11 September 2020

CIPL Response to the Indian Ministry of Electronics and Information Technology's Report by the Committee of Experts on a Non-Personal Data Framework

I. INTRODUCTION

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the Ministry of Electronics and Information Technology's (MeitY) Report by the Committee of Experts on a Non-Personal Data Framework. As a starting point, CIPL appreciates MeitY's consideration of how India can unlock economic, social and public value from data, including through data sharing to enable the availability of data throughout India's digital ecosystem. CIPL supports accountable data sharing between organizations in both the public and private sectors and this has become even more important following the COVID-19 pandemic. However, CIPL cautions the pursuit of a non-personal data framework in advance of finalizing India's rules on the protection of personal data via the proposed Personal Data Protection Bill (No. 373 of 2019). In addition, multiple aspects of the framework raise questions around potentially negative impacts it would have on Indian and global businesses, individuals and regulators. This short response outlines the relevant concerns.

1. Interaction with the Personal Data Protection Bill

The Personal Data Protection Bill (PDPB) is currently undergoing a review by a Joint Parliamentary Committee of both houses of the Indian Parliament. If passed, organizations established or operating in India will need to invest significant time and resources to enable compliance with the many new rules introduced by the PDPB. The PDPB contains very expansive provisions and will require much more on the part of organizations than under the current Information Technology Act 2000 and its 2008 Amendment. Added to this, many of the Bill's provisions are not sufficiently clear and may be elaborated upon following the report of the Joint Parliamentary Committee. For example, the definition of "critical personal data" has yet to be defined; the role of the data protection authority and the central government in specifying additional categories of sensitive personal data is still not clear; and new concepts such as "significant data fiduciaries" will likely raise new questions. The non-personal data framework equally introduces novel concepts, such as new definitions for public, private and community non-personal data, as well as a new definition for sensitive non-personal data. It also introduces new roles, including "data custodians" and "data trustees," as well as a whole new framework for mandatory data sharing with governments and organizations. Furthermore, some potential overlap and inconsistencies may arise in the interaction of the PDPB with the non-personal data framework. For example, the PDPB includes specific rules on consent and a definition of anonymized data. However, the non-personal data framework introduces a new requirement to obtain a separate consent from individuals to anonymize data. In addition, the standard of anonymization to be used is not clear. For instance, the PDPB leