Computer & Communications Industry Association
Tech Advocacy Since 1972

February 24, 2020

Via electronic email: jpc-datalaw@sansad.nic.in; mrs.mlekhi@sansad.nic.in

Smt. Meenakshi Lekhi,
Member of Parliament,
Chair, Joint Committee on The Personal Data Protection Bill, 2019

Director, Lok Sabha Secretariat,
Room No. 152, Parliament House Annexe,
New Delhi, 110001

Re: Comments of the Computer & Communications Industry Association on the Personal Data Protection Bill, 2019

Dear Smt. Meenakshi Lekhi, MP:

The Computer & Communications Industry Association (CCIA) respectfully submits these comments regarding the Parliament of India's Joint Committee consultation[1] on the proposed Personal Data Protection Bill (PDPB).[2] CCIA appreciates the opportunity to provide its views on the proposed legislation, and raise concerns about aspects of the law that would impact the growth of India's digital economy and have negative implications for Internet services and their users.

CCIA is an international, nonprofit association representing a broad cross section of large, medium, and small companies in the high technology products and services sectors, including Internet products and services, electronic commerce, computer hardware and software, and telecommunications.[3] For over 40 years, CCIA has advocated for promoting innovation and preserving full, fair, and open competition.

[1] Consultation Announcement, Joint Committee on the Personal Data Protection Bill, 2019 (Feb. 4, 2020), *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/pr_files/Press%20Communique-English%204%20Feb%202020.pdf.

[2] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, [In.] *available at* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (hereinafter "PDPB").

[3] A list of CCIA members is available at https://www.ccianet.org/members.

As a general observation on administrability, the PDPB outlines a complex regulatory framework for managing the protection of personal data in India. Given the complexity and scope of the PDPB, regulators must ensure a sufficient implementation period after the Data Protection Bill is enacted. This is critical for stability of the digital economy and for industries, especially SMEs, to understand the extent of their obligations under the new law and update practices as needed. CCIA recommends an effective date for the PDPB set at least 24 months following enactment, consistent with the sunrise period adopted by the General Data Protection Regulation (GDPR) in the EU.[4] Furthermore, the bill must provide clear resolution mechanisms with regards to any conflicts and jurisdictional questions that may arise pertaining to existing laws and regulations, such as between the PDPB's provisions on transferring personal data outside India and the Reserve Bank of India's directive on the storage of payment system data.[5]

CCIA's comments below outline concerns regarding the following: the scope of the PDPB's data portability requirements (Section 19), proposed restrictions on transferring personal data outside India (Chapter VII), issues regarding the independence of the proposed Data Protection Authority (outlined in Chapter IX), and the proposed authority for the Central Government to compel the production of anonymized or non-personal corporate datasets for formulating policy or targeting services (Section 91).

I. Section 19: "Right to Data Portability"

Section 19 of the Bill provides for a right to data portability for individuals with respect to personal information processed by data fiduciaries. Data portability can be a tool that enables users to assert control over their personal information or try different products and services; however, mandating the disclosure of proprietary information through portability tools would undermine intellectual property protection. Moreover, depending upon implementation, data portability provisions can have anticompetitive effects.

CCIA is concerned that the PDPB's right of data portability could be interpreted as extending to information that includes confidential or proprietary business information. Specifically, the data categories subject to the portability requirement designated in Section 19 (a)(ii iii) include "the data which has been generated in the course of provision of services or use of goods by the data fiduciary", and "the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained."[6] These datasets may include data that qualifies as a proprietary asset or intellectual property of the data fiduciary, such as sensitive company insights

[4] *Compare* General Data Protection Regulation, Art. 99 *with PDPB* § 1 (2).

[5] *See* Reserve Bank of India, DPSS.CO.OD No. 2785/06.08.005/2017-2018, "Storage of Payment System Data" (Apr. 6, 2019), *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF.

[6] *PDPB* § 19 (I)(a)(ii, iii).

and protected analytics generated through the investment of significant financial and technical resources.

Furthermore, the revised Bill contains an expansive definition of "personal data" that threatens to create overbroad portability requirements that are inconsistent with emerging international portability standards and the commonly understood categories of personal data. Under Section 19 (a)(i), an individual also has a right to receive "personal data provided to the data fiduciary." However, the revised Bill's definition of "personal data" includes "data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, *and shall include any inference drawn from such data for the purpose of profiling*" [emphasis added].

In contrast, Article 20 of the GDPR provides for a right to data portability concerning only "personal data concerning him or her, which he or she has provided to a controller." Subsequent regulatory guidance has clearly excluded "inferred data" and "derived data" from the right to portability under the GDPR.[7] Therefore, to promote consistency and ease of data transfers, ensure individual control over their personal data, and protect business proprietary information, any data portability right under the PDPB should be limited to personal data that an individual has provided to a data fiduciary and not extend to the category of "inferred" data.

II. Chapter VII: "Restriction on Transfer of Personal Data Outside India"

CCIA welcomes revisions to sections concerning the localisation of personal data from the 2018 draft; however, the restrictions on the transfer of personal data outside India outlined in Chapter VII of the PDPB would nevertheless present barriers for digital commerce.[8] The PDPB would place prescriptive requirements for data mirroring and localisation for "critical" personal data, and "sensitive" personal data with only limited exemptions included for these categories of information.[9]

Data localisation requirements can increase data security risks and costs, as well as introduce privacy risks, by requiring storage of data in a single centralized location that is more vulnerable to natural disasters, intrusion, and surveillance. When Governments assert national security

[7] *See* Article 20 Data Protection Working Party Guidelines on the right to data portability (adopted Apr. 5, 2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 at 10.

[8] Section 40 of the 2018 draft of the PDPB required that every data fiduciary "ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act." *See* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[9] *PDPB* Chapter VII "Restriction on transfer of personal data outside India".

grounds for localisation, it is critical that these regimes are narrowly used, transparent, and provide clarity on the types of critical personal data affected by these mandates.

Localisation and mirroring requirements are also likely to restrict the ability of local companies to participate and compete in the global marketplace by limiting access to the global supply chain. Local businesses may not be able to expand their product or services to large numbers of potential customers around the world. This isolation may result in reduced investment and access to capital and customers. Recent analysis from the OECD has revealed an increasingly level of restrictiveness for digitally-enabled services in part due to restrictions on cross-border movement of data.[10]

Should the Joint Committee nevertheless determine that restrictions on the transfer of personal data outside India are appropriate, the categories of information subject to such restraints must be clearly defined at the outset. As drafted, the PDPB establishes restrictions on "critical personal data" defined solely as "such personal data as may be notified by the Central Government to be the critical personal data".[11] This definition is insufficient and provides no clear direction for companies to establish compliance for this data category. Further, the open-ended mandate that would permit the Central Government to designate additional categories of "critical personal data" should be removed.

III. Chapter IX: Data Protection Authority of India

In order to ensure consistent and effective enforcement of the data protection responsibilities under the PDPB, the Data Protection Authority of India (DPA) must be a strong, independent, fairly-funded regulator, with the requisite expertise to oversee rapidly changing digital services. The DPA must also be empowered to engage with its counterparts around the world to facilitate collaboration and exchange of best practices.

As currently drafted, there are concerns that the PDPB falls short of realizing this objective for the DPA. The 2019 version of the Bill outlines a governance structure where the members of the DPA are to be appointed only by the Central Government, excluding external or judicial participants in the selection process, as was the case in previous drafts of the Bill.[12] Limiting appointments to the DPA to the executive would make it harder for the DPA to fulfill its necessary role as an independent authority that can exercise impartial oversight over both private industry and government bodies. CCIA recommends revisions to this Chapter to ensure that the

[10] OECD Services Trade Restrictiveness Index: Policy Trends up to 2020, *available at* https://issuu.com/oecd.publishing/docs/oecd-stri-policy-trends-up-to-2020?fr=sNmVlNzYxOTI3Mw.

