ITI Promoting Innovation Worldwide

March 8, 2022

Shri Ashwini Vaishnaw,

Honourable Minister,

Ministry of Electronics & Information Technology,

Government of India

Dear Shri Vaishnaw,

The Information Technology Industry Council (ITI) is the premier global advocate and thought leader for the information and communications technology industry. ITI's membership comprises leading technology and innovation companies from all corners of the tech sector, including software, digital services, and internet companies. They are headquartered across Asia, the United States, and Europe, and many are significant investors and employers in India. Because of the broad nature of our membership, we bring a global perspective that considers the diverse views of our membership when we engage with policymakers around the world to work toward policy initiatives that promote innovation and inclusiveness in the global economy.

On behalf of the information technology sector, we are writing you to share our concerns with the Report of the Joint Parliamentary Committee on Personal Data Protection Bill, 2019 (Report) presented before the Lok Sabha on December 16, 2021. We appreciate and commend the efforts of the Joint Parliamentary Committee (JPC) in undertaking an extensive exercise to produce a data protection and privacy legislative framework for India. We also appreciate the recommendations of the JPC with respect to promoting India's digital economy and start-ups.

However, we believe certain recommendations of the JPC will unintentionally limit the ease of doing business in India, hamper the country's continued economic growth, and constrain the ability of Indian and global companies to innovate in India. ITI foresees a risk that other competing economies that offer less complex and more practical regulatory environments for data may attract investments away from India. We are optimistic that the Honourable Prime Minister's vision of making India a $5 trillion economy can materialise soon if the Indian Government continues to focus on risk-based regulations and policies that balance regulatory burden with benefits to the Indian public.

Furthermore, given the implications of certain elements of the Report, we feel strongly that the process of developing a comprehensive data protection framework must be transparent, risk-based, and iterative to ensure alignment with government objectives and the avoidance of collateral impacts on Indian businesses, consumers, and workers. As such, we reiterate our request as expressed in a multi-association letter dated March 1, 2022 sent to the Ministry of Electronics and Information Technology (MEITY), to conduct additional consultations with all concerned stakeholders before the introduction of the updated data protection bill in Parliament.

In addition to our narrative responses immediately below, we have included several of our key concerns in Annexure A of this document.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

ITI Key Concerns and Recommendations

1. Incorporation of non-personal data (NPD) within a single legislation

The policy objective of regulating non-personal data is fundamentally different from that of personal data protection. The former is premised upon data sharing in the interest of transparency and openness while the latter is concerned with protecting user privacy. Regulating non-personal data requires a distinct set of considerations and approaches, which has also been acknowledged by MEITY's Committee of Experts on Non-Personal Data Governance Framework released in December 2020.[1] MEITY has also recently released a consultation on Data Accessibility and Use Policy which restricts the sharing of non-personal data from government agencies and departments. This clearly indicates the government's intention to have a wider stakeholder consultation before mandating any form of data sharing. Meanwhile global regulations in mature privacy regimes such as Europe's GDPR, Canada's Personal Information Protection and Electric Documents and Brazil's LGPD have also refrained from regulating non-personal data as part of the same schemes, considering the issues highlighted above. Additionally, the Report contemplates that NPD and personal data can be subjected to the same regulator, the Data Protection Authority (DPA). This approach may be impractical given that NPD and personal data require different sets of expertise and will lead to regulatory uncertainty due to fundamental conceptual differences between NPD and personal data. To that end, expanding the potential scope to include NPD will complicate breach notification requirements in Chapter VI, potentially creating uncertainty and compliance burdens on industry members. Deployment of procedural safeguards such as Intellectual Property Right (IPR) protections may be needed for mandatory sharing of NPD. We therefore consider it essential to exclude non-personal data from the proposed personal data protection legislation to align with global frameworks and request MEITY to reconsider Recommendation No. 2 of the Report.

2. Strict data localization obligations

Even though the free flow of data is an important contributor to India's economy, Recommendation No. 12 of the Report insists on gradually moving towards complete localization of data. Effective privacy protection measures do not rely on localization requirements as there is little evidence to suggest such localization obligations further the aims of data protection. In fact, the goal of keeping Indian citizens' data secured might be undermined through this requirement by creating a single point of failure as a target for a cyber intrusion/attack and reducing access to state-of-the-art solutions globally. Further, the Report's recommendation that the storage of Sensitive Personal Data (SPD) and processing and storage of critical personal data (CPD) take place exclusively in India raises significant concerns. Combining the NPD with personal data under one framework fails to acknowledge the complexity presented by mixed datasets, i.e., types of data that are inextricably linked and cannot be separated in order to adhere to these definitions, a complexity that is widely acknowledged in jurisdictions such as the EU. The lack of clarity in the definitions of SPD, CPD and personal data exacerbates this concern, because if the JPC is correct

[1] MEITY. "Report by the Committee of Experts on Non-personal Data Governance Framework". December 16, 2020. Clause 5.3 "In this regard, it would be appropriate to amend the provisions of the PDP Bill to ensure that it does not regulate non-personal data…."

that CPD is not easily segregated from other data types, the unavoidable result is that all data in India will in effect become subject to a hard data localization requirement. The net effect of these provisions would ultimately raise privacy and cybersecurity concerns over the large volumes of data to be held in India, likely hindering foreign direct investments in the country. The expansion of the data localization provisions that requires providers to mirror copies of SPD and CPD already in their retrospective application could lead to operational challenges for many Indian and foreign companies that hold SPD and CPD. We request MEITY to reconsider these data localization obligations, in the interest of protecting the privacy of India-based users and promoting the Government of India's ease of doing business goals.

3. Restrictions on cross-border transfers

Recommendation No.11 in the Report maintains the 2019 Bill's extensive requirements for the transfer of data outside of India and adds additional restrictions for the Data Protection Authority to consult the Central Government for all cross-border transfers of sensitive personal data (SPD). This proposed requirement not only undermines the independence of the new proposed DPA, but undoubtedly creates further business uncertainty regarding cross border transfers as well as friction in the Indian business environment that will slow data innovation, compounding the risks and costs of doing business in India. Additionally, despite valid law enforcement access concerns, adding such a central government "check" would place companies in difficult conflict of laws situations by placing them in an untenable position due to the divergent legal requirements across multiple jurisdictions. Further, placing upon individuals the responsibility to consent to every transfer of their SPD creates a likelihood of "consent fatigue" and may ultimately run counter to the objective of engendering greater consumer control over SPD. Finally, as data transfers are often necessary for the functioning of global services, it will be technically impracticable or infeasible to require providers to provision their services to users who withhold their consent for data transfers, as the proposed bill currently does. We request MEITY to ease the requirement of obtaining approval of the DPA and the Central Government for every cross-border transfer. As an ideal alternative, the DPA should be empowered to approve model contractual clauses and other internationally recognized prevailing cross border data transfer mechanisms (e.g., the APEC Cross Border Privacy Rules System) that govern companies' data protection and transfer practices and ensure adequate safeguards. We also request MEITY to incorporate a ground for data transfers based on necessity for the performance of a contract or the provision of a service.

4. Certification of Hardware Devices

The requirement of monitoring, testing, and certification of hardware devices by the DPA under Recommendation No. 10 should not be included in a personal data protection framework as it will create an additional layer of compliance that will delay commercial access of hardware in the Indian market. This certification process will require the DPA to be armed with specific technical expertise that cut across many technology segments and overlap with the existing Ministry of Communications' Mandatory Testing and Certification of Telecom Equipment (MTCTE) program (administered by the Telecommunications Engineering Centre (TEC) that already tests and certifies numerous hardware devices that connect to the telecom network. Redundant testing and certification schemes make it more complex and costly to introduce products to the Indian market. Introducing such redundancies increases the cost of compliance, restricts market access, causes

import delays, and runs counter to the Indian Government's stated goals of enhancing ease of doing business and increasing investments in the country. Further, this requirement is an outlier to global privacy protection frameworks and would most certainly add costs to doing business, adversely impacting India's Ease of Doing Business landscape, and create regulatory confusion. We therefore strongly recommend MEITY to remove this provision altogether.

