ambiguous phrases such as 'public and/or state policy', and ensure that businesses are not subjected to arbitrary approval processes that cause regulatory uncertainty and unpredictability. Explicit consent should not be mandated for transfer of SPD in addition to satisfaction of the other conditions contained in Section 34(1).**

- **To ensure that the restrictions with respect to overseas processing are harmonised with the DP Bill, all relevant sectoral regulations should be reviewed based on industry consultations.**

- **India should explore bilateral and multilateral frameworks and certification systems and make suitable changes to the DP Bill to promote the growth of the digital economy, trade and consumer choice.**

3. CERTIFICATION OF HARDWARE AND SOFTWARE PRODUCTS[3]:

The JPC recommends that the DPA should create a framework to monitor, test, and certify hardware and software for computing devices, to ensure 'integrity of hardware' and prevent 'interdiction or seeding' that may lead to a breach of personal data. The JPC also suggests that the DPA must 'keep a check' on hardware manufacturers to safeguard the integrity of digital devices. The JPC has suggested that the Government should set up a dedicated lab/testing facility, with branches spread throughout India, that will provide certification services for hardware and accompanying software. The DP Bill includes a provision that requires the DPA to ensure monitoring, testing and certification by an

[3] **Our member Reliance Jio has divergent view on certification of hardware and software products**

appropriate agency authorized by the Central Government for this purpose to ensure integrity and trustworthiness of hardware and software on computing devices to prevent any malicious insertion that may cause data breach. The standards of software testing, the agency that will be involved in such testing, the requirements for certification etc. have not been specified. This creates uncertainty and will increase compliance and operational costs in India.

Issue / Impact:

- Data fiduciaries under the DP Bill collecting personal data or SPD of data principals are already subjected to a comprehensive regime under the DP Bill, which includes obligations and safeguards in relation to how such data must be collected, processed, stored, etc. These obligations will continue to apply to hardware manufacturers, software providers and users who qualify as data fiduciaries under the DP Bill. Given this, it is unclear why a need for a certification mechanism has been envisaged.

- There is already an existing regime for hardware certification in relation to devices sold in India, which is governed by multiple regulators such as:
    - The Electronics and Information Technology Goods (Requirement for Compulsory Registration) Order, 2012 (Order), certain electronic products or devices are required to be compulsorily registered with the Bureau of Indian Standards (BIS) as a part of the Compulsory Registration Scheme (CRS).
    - Import of wireless equipment may require, as applicable: (a) an import license issued by the Wireless Planning and Coordination Committee (WPC); (b) type approval from WPC; (c) certification from the Telecommunications Engineering Centre (TEC); and (d) certification under the Mandatory Testing & Certification of Telecommunication Equipment (MTCTE) regime.
    - Under the Consumer Protection Act, 2019, service providers and product manufacturers are required to ensure that the product contains adequate instructions of correct usage to prevent harm or any warning regarding improper or incorrect usage, failing which they can be held liable. Additional labelling and disclosure requirements may apply under the Legal Metrology (Packaged Commodities) Rules, 2011.
    - Certain software and hardware used in the telecom industry are also subject to contractual conditions imposed from the unified license and the trusted telecom portal requirement.

- The above rules and regulations are sufficient to address the hardware and software certifications required, which should not be implemented under the DP Bill. If any additional requirements are to be imposed, it should be done under the existing framework and should sufficiently protect the confidentiality of the intellectual property of the developers.

- Global standards have been developed after rigorous testing and experimentation by various experts across different geographies. Introducing an untested compliance framework may lead to incompatibility of Indian devices with global technologies, further causing vulnerabilities. Additional certification and monitoring requirements will only burden companies, including enterprise service providers, who will have to modify their hardware and software technologies to comply with these obligations, significantly increasing operating costs. Further, testing and certification processes are time consuming and India is yet to build capacity for test labs to carry out certification in a timely manner and the electronics industry already suffers from huge lag when it comes to releasing a new product in the market. This delay has a direct impact on the

economy will further impact the electronics industry which is already affected by the shortage of chips. Needless to say, any delays in certifications also directly impacts the whole of India as they are heavily reliant on electronic devices for carrying out their occupation.

- Worldwide, manufacturers are already required to adhere to time-tested security standards and additional obligations will lead to unnecessary increase in compliance costs, thus disincentivizing entry into the Indian market and adversely affecting consumer choice through supply of quality products in the Indian market. An Asian Development Bank study notes that India already suffers from a lack of coherence with international standards, leading to an adverse impact on India's exports. Exporters suffer a 4.7-5.7% reduction in sales because of additional compliance costs arising out of barriers such as domestic standards, making them unviable in the global market, especially those with limited administrative and technical capacities. A 5% rise in marginal costs and 4% rise in prices because of these barriers also results in firms becoming unviable or reducing their profit margins.

- Across the world, international organisations and regulators have advocated for the need to harmonise standards. The WTO's Technical Barriers to Trade (TBT) Agreement commits India, as a WTO member, to use international standards as a basis for technical regulations, as far as possible. The Agreement also obliges India not to implement technical regulations that are more trade restrictive than necessary or with the view or effect of creating unnecessary obstacles to international trade. Imposing new certification requirements based on arbitrary, local standards would run counter to India's commitments in the WTO. Further, the WTO has noted that harmonisation helps achieve better compatibility between products, and a harmonised system allows for many more products to be available in the market – making it more economically viable for consumers. The European Commission has also argued for the need to support international standards to achieve greater harmonisation.

- Given that there are multiple certifications sought under the existing regimes and international standards, which fall under multiple regulators/ departments, such as TEC, WPC, BIS, MEITY, etc., the current proposal for involving the DPA as an additional regulator can result in uncertainty and confusion for the stakeholders and create conflict between different regulators. Further, such a requirement is unprecedented and there is no equivalent requirement under statutes such as the GDPR. There is no need for a separate certification process from a privacy and security point of view since most entities already ensure that hardware and software are compliant with global standards from a privacy perspective. However, in the interest of national security, if there is a need, a self-certification/self-declaration model may be adopted, as such data fiduciaries will already be compliant with the other conditions under the DP Bill. Any certification procedure should be introduced outside the DP Bill with an existing regulator and should sufficiently protect the confidentiality of the intellectual property in the hardware and software, in the interest of the growth of the industry and India's various international treaty obligations.

IAMAI Suggestions:

- **We recognize the Government's effort to strengthen its informational security framework through monitoring and certifying digital devices through which data is collected. However, we believe that introducing an additional and untested framework for this purpose through the DP Bill is out of place in the DP Bill.**
- **The government should refrain from introducing national or local standards or certification requirements and should instead focus on ensuring the adoption of internationally recognised standards which ensure compliance with globally accepted security-related testing of hardware**

and software products. Further, in the event there is a need for a regulation, self-declaration/certification model may be adopted to ensure that it does not hamper India's economy. The DP Bill should also refrain from widening its scope beyond data regulation to manufacturing and hardware.

4. SOCIAL MEDIA COMPANIES AS "PUBLISHERS":

Social media intermediaries (***SMIs***) and social media platforms – The JPC Report distinguishes between SMIs and "social media platforms" based on the reasoning that many social media companies are not intermediaries and rather "publishers" because of their "ability" to select the receiver of content and exercise control over access to content hosted by them. The Report contains a recommendation that these platforms should be liable for the content they host, particularly for content from unverified accounts on their platforms. This goes against the principle of safe harbour, established under Section 79 of the Information Technology Act, 2000 (***IT Act***) and the treatment of social media companies as "intermediaries".

Issue / Impact:

- The DP Bill is a data protection legislation and regulation of SMPs, as well as the criteria for safe harbour is not within the scope the DP Bill. As intermediaries are already governed by the IT Act and i.e. the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (***IT Rules***) adding new provisions such as SMP in the DP Bill will lead to regulatory conflicts and uncertainty and impact ease of doing business. The JPC itself comments in the Report that the DP Bill is a data protection legislation and the matter of social media regulation is a substantially different matter that requires its own regulation.
- Mere "ability" to select the receiver of third-party content or can control access to such content should not disqualify SMPs from safe harbour, especially since they would have to exercise this ability, on a case-to-case basis, to adhere to their due diligence obligations under the IT Rules.
- By making "ability" the criterion for disqualification from safe harbour, the very understanding of safe harbour under the IT Act that all intermediaries in India have structured their operations around is being completely overhauled.
- Further, by making SMPs liable for content that is posted on their platforms could potentially make SMPs extra-cautious about third party content on their platforms, leading to disastrous effects on the right to free speech and expression of their users.

IAMAI Suggestions:

- **In light of our concerns, we urge the MeitY to reconsider the recommendation to bring intermediary regulation within the scope of the DP Bill. Further, to be consistent with extant law, social media intermediaries continue to have safe harbour and not be regulated as publishers based on their "ability" to control content, given that this ability stems from a legal obligation.**

- **The DP Bill should not make provisions regarding social media regulation and safe harbour as it this lead to unnecessary regulatory overlaps**.

- **We posit that regulation of social media platforms is beyond the scope of a data protection legislation, creates unnecessary obligation for an SMI and does not in any way further the cause of data privacy of users.**

5. BROAD DEFINITIONS UNDER THE DP BILL:

Harm – In addition to Section 3(23) of the DP Bill that defined "harm" in an inclusive manner, the JPC has expanded on the definition to include "psychological manipulation which impairs the autonomy of any individual" and has empowered the Central Government to prescribe any other kinds of harm which may arise in the future owing to increasing technological innovation.

Issue / Impact:

- The scope of "psychological manipulation which impairs the autonomy of any individual" is vague and needs to be narrowed down to avoid ambiguity in interpretation of the law. Such a broad phrase (which has not even been defined by any global data protection law) will undoubtedly have far reaching consequences for various services provided by data fiduciaries. Even personalised and targeted services for the emotional and physical well-being of user may potentially come under the ambit of the "harm" on account of this phrase.

- In the absence of any guidance on what qualifies as psychological manipulation or what can be prescribed as harm in the future, data fiduciaries will not be able to anticipate the changes required to their operations to comply with this requirements, which creates business uncertainty and risk of business disruption and non-compliance. Fair business practices employed by businesses such as through algorithms designed using artificial intelligence/ machine learning technologies to provide targeted delivery or better consumer experience could also be called in to question by way of such broad scope.

- Additionally, a broad definition such as this also creates uncertainty as it has been drafted as a catchall provision without the intent to target specific types of harms, which will lead to lack of clarity in enforcement, as both data fiduciaries and processors as well as regulators will face difficulty in determining what falls within the scope of this definition.

- This wide scope will also have an indirect impact on the age verification requirements that may be prescribed by the DPA, for which one of the considerations is the possibility of harm that can arise to a child due to processing of her data by a data fiduciary. As a result, businesses will always be under a fear that their operations and business infrastructure may need to be continuously tweaked and overhauled pursuant to changes in the definition. The privacy by design policy implemented by data fiduciaries is also required to consider any harm that can be caused due to psychological manipulation of a data principal – any changes in the definition will lead to such policies also undergoing constant change, significantly increasing operational and compliance costs for business, which will reduce ease of doing business in India. The definition of harm must therefore be limited to include only categories that are in line with global standards.

IAMAI Suggestions:

- **In light of our concerns, we submit that the MeitY must reconsider the addition of psychological manipulation which impairs the autonomy of any individual" to the definition of "harm". The definition of harm should be exhaustive and not inclusive.**

- **Even if the phrase is retained in the text of the DP Bill, a specific meaning should be assigned and what constitutes "psychological manipulation" and when the same would "impair the autonomy" should be made very clear.**

- **We recommend that these definitions should be revised to align with the objectives of the DPB as regulatory uncertainty arising from problematic definitions often has a disproportionate impact on small businesses who do not have the capital to continue revamping their operations and services due to continuing changes in regulations.**

Personal Data - The inclusion of the phrase "any inference drawn from such data for the purpose of profiling" in the definition of personal data has widened the scope of the definition and made it open ended, subjective and vague. This is likely to have serious ramifications for businesses operating in India.