[11] *PDPB* § 33 (2).

[12] *Compare PDPB* § 42 and *PDPB* (2018) § 50, *available at* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

DPA and Adjudicating Officers can serve as effective and independent enforcement authority of data protection obligations.

IV. Section 91: "Act to Promote Framing of Policies for Digital Economy"

The PDPB would grant the Central Government power to demand the production of broad categories of business data that threatens to undermine privacy protections for users and appears to conflict with established intellectual property rights in India. Specifically, Section 91 of the PDPB would establish new authority for the Central Government to direct any data fiduciary or data processor to produce any "personal data anonymized" or other "non-personal data" to "enable better targeting of delivery of services or formation of evidenced-based policies."[13] As an initial matter, this proposed regulation of non-personal data appears to exceed the intended scope of the PDPB, which is limited to the protection of personal data.[14]

Furthermore, the ability for the government to obtain such data, based on unclear "policy" grounds, raises serious privacy concerns.[15] Anonymization of data is a highly technically complex practice that is difficult to ensure in perpetuity.[16] The PDPB lacks both detailed definitions for "anonymisation" and "non-personal" and limitations on subsequent access to and use of information produced pursuant to this Section, thereby placing the privacy of both individuals and social groups at risk.[17]

In addition to these privacy concerns, the ability for the Government to demand the production of extensive datasets collected, inferred, or aggregated by companies, including intellectual property and confidential business information, appears to conflict with existing intellectual property law in India. The Copyright Act, 1957 extends "literary work" protection to business

---

[13] *PDPB* § 91 (2).

[14] *PDPB* § 2.

[15] *See* Udbhav Tiwari, *Don't Rush Into Bad Law: Giving India Data Protection Law it Deserves*, India Express (Dec. 9, 2019), https://indianexpress.com/article/technology/opinion-technology/personal-data-protection-bill-giving-india-the-data-protection-law-it-deserves-6157994/ ("Allowing the government to force companies to transfer non-personal data raises serious intellectual property concerns, and can still threaten users even if they're not individually identified. For example, would we want the government knowing which housing colonies in a city have a propensity to buy pro-LGBTQIA+ posters, books about a specific caste, or religious objects? This data may not contain any identifying information about a specific individual but can be used by malicious actors with disastrous consequences.").

[16] Boris Lubarsky, *Re-Identification of 'Anonymized' Data*, 1 Geo. L. Tech. Rev. 202 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/

[17] Chapter VIII of the PDPB outlining "Exemptions" may also exacerbate privacy concerns. The text in the current version of the PDPB will enable the Central Government to grant exemptions from complying with obligations set out in the legislation to a far broader set of government agencies than in the 2018 Bill. *Compare PDBP* § 35 with *PDPB, 2018* § 42, *available at* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

datasets in certain cases, as well as insights, analysis, and conclusions drawn from them.[18] The PDPB's proposed government mandate to share these categories of "non-personal" data would therefore conflict with existing law and public policy.

V. Conclusion

Thank you for the opportunity to share the views of CCIA on The Personal Data Protection Bill, 2019. As outlined in these comments, adjustments to the proposed PDPB are warranted to ensure that India establishes a data protection framework that will uphold the fundamental right of privacy and provide consistent expectations and data processing responsibilities for all participants in the digital economy. Industry looks forward to continuing to engage with the committee and other stakeholders in the Government of India's important work of drafting a framework for the protection of personal data.

Respectfully submitted by:

Keir Lamont
Policy Counsel
Computer & Communications Industry Association

[18] *See* Vidushpat Singhania, *Is There a Database Right Protection in India?* Lakshmikumaran & Sridharan (Mar. 2013), https://www.lakshmisri.com/newsroom/archives/is-there-a-database-right-protection-in-india/#.