5. Treatment of social media companies as publishers

During the open comment period for the PDP Bill in 2019[2], we had highlighted in our response that the inclusion of special rules for social media intermediaries within the data protection bill – and specifically those that would effectively stipulate the legal treatment of social media intermediaries as publishers – would not enhance the privacy protection for Indian citizens. We maintain this position and further submit that the inclusion of intermediary guidelines and content regulation provisions within a data protection framework will cause significant regulatory uncertainty and impose untenable burdens on firms falling within scope. Intermediaries in India are already regulated comprehensively under India's Information Technology Act, 2000 (IT Act). We urge MEITY to reconsider this proposal as it is contrary to the principle of safe-harbour encapsulated in Section 79 of the IT Act for all intermediaries.

The JPC's recommendation will be fundamentally inconsistent with the existing law in India and impact the operations of Internet companies, which are premised on the assumption of safe harbour and already entail the performance of mandatory due diligence under the IT Act. We oppose the notion of treating social media intermediaries as publishers as such treatment can bring about a chilling effect on the right to free speech and expression of social media users. We therefore urge MEITY to reconsider Recommendation No. 6 of the Report dealing with intermediary liability and the treatment of social media intermediaries as publishers within the data protection framework.

6. Age-gating and limitations on processing data of children

The requirements relating to processing the data of children in Recommendation No.5 deviates from well-established global best practices. For example, the GDPR provides an age range of 13-16 years for consent of processing personal data to ensure the privacy of users within that range is protected, while giving minors the autonomy to make decisions. We fully share the objective of enabling a safe online environment for children, which seems to form the basis for the age-gating and requirements of consent. We further agree that parental consent may be justified for children below the age of 13 years. Additionally, there is also a blanket restriction on data fiduciaries' profiling, tracking, and monitoring the behaviour of children, in addition to restrictions on targeted ads and data processing that may cause significant harm to children. Even where well-intentioned, such blanket restrictions can potentially deprive children and young persons in reaching useful content. For instance, such prohibition can impede availability of content related to mental health support services to young persons in need. We note that verification of age of users (as is currently required) can be done through varying mechanisms, but one possible mechanism involves

[2] Information Technology Industry Council (ITI). "Recommendations for the Personal Data Protection Bill 2019". March 4, 2020.

monitoring of user activity to install age-appropriate safeguards. We request reducing the age limit from 18 to between 13-16 years for minors, at parity with global standards. We also call for the removal of blanket restrictions on reprocessing of data for targeted advertising, among other purposes. Finally, we call for allowing enterprises to develop their own age verification mechanisms drawing from internationally accepted guidelines

7. Contractual necessity and legitimate interests as essential non-consent-based grounds of processing

We note that Recommendation No. 37 has identified legitimate interests of the data fiduciary as a tenable ground for processing of personal data without requiring the consent of the data principal for "reasonable purposes", as to be determined by the DPA. However, we believe that the involvement of the DPA in the procedure renders the provision less meaningful, as processing data for legitimate interests should be an express, independent ground of processing available to all data fiduciaries in addition to consent. We note that it is not always practical for data fiduciaries to seek consent at every step for processing personal data, especially when such processing takes place in pursuance of contractual obligations owed to a data principal. Similarly, processing personal data of data principals on the basis of a data fiduciary's legitimate interests (such as to detect fraudulent transactions, detect and research malicious cyber threats, etc.) without having to obtain additional consent is a crucial ancillary purpose of processing that should be enabled and empowered. We encourage the MEITY to incorporate provisions allowing data fiduciaries to process personal data without consent for contractual obligations and legitimate interest as globally recognized grounds.