Issue / Impact:

- As a result of this, all inferred data, including data that is not been directly provided by data principals, will be considered to be included within the definition of personal data, and obligations under the DP Bill will extend to such data held by data fiduciaries. This could, in addition to significantly increasing the compliance burden on entities, also have serious implications for an enterprise's economic interests. For instance, the right to data portability will empower the data principals with the right to port the data which is inferred by the data fiduciary to form a part of the profile of the data principal. Such inferred data may form a crucial part of the business model, allowing them to have a certain competitive advantage. If such inferred data is required to be mandatorily transferred to another service provider, even so a competitor, it would disincentivise entities from operating in India and being subject to even more restrictive regimes than what are followed globally. It may even result in negatively impacting business models that rely on artificial intelligence/ machine learning (**AI/ML**) technologies to process their data, and could result in disclosure of proprietary information pursuant to the right to data portability.

- This broad definition also marks a departure from global practices such as the GDPR, as it does not provide for an understanding of what constitutes an 'inference'. Under the GDPR, inference data can only be qualified as such, if it meets certain essential conditions. Since the DP Bill already contains adequate provisions prescribing safeguards against excessive or large-scale profiling, it should remove inference data from the definition of personal data, or aim to clarify what could exhaustively be considered as inferences.

IAMAI Suggestions:

- **The term 'any inference drawn from such data for the purpose of profiling' must be deleted from the definition of personal data.**

Automated Means - The definition of 'automated means' includes equipment which is capable of operating automatically in response to instructions given or otherwise for processing personal data.

This definition will therefore possibly include all situations where personal data of a data principal is processed electronically, including processing done through AI/ML processes.

Issue / Impact:

- Since the definition of "data" also includes data processed through automated means, a wide-ranging scope of automated means will result in far-reaching consequences for businesses that are based on AI/ML and other similar processes for their operations.

- The definition is also problematic since it intends to bring within its fold every situation where data is processed electronically, regardless of whether there is any human intervention. This can have wide reaching impact for AI/ML tools.

- The DP Bill also grants a data principal the right to receive his or her personal data in a structured, commonly used and machine-readable format where the processing is carried out by automated means, however, exempts small entities from this requirement. Such classification may also result in large establishments divesting in order to classify as small entities, and escape obligations under the DP Bill.

IAMAI Suggestions:

- **The definition of automated means must not include 'or otherwise'.**

Sensitive personal data and critical personal data - Under the DP Bill, the definition of SPD can be broadened at any time by the Central Government. Further, the DP Bill empowers the Central Government to notify certain categories of personal data as CPD that can only be processed in India.

Issue / Impact:

- This broad right to amend the definitions of these terms with no clear mechanisms for industry consultation or checks and balances will lead to uncertainty in terms of implementation, as companies handling personal data, SPD and CPD will face constant requirements to update and revise their data handling processes based on such notifications, leading to high costs of compliance and impacting their efficiency and ability to innovate. There should be certainty regarding the scope of these definitions and the government should not be permitted to expand the scope through notifications.

IAMAI Suggestions:

- **The definitions of SPD and CPD must not be permitted to be expanded through modifications, without consultations with the relevant stakeholders.**

6. JOINT LIABILITY AND COMPENSATION:

The DP Bill provides for joint and several liability of data fiduciaries and data processors "*[w]here more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal*". While this is a beneficial step for data principals, the mechanism by which it is implemented is unjust and fails to address the complexities associated with such a compensation structure. Under the proposed mechanism, any data fiduciary or data processor can be ordered to pay the entire compensation

amount and later claim from each of the other data fiduciaries or data processors the amounts corresponding to their responsibility for the harm caused.

Issue / Impact:

- As per the proposed mechanism, even though a data fiduciary has a majority of the responsibility for a specific harm caused, it is possible that a data processor which was merely acting according to its contractual obligations on behalf of the data fiduciary be required to pay the full compensation amount to the aggrieved data principal, even if the extent of harm caused by it is far less. Even after such payment, there is uncertainty as the DP Bill does not specify any clear mechanism by which the paying entity may claim against the other data fiduciaries or data processors, nor a timeline within which this must take place.

- The data fiduciary determines when to collect personal data, the reasons for collecting personal data, and also controls all decisions on how it uses and discloses that personal data, while data processors merely process data on the instructions of the data fiduciary. Therefore, data processors typically have no insight into the type of data that is stored or processed using their services and cannot distinguish personal data from other types of data. As a result, data processors are not typically in a position to know what steps they ought to take to ensure that they are not acting negligently with respect to the personal data they process on their systems other than to ensure they have appropriate technical and organizational measures for the security of their own systems. This could also jeopardize India's IT industry, which consists of a multitude of small data processors which cannot afford to bear the burdens brought by this Section 65.

IAMAI Suggestions:

- **Section 65 should be amended to lay down clear criteria for determination of the obligation of payment on processing entities and data fiduciary.**

7. AGE OF CONSENT

The DP Bill sets the age of consent at 18 years. While, the JPC refers to the recommendations of the Srikrishna Committee Report, and reinstates them as a justification for retaining 18 years as the valid consenting age for processing of personal data, there exists teething issues in keeping the age of majority as the age of consent.

DP Bill would require platforms that serve users under 18 to verify children's age and seek parental consent.

Issues/Impact

- Keeping a blanket threshold of 18 years as the age for providing valid consent would be inimical to the growth of industries that offer tailored knowledge as well as entertainment focused products and services for children. This threshold is also much higher than global standards, and in a globally inter-connected digital reality that we live in, it is important that already established principles are followed to the extent possible. For example, in the United States, the Children's Online Privacy Protection Act pegs the threshold at 13 years, while it is 16 years under the EU GDPR, and many EU Member States have made use of their right to lower the age to 13 (eg. Belgium), 14 (Austria) and 15 (France). The threshold of 18 years may result in a very large number of users being cut off from access to these services, which could impact their overall well-being, as well as their intellectual and emotional development.

- Setting the age of consent to data processing at 18 years will create additional friction in teenagers' online experience that will stand in the way of their access to knowledge and prevent them from getting the full benefits of online services. Many of these teenagers rely on online services to learn and self-educate. Age-gating requirements will also be applied unevenly, creating disparity and disrupting the equalizing power of the Internet. For the children of less educated, less digitally literate families, the additional requirements of parental consent might be enough to impede their access to online services altogether.

- The DP Bill requires a data fiduciary to verify the child's age and obtain the consent of their parent or guardian. The DP Bill goes on to state that age verification and parental consent mechanisms must take into certain factors which may be expanded based on factors prescribed in the future. In the absence of certainty on guidelines on age verification and parental consent mechanisms, there may be a "chilling effect" on companies providing services to children, causing pre-emptive or defensive ceasing of services. Further, it would pose significant logistical challenges for providers, impacting business predictability and ease of doing business.

- Obtaining parental consent would prove difficult in practice, in addition to the age verification burden. These additional identification requirements would pose barriers to many developers building startups, in addition to established companies. Further, the DP Bill's proposed age verification mechanism would invariably result in data fiduciaries having to collect more information about all individuals, including data which is potentially sensitive personal data. Practically, the service providers may need to verify the age of all users to comply with the requirement, which could create more privacy risks for users, including children. This seems to reduce and not increase privacy protections. Very importantly, such age verification could also undermine the privacy of these users and affect anonymity on the internet, essentially taking away certain privacy choices from individuals.

- Given all the challenges outlined above, the unintended outcome of this requirement may be that data fiduciaries would instead choose to pre-emptively or defensively not provide services to children to avoid the compliance burden. It could also mean that companies can only offer services when users are "signed-in" and reducing options for individuals to stay anonymous.

IAMAI Suggestions:

- **In light of our concerns, we submit that that the MeitY brings in a graded, proportionate risk based approach for children's age of consent depending on the kind and nature of service provided. The rigid approach of setting the age of majority as the age of consent would be against the principle of 'best interest of the child' in a digital world as it creates barriers for a child to attain educational and recreational fulfilment available on the internet. In fact, the definition of a 'child' should be reduced from 18 years based on global norms like the GDPR.**
- **We also further appeal to MeitY to study more effective risk-based approaches followed in other jurisdiction.**
- **The requirement to verify the age of children should be removed to avoid creating new privacy risks through the collection of potentially sensitive information of children and all users.**

- **Parental consent mechanisms should not be prescriptive, as it creates practical challenges and could result in a 'chilling effect'. Rather, the implementation guidelines should focus on**

empowering young users and their parents with transparency and privacy tools, while allowing service providers to consider a broader range of technical solutions to ensure this.

- **Alternatively, age verification should be a self-declaration, and onus for the veracity of information should ideally lie on the data principal.**

- **Requirement for obtaining parental consent should be removed and even if the requirement is to be retained, any change requiring parental consent to process data for users under the age of consent (with or without age verification) should be applied on a going-forward basis. In other words, if a user has legally consented to the data processing typical for an account before enactment of this legislation, that individual should be able to use that account as agreed without additional parental consent.**
- **We recommend that Chapter IV of the DP Bill should be made applicable only to those services which are directed to children.**

8. PROHIBITIONS ON PROCESSING CHILDREN'S DATA:

Profiling, Tracking, or Monitoring – Pursuant to the removal of the concept of a "guardian data fiduciary", every data fiduciary is now barred from "profiling, tracking, or behavioural monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child." under Section 16(4) of the DP Bill.

Issue / Impact:

- Profiling, tracking, monitoring, etc. are important tools in the hands of the data fiduciary to help them keep children safe online. If a complete prohibition is imposed on monitoring and profiling activities, data fiduciaries may not be in a position to take necessary steps to detect their underage users and adequately safeguard their interests. Further, the DP Bill does not distinguish between the above actions and broadly restricts actions such as tracking or behavioural monitoring even when such actions may be required to improve technology on the platform and address social issues (for e.g., promoting child safety). If this concept is implemented, the DP Bill should be modified to clarify the specific and reasonable scenarios where tracking, profiling, etc., is restricted, for instance only where such activities may cause significant harm to the child.

- Additionally, it seems that the underlying rationale behind a complete prohibition on data fiduciaries from targeting advertisements directed at children is that all targeted advertisements are harmful to the interests of children. But this assumption in simply not tenable and by imposing such a prohibition, data fiduciaries will not be able to provide educational, emotional and physical well-being related services.

- Additional compliances may also be attracted by data fiduciaries processing data relating to children or providing services to them since the DPA is empowered to notify them as a significant data fiduciary (**SDF**). Being notified as an SDF imposes significant compliances on a data fiduciary, which include undertaking data protection impact assessments, audit of policies, appointment of data protection officer etc. The DP Bill however fails to provide any threshold parameters or conditions for a data fiduciary to be notified as an SDF, so long as they process children's data or provide services to them. Such a broad application may lead to multiple entities being notified as

SDFs – and the applicable additional burdens may deter such entities from developing and providing services to children and consequently impact the quality of services provided to children in India.

IAMAI Suggestions:

- **In pursuance of our concerns, we submit that the relevant provisions under Section 16 of the DP Bill should only be limited to prohibiting processing activities that are proven to cause significant harm to children.**
- **To impose reasonable restrictions on data fiduciaries, Section 16(4) should be modified as follows: "*The data fiduciary shall be barred from profiling, tracking or behavioural monitoring or targeted advertising that can cause significant harm to the child or undertaking any other processing of personal data that can cause significant harm to the child*."**
- **The power to classify data fiduciaries processing children's data or providing services to them as SDFs should be removed.**

9. REQUIREMENT OF SERVICES TO NOT BE DENIED BASED ON EXERCISE OF CHOICE*:*

Denying services based on choice - Section 11 of the DP Bill provides that consent be obtained from a data principal for PD processing activities. However, as part of this provision, the JPC has now added that the provision of any goods or services, the performance of any contract, etc. should not be denied "*based on exercise of choice*".

Issue / Impact:

- We note that the practical applicability of this provision is unclear due to lack on any insight about the reason for its inclusion. The question that presents itself at this juncture is what happens in cases where it is not possible to provide a service in the absence of relevant PD because a data principal exercises their choice in not consenting to the processing of their PD.

- We also note that mandating data fiduciaries to not deny goods or services, etc. on the basis of a lack of consent to provide PD that is not "necessary" for the relevant purposes is ambiguous. The enforcement of this provision will be impossible without specifying the standards or thresholds to determine which PD is considered "necessary" for the processing of any purpose. The necessity of a dataset depends on its required use. A data set that may be "necessary" for providing a personalised service may not come within the scope of "necessary" for a more generic service. On a literal reading this provision, data fiduciaries may have to always explain to a data principal the reason behind the exact level of PD required, followed by customization of services in accordance with the degree of consent granted by such data principal. This will prove to be a time and cost inefficient system.

IAMAI Suggestions:

- **In light of the concerns presented above, we urge the MeitY to do away with the addition "*based on exercise of choice*" as it is ambiguous and would lead to operational difficulties.**

- **We also submit that the MeitY should remove the requirement of mandating data fiduciaries to not deny goods or services, etc. on the basis of a lack of consent to provide PD that is not "necessary".**

10. ABSENCE OF CONTRACTUAL NECESSITY AND LEGITIMATE INTERESTS AS SECONDARY PROCESSING GROUNDS:

Legitimate interests - This has been recognised as a ground for processing PD for "reasonable purposes" (as may be notified by the DPA) without a data principal's consent under Section 14 of the DP Bill.

Issue / Impact:

- Although we appreciate this inclusion, the involvement of the DPA renders the inclusion futile. Enabling the DPA to make such determinations for every conceivable activity may overburden the DPA, which is already tasked with other regulatory and quasi-judicial responsibilities. Therefore, data fiduciaries should be empowered to process PD without consent upon a determination of its own legitimate interests and without involvement of the DPA. Similarly, data fiduciaries should be able to process PD without consent for contractual obligations. This is because it may sometimes be infeasible for data fiduciaries to seek consent for every instance of processing in furtherance of their contractual obligations with data principals.

IAMAI Suggestions:

- **In light of the above, we request the MeitY to explicitly enable data fiduciaries to process PD without consent for global recognised secondary grounds of processing such as "legitimate interests" and "contractual necessity".**
- **We recommend that the DP Bill should expand the legal bases for processing by replacing the provisions relating to "reasonable purpose" with the more expansive concept of legitimate interest to promote innovation and development of cutting-edge technologies across sectors like fintech and healthcare.**
- **Further, we recommend that routine/repetitive processing of personal data and SPD should be allowed on the basis of contractual necessity.**

11. IMPOSITION OF HIGH PENALTIES:

High Penalties - Under the DP Bill, Section 57 provides a penalty extending to 2 to 4% of the "total worldwide turnover" of a data fiduciary. However, the quantum of penalty as may be imposed on a data fiduciary is now left to be prescribed by the Central Government in the form of rules.

Separately, the DP Bill seeks to penalise any person who knowingly or intentionally re-identifies any de-identified personal data, without consent. The DP Bill provides for imprisonment of up to 3 years or a fine, which may extend to INR 2,00,000, or both. Under the current definition of the DP Bill, harm is not a pre-requisite, and it is not necessary to show that harm was caused.

Issue / Impact:

- The definition of "total worldwide turnover" is very broad and can include revenue that is not generated by a data fiduciary in India. The fact that such revenue may not be directly related to data processing activities in India has not been taken into account. This is not in consonance with the concept of "relevant turnover" (as has been recognised for the penalty provisions under the

Competition Act, 2002). This will undoubtedly have a negative impact on ease of doing business in India for global companies.

- The criteria for imposition of a penalty is not very specific. It is unclear, for example, what failure to take "prompt and appropriate action in response to a data breach" exactly means. Thus, it is important that there is a clear indication of what factors need to be taken into account to give rise to a penalty in such cases.

- The Central Government has broad discretion in determining the range from 0.1 to 4% of the global turnover of a data fiduciary while imposing a penalty. However, such discretion should at the very least be supported by guiding principles.

IAMAI Suggestions:

- **In light of the concerns listed above, we submit that the MeitY should take steps to formulate guiding principles within Section 57 of the DP Bill. These principles should include standards that will help avoid arbitrary levy of penalties and will help in prescribing the exact quantum of penalties. These guiding principles should focus on the following factors: (a) a penalty levied should not exceed the total gain, benefit or unfair advantage accruing to the data fiduciary, and (b) a penalty as a percentage of turnover should be based on an assessment of "significant harm" that is caused to a data principal.**

- **Additionally, the term "total worldwide turnover" should be reconsidered in light of the reasons highlighted above.**

- **Further, the threshold of penalties under the DP Bill is excessive compared to other privacy legislations around the world. Accordingly, we recommend that the DP Bill should propose a graded penalty mechanism depending on the severity of harm caused to data principals**

- **Further, steps should be taken to avoid double punishment being meted to data fiduciaries for the same contravention (penalties under Section 57 and compensation under Section 65) as this poses the risk of significantly impacting the ease of doing business in India and may inhibit global companies from investing in India's technology sector.**

- **We recommend that the DP Bill be revised to remove the criminal penalties.**

12. EXPANSION IN TRANSPARENCY REQUIREMENTS:

Algorithmic Transparency – We note that certain amendments have been made to the transparency and disclosure requirements applicable to data fiduciaries vis-à-vis Section 23. Now, disclosure of information relating to the "*fairness of algorithm or method used for processing of personal data*" has to be done by the data fiduciaries. According to the JPC, will help prevent its misuse.