8. Broad and unclear definitions of harm, SPD and CPD, and financial data

The Report has suggested an addition to the definition of "harm" under Recommendation No. 23 by adding the phrase, "psychological manipulation which impairs the autonomy of any individual". Additionally, the JPC has given further powers to the Central Government for inclusion of more classes of harm. However, there is no guiding clarification in the Report or any other global law, on what would amount to psychological manipulation and when individual autonomy can be said to be deprived. Even global data protection laws currently do not attempt to regulate such kind of harm. Such fundamental ambiguity in a critical definition can have a disproportionate bearing on certain services (such as personalized online services). Moreover, the Government is empowered to prescribe other kinds of harm arising due to technological leaps. This not only creates operational uncertainty in the law but is also not at parity with global standards. Further, the definition and scope of SPD and CPD is wide and concerning. The definition of SPD is broad, not exhaustive like the GDPR, whereas the scope of CPD has not yet been defined by the Government. Additionally, the term "financial data" has been widely defined, thereby leading to a lack of clarity on its ambit. This may lead to ambiguities and increased compliance on data localization and cross-border data transfers. We urge MEITY to reexamine these broad definitions of SPD, and financial data, as well as reconsider the inclusion of this added definition of "harm," consider the removal of the category of CPD, minimize legal ambiguity, and clarify what amounts to psychological manipulation and when it can be considered to have impaired individual autonomy.

9. Transparency requirements with respect to algorithms

Recommendation No. 44 requires data fiduciaries to fulfill certain transparency and disclosure requirements. The Report has added an additional requirement of disclosure relating to "fairness of algorithm or method used for processing of personal data". This requirement, which is an addition to the Bill's already broad transparency requirements, coupled with a lack of safeguards, exposes data fiduciaries to the risk of having their proprietary rights compromised as they may be required to publicly disclose their source code, algorithms, machine learning techniques, etc. We therefore suggest that the MEITY to reconsider the inclusion of transparency requirements with respect to the algorithms used by data fiduciaries as there are other provisions in Recommendation No. 29 that would safeguard a data principal from discriminatory processing activities.

10. Alternative financial system

Recommendation No. 8 proposes to establish an alternative to the SWIFT payment system which raises significant concern. The global financial system has continued to function well and adapted with technology advancement to improve privacy protection for individuals. To enhance data protection there are several available tools and laws, including the pending PDP Bill, that can serve to elevate privacy without taking a disproportionate approach of creating an entirely different financial system than the rest of the world. We therefore strongly recommend MEITY to remove this provision altogether.

11. High civil penalties

Recommendation No. 71 of the Bill prescribes high penalties ranging from 2% to 4% of the "total worldwide turnover" of a data fiduciary. The provision contemplates "total worldwide turnover" to include the revenue generated by a data fiduciary outside India as well. However, it does not account for the fact that revenue generated outside India may be irrelevant as it may not have any link with processing activities in India. Further, a penalty can be imposed if a data fiduciary fails to "take prompt and appropriate action in response to data security breach". However, it has not been clarified as to what amounts to prompt and appropriate action and on what factors such actions are to be assessed. Additionally, the Government is armed with wide discretion to determine the quantum of penalty. We suggest that the term 'total worldwide turnover' must be reconsidered and include additional guidelines on penalties, as well as taking into account the overlap between penalty and compensation to avoid adverse impact on investments in India.

12. Unclear transition provisions

We welcome the Report's suggestion on 24 months (under Recommendation No. 3) be provided for the implementation of the Bill from the date of notification. However, the definite timelines have been left to be decided by the Government. The JPC has also recommended specific transition periods for certain provisions such as 3 months for the appointment of DPA and 6 months for the commencement of the DPA's activities, beginning of registration of data fiduciaries within 9 months and commencement of work of Adjudication Officers and Appellate Authorities within 12 months. These timelines, however, are only recommendations and the task of providing definite timelines

within the law is left to the Central Government. We encourage METIY to adopt a precise timeline for the Bill to ensure ease of doing business and provide compliance certainty.