Issue / Impact:

- While acknowledging this step, we note that this compliance is very broad and may encroach upon the data fiduciaries' intellectual property rights, it may be harmful to data fiduciaries if they are mandated to publicly disclose their algorithms and other proprietary information, especially without adequate safeguards. Technology companies invest heavily in data science technologies

to make use of raw/factual data and disclosure requirements will negate the competitive advantage held by these companies, making their investment worthless. Companies will be disincentivized from investing in technological advancements and research and development relating to data science, which will have a negative impact on the economy of the country. It will also impact new investments in India and may lead to a flight of capital from India to countries which recognize the right of companies to proprietary data and algorithms. The disclosure of algorithms and data will dilute competitive advantage and competitors anywhere in the world could leverage any disclosed proprietary data. This will starve the Indian start-up ecosystem from crucial foreign funds as investors will flock to other investment destinations.

- While the recommendations intend for sharing of algorithms for possible evaluation for 'fairness', it is unclear on what basis and by which agency will an algorithm will be determined as 'fair'. Overly broad transparency and explainability obligations may have negative implications for the protection of business secrets or for the pursuit of legitimate public or private interests. This may delay or prevent the adoption of AI systems.

- There are other safeguards provided in the DP Bill (such as Section 5 which seeks to ensure fairness of data processing activities and the definition of "harm" which includes discriminatory treatment – read with Section 65 on compensation, annual auditing of policies, appointment of Data Protection Officers, and the requirement of data protection impact assessment under certain circumstances by significant data fiduciaries) which will protect a data principal against discriminatory treatment they may face through automated decisions.

IAMAI Suggestions:

- **Given our concerns with regard to the inclusion of algorithmic transparency, we urge the MeitY to reconsider this addition. Currently, the NITI Aayog is in the advanced stages of developing a nuanced and risk based approach to regulating specific AI use cases. The NITI Aayog has done so after several years' worth of consultations with sectoral experts and a deep examination of the subject. Including a broad provision on algorithm fairness in the DP Bill would only serve to contradict the NITI Aayog's approach, and create fear, uncertainty and doubt within industry and with investors. Given the Government's goals of becoming a global AI leader, we recommend that this provision be deleted in its entirety.**

13. LACK OF A TRANSITION PROVISION IN THE DP BILL:

Transition Period - The JPC Report, recommends that a phased period of 24 months be provided for implementation of all provisions of the DP Bill from the date of notification. The JPC has suggested that a phased implementation should be undertaken to ensure that the Chairperson and Members of DPA are appointed within 3 months, the DPA commences its activities within 6 months, the registration of data fiduciaries should start no later than 9 months and adjudicating officers and the Appellate Tribunal commences their work no later than 12 months.

Issue / Impact:

- We appreciate this recommendation of the JPC, however, we note that it has not been reflected in the amended text of the DP Bill. This will undoubtedly create confusion and operational/compliance mismanagement in the implementation of the DP Bill. Lack of such provisions

will also hamper the ability of the stakeholders to prepare themselves to be compliant with the DP Bill.

IAMAI Suggestions:

- **We submit to MeitY that there is a need for incorporating a precise timeline within the DP Bill in pursuance of its positive impact on the ease of doing business and to provide certainty to entities as well as individuals on the date from which operation of the provisions of the DP Bill will be enforced.**

14. APPOINTMENT OF DATA PROTECTION OFFICER BY SIGNIFICANT DATA FIDUCIARY:

Issue / Impact:

The JPC report recommends that every significant data fiduciary shall appoint a data protection officer (**DPO**) who shall be a senior level officer in the State or key managerial personnel in relation to a company. For purposes of this sub-section, the expression key managerial personnel mean CEO or MD, CS, whole time Director, CFO or such other personnel as may be prescribed.

IAMAI Suggestions:

- **We suggest that the requirement that the DPO should be a key managerial personnel should be replaced by a senior personnel.**

15. **OBLIGATIONS UNDERMINING INTELLECTUAL PROPERTY OF BUSINESSES:** In furtherance of the policy objective to establish transparency, the DP Bill requires data fiduciaries to provide information about the fairness of the algorithm or method used to process personal data, amongst other information. To fulfil such an obligation, the data fiduciary will necessarily have to disclose the working of the algorithm itself. Such an obligation can have significant ramifications for business models who offer services based on their unique algorithms, such as algorithms deployed by music apps to curate customized and personalized recommendations and similar business models based on algorithmic curations for movies, news etc.

    Separately, we note that revelation of a data fiduciary's trade secret cannot has not been recognised as a ground for refusing a data portability request made by a data principal. A data fiduciary can only refuse to carry out a data portability request if it is not technically feasible, subject to the regulations prescribed by the DPA.

    Issue / Impact:

    - We believe that in today's data-driven era, businesses heavily invest in the development of their unique algorithm or technologies to analyse data for their services and providing such proprietary information could result in disclosure of their sensitive and confidential information, threaten IP protections, and chill innovation and the development of new technologies.
    - There is also no obligation on the authorities to maintain a duty of care or confidentiality towards such information shared with them. Imposing requirements to share algorithms without any safeguards will disincentivise companies from investing in technological

advancements and R&D relating to data science. It will also impact new investments in India. This may lead to a flight of capital from India to such countries, which recognise the right of companies to proprietary data and algorithms.

- The disclosure of algorithms and data will result in a loss of competitive advantage and competitors all around the world can leverage any proprietary data disclosed to advance their position. This will starve the start-up eco system from much needed foreign funds as investors will flock to other investment destinations. It will also impact India's position in ease of doing business rankings.
- Additionally, India's international commitments – such as its obligation under the TRIPS to provide a minimum level of protection to IP rights such as trademarks, copyrights, patents, trade secrets, may also be questioned if requirements which may compromise businesses' IP are implemented.
- The requirements of transparency are sufficiently addressed by the gamut of accountability tools prescribed under DP Bill currently, including but not limited to the requirement for annual auditing of policies, the conduct of processing of personal data, the appointment of data protection officers, and the requirement of data protection impact assessment under certain circumstances by SDFs.
- Separately, considering revelation of a data fiduciary's trade secret cannot be a ground for refusing a data portability request, not providing sufficient exemptions and safeguards for protection of intellectual property of businesses, will have a chilling effect on innovation and the development of new technologies. Data fiduciaries, from the fear of disclosure of their proprietary or confidential information, will choose to not operate or process data in India, which will have several ramifications on an economic and international front, as discussed above.
- Developed frameworks such as GDPR recognise that rights of data principals should not adversely affect trade secrets and copyright protecting software. Similarly, the OECD recognises that a failure to guarantee IP protections would dilute the rewards for investing in innovation, and that there is a positive relationship between the stringency of trade secret laws and the extent of innovation in the economy. The European Parliamentary Research Service study on algorithmic transparency also notes that mandating confidentiality through IP laws is the only way to protect a company's competitive edge and prevent its rivals from copying their algorithms. Not retaining the trade secret exception in the right of data portability provision could have serious implications on IP rights and stifle innovation. It can also negatively affect India's obligations under international trade agreements to which India is a party to and may lead to international trade issues.
- If such exceptions are not carved out to protect businesses, it will stifle innovation and competitors will find ways to disclose IP and trade secrets through frivolous claims of privacy violation. Trade secrets must therefore be exempted from data portability requests.

IAMAI Suggestions:

- We recommend that algorithms and methods of processing be kept outside the purview of the transparency obligation and instead be exceptions to the transparency and data portability rights of data principals.
- The MeitY should consider carving out IP and trade secrets as exceptions to the (i) obligation to disclose algorithms and data processing methods and (ii) data portability requests, so as to prevent dilution of IP protection through these proposed changes. Businesses should not be required to effect any data portability requests if they involve disclosing a trade secret or proprietary algorithm.

16. COMPLIANCE BURDEN AND DISCRETIONARY POWERS WITH THE DPA:

Issue / Impact:

Heavy Compliance burden compared to global data frameworks

- DP Bill vests many discretionary powers with the DPA and imposes several additional obligations, especially on SDFs, which are not part of other prominent data protection regimes like the EU GDPR. For example, DP Bill provides for:
    - Mandatory registration
    - External audits and publication of 'trust scores'
    - DPA's approval for data transfers, new technologies, codes of practice, etc.
    - DPA to specify what would constitute a 'reasonable purpose' exception
    - Certifying the "Privacy by Design policy" to participate in the sandbox and otherwise
    - Methods of anonymisation, de-identification, data erasure etc.

- Such high-handed regulation will severely impact emerging digital sectors like fintech, healthcare, etc., where firms process large volumes of data. Moreover, there are concerns about the capacity of the DPA to establish the necessary infrastructure and expertise to approve, monitor and enforce these provisions.

- The exercise of the DPA's discretionary powers will have a significant impact on the processing activities undertaken by businesses (for example, additional requirements for notice and obtaining consent, 'reasonable purposes', data portability, etc.). Frequent changes will require businesses to overhaul their technical and organisational practices. All this unpredictability would impede the ability of businesses to plan their operations ahead of time to off-set costs. For small businesses and start-ups especially, this would be a huge set back.

Lack of regulatory capacity and expertise within the DPA

- The DPA is entrusted with various supervision and enforcement functions under the DP Bill. The developments in technology are so dynamic that attempting to monitor for compliance will likely place an overwhelming burden on any government agency or regulator entrusted with such monitoring obligations.
- It is also unclear whether the DPA will have the necessary regulatory capacity to make determinations regarding classification of SDFs and social media intermediaries. Instead of nurturing the technology ecosystem as intended, this regulatory load will ultimately harm consumers, businesses and the government as well.

Grounds for classification as SDFs

- The factors to be taken into account for the classification of SDFs are quite subjective. This creates significant discretion with the DPA, and we believe that the parameters for classifying a data fiduciary should be more specific.
- Further, some of the factors for classification as an SDF are unreasonable. For e.g., turnover of a data fiduciary and usage of new technologies for processing is not a reasonable classification for an entity to be classified as an SDF, especially given the use of such technologies in cutting-edge domains such as healthcare, fintech, etc.

Need for a consultative approach to rule-making

- DP Bill establishes the DPA as an independent regulator to oversee monitoring and enforcement. In order to administer its functions, the DPA is empowered to make regulations, issues codes of practices and to give directions. Accordingly, we believe the DPA should be required to engage in a thorough consultation process before exercising these powers. Besides this, it must conduct adequate ex-ante and ex-post assessments of regulatory impact.
- Though DP Bil provides for mandatory consultations between the DPA and other stakeholders before issuing codes of practice, it is important that this requirement be extended to the various other rule-making powers of the DPA, to ensure that the expertise within the private sector is appropriately leveraged.
- According to DPB, the government need not consult the DPA on key aspects of rule-making, including:
    - Data classification (i.e. notifying categories of critical personal data and additional categories of sensitive personal data)
    - Grievance redressal (manner of making complaints, etc.)
    - Exempting certain data processors (eg. for the purpose of outsourcing activities) and government agency from the applicability of the law.
- Ensuring that the DPA consults other stakeholders, and is consulted by the government on key delegated rule-making powers will help promote business predictability.