ANNEXURE A

Recommendations of Parliamentary committee and earlier PDP bill 2019	ITI suggestions	Reasons
Incorporation of non-personal data (NPD) within a single legislation (Recommendation No. 2, 16 & 25) (Clause 2 and Clause 3(28) of Bill)	Separate NPD from the privacy framework being articulated under data protection bill. Continue the wider stakeholder consultation on regulating and mandatory sharing of non-personal data.	There is difficulty in distinguishing PD and NPD in cases of mass movements of mixed data sets. Deployment of procedural safeguards such as Intellectual Property Right (IPR) protections may be needed for mandatory sharing of NPD. Legislative framework on NPD is evolving globally and we urge the government to give wider consensus approach on non-personal data regulation framework.
Strict data localization obligations (Recommendation No. 12)	Reconsider data localization obligations, in the interest of protecting the privacy of India-based users and promoting the Government of India's ease of doing business goals.	Combining the NPD with personal data under one framework fails to acknowledge the complexity presented by mixed datasets, i.e., types of data that are inextricably linked and cannot be separated to adhere to these definitions, a complexity that is widely acknowledged in jurisdictions such as the EU. The inability to segregate data between SPD, CPD and personal data may lead to hard localization.
Restrictions on cross border data flows (Recommendation No. 11) (Clause 33 and 34 of Bill)	Ease the requirement of obtaining approval of the DPA and the Central Government for every cross-border transfer. The DPA should approve model contractual clauses and other internationally recognized	We request MEITY to ease the requirement of obtaining approval of the DPA and the Central Government for every cross-border transfer.

	prevailing cross border data transfer mechanisms.	
Certification of hardware devices (Recommendation No. 10&66) (Clause 49(2)(o) of Bill)	MEITY should not include this provision in the new redrafted bill.	Redundant and repetitive testing and certification schemes make it more complex and costly to introduce products to the Indian market. Introducing redundancies increases the cost of compliance, restricts market access, causes import delays, and runs counter to the Indian Government's stated goals of enhancing ease of doing business.
Treatment of social media companies as publishers (Recommendation No. 6 &27) (Clause 3(44) of Bill)	MEITY is requested to drop elements of the Report dealing with intermediary liability and the treatment of social media intermediaries as publishers within the data protection framework.	Inclusion of intermediary guidelines and content regulation provisions within a data protection framework will cause significant regulatory uncertainty and impose untenable burdens on firms falling within scope.
Age-gating and limitations on processing data of children (Recommendation No. 5&38) (Clause 16 of Bill)	We request reducing the age limit from 18 to between 13-16 years for minors, at parity with global standards. We also call for the removal of blanket restrictions on data fiduciaries, as data fiduciaries should be allowed to develop their own age verification mechanisms.	Broad restrictions can potentially deprive children and young persons in reaching useful content.
Contractual necessity and legitimate interests as secondary grounds of processing (Recommendation No. 37)	We encourage MEITY to incorporate provisions allowing data fiduciaries to process personal data without consent for contractual obligations and legitimate interest as globally recognized grounds.	It is not practical for data fiduciaries to seek consent at every step for processing personal data, especially when such processing takes place in pursuance of contractual obligations owed to a data principal.

Broad and unclear definitions of harm, SPD and CPD, and financial data (Recommendation No. 23) (Clause 3 (41), Clause 3(21), Clause 3(23))	METY should reexamine these broad definitions on SPD, CPD, and financial data, as well as reconsider the inclusion of this added definition of "harm," to minimize legal ambiguity, and clarify what amounts to psychological manipulation and when it can be considered to have impaired individual autonomy.	Definitions are broad and ambiguous, which creates uncertainty for businesses. It also lends itself prone to legal challenges.
Transparency requirements with respect to algorithms (Recommendation No. 44)	MEITY should reconsider the inclusion of transparency requirements with respect to the algorithms used by data fiduciaries as there are other provisions to safeguard a data principal from discriminatory processing activities.	Such requirement, coupled with a lack of safeguards, exposes data fiduciaries to the risk of having their proprietary rights compromised as they may be required to publicly disclose their source code.
Alternate financial system (Recommendation No. 8)	MEITY should remove this clause and continue to work with stakeholders to develop a globally interoperable Indian financial system.	To enhance data protection there are several available tools and laws, including the pending PDPB, can serve to elevate privacy without taking a disproportionate approach of creating an entirely different financial system than the rest of the world.