IAMAI Suggestions:

- MeitY may consider narrowing down DPA's prescriptive powers so as to minimise business unpredictability and compliance burden, by promoting co-regulation and self-regulation models, specifically:
- Mandatory registration requirements for SDFs should be removed, since the DPA will be notifying authority for SDFs and can review or publish the list of SDFs if required.
- The parameters for classification of SDFs should be more specific and reasonable. Unreasonable grounds such as turnover of a data fiduciary should be removed.
- The concept of ‘trust scores’ should be encouraged as an industry best practice.
- Submission of a "Data Protection Impact Assessment" should not be made mandatory for the use of new technologies or involving sensitive personal data categories.
- Audits should be performed by the Data Protection Officer of the data fiduciary (and not external auditors) to encourage corporate accountability through self-regulation, prevent duplication of efforts and an increase in compliance costs for start-ups.
- Specifically, we recommend that ‘social media platforms’ need not be separately regulated by the DPA, since the term ‘social media intermediary’ (SMI) is subject to strict regulations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. We posit that regulation of social media platforms is beyond the scope of a data protection legislation, creates unnecessary obligation for an SMI and does not in any way further the cause of data privacy of users.
- We recommend that there should be minimal DPA intervention in routine business operations. Frequent changes based on rules and regulations issued by the DPA will require businesses to overhaul their technical and organisational practices, which would be expensive and cumbersome. Instead, the DPA should rely on self-regulatory efforts (e.g. internal audits, rather than external audits) and market driven efforts (e.g. voluntary mechanisms around trust scores). The functions of the DPA should be focused more towards capacity building, education & awareness and grievance redressal.

- To promote consultative rule-making, industry bodies, companies and start-ups should be consulted before any standards are prescribed around security, anonymisation, portability etc. It is also recommended that the government be required to consult with the DPA on key issues like data classification.

17. **RIGHT TO BE FORGOTTEN:** The DP Bill provides the data principal with the right to be forgotten, i.e., the right to restrict or prevent the continuing disclosure or "processing" of his/her personal data by a data fiduciary in certain specified circumstances.

Issue / Impact:

- The inclusion of processing, in addition to disclosure under the right to be forgotten, results in an expansive scope of the provision – even more so considering the definition of processing under the DP Bill, which also includes storage. This may have an unintentional impact on business models of cloud service providers providing online storage and other similar services.
- This approach also goes against international standards such as the GDPR where a data subject is granted a right to erasure (also referred to as right to be forgotten), but not both.
- Given that the DP Bill separately provides the data principal the right to erasure of personal data which is no longer necessary for the purpose for which it was processed, the right to be forgotten should be limited to continued disclosure and should not include processing. This will ensure alignment of the rights under the DP Bill with global practices and prevent overlap with other rights under the DP Bill.

IAMAI Suggestions:

- **We recommend that the right to be forgotten provision must be limited to continued disclosure and exclude processing from its ambit. This will not only be as per international standards, but also avoid redundancy within the DP Bill itself.**

18. **PROCESSING OF PERSONAL DATA FOR OTHER REASONABLE PURPOSES:**

Issue / Impact:

In an increasingly digitised economy, telephone directory, caller ID and spam blocking is an inalienable building block to enable safe communication for the community in a world where frauds, stalking, and harassment are being continuously perpetrated and initiated online and by telephone calls and messages. Provision of telephone directory, caller ID and spam blocking is an inevitable need of society for reasons of public safety, fraud and crime prevention. It serves a fundamental public interest particularly those of the unsuspecting and vulnerable sections of society including the elderly.

The bill in its current draft can potentially have negative and unintended consequences for those services that enable telephone directory, caller ID and spam blocking services as the Bill treats the name and phone number as personal data without making any allowance for provision of such services. In our view it is vital that the provisions of the Bill that restrict the sharing of information should focus on risks or concrete harm and seek to preserve services that deliver a community benefit. By designating name and phone number as personal information without providing an exception for the provision of telephone enquiry and directory services, the Bill risks inadvertently legislating away a vital community service that has minimal to no harm from a privacy perspective. The Bill has sought

to recognise this for the operation of search engines and in our view should do so as well for telephone enquiry and directory services.

It is a basic minimum expectation of recipient of call / message to know who the caller / sender is (akin to a homeowner's right to know who is on their doorstep), consent cannot be the norm because of the inherent conflict and impracticality of obtaining consent for such purpose and as such should be afforded legislative recognition to process names and phone numbers without consent.

The expectation of an individual to keep their name and phone number private when making phone calls is outweighed by the critical public interest and public safety concern addressed by identifying the calling party. It is in the reasonable expectation of both the originator and recipient of communication (whether by phone or SMS) that the identity of the originator is known. This is vital to avoid harms associated with online and telephone-based frauds, crimes, harassment and stalking.

IAMAI Suggestions:

- **Section 14 of the Bill that deals with "reasonable purposes" for which data may be processed without consent needs further legislative clarification.**
- **Due to the overwhelming public interest, processing of personal data without consent for telephone directory, caller ID and spam block purposes be specifically included in Sec. 14(2) of the Bill, similar to how 'the operation of search engines' has been included. This would serve the purpose of protecting citizens, and especially the vulnerable sections of society from unlawful activity such as frauds, stalking and harassment.**

19. OTHER ISSUES:

We would like to highlight some additional points which are as under:

- **Data Breach Reporting Obligations**: The DP Bill requires data fiduciaries to mandatorily report to the DPA, all personal data breaches within 72 hours of becoming aware of such breach, by way of a notice. Further, the DPA is required to direct data fiduciaries to mandatorily report a breach to the data principal and post details of the same on its website DP Bill should align with other global privacy frameworks by requiring Data Fiduciaries to notify the DPA of a data breach only when the breach presents a "significant risk of material harm" to data principals. Requiring Data Fiduciaries to notify the DPA of any data breach (regardless of harm) risks overwhelming the DPA with notifications, and could end up exacerbating security risks by distracting the DPA from the more serious data breaches.

- **Lack of Clear Parameter for Government Access to Data (Recommendation 56):** The government can exempt itself from the law after following just, fair, reasonable, and proportionate procedures. At the same time, the Committee, when discussing offenses committed by government entities, acknowledges that government agencies and departments can be significant data fiduciaries in many contexts, and thus should establish Standard Operating Procedures (SOPs) and in-house inquiry processes for fixing liability for any offense.
- **Unclear Independence of the DPA from the Government (Recommendation 62 & 63):** The Committee recommends that the selection committee for the DPA have wider representation from technical, legal, and academic experts, in addition to the bureaucrats, however, the selection process remains heavily in favour of the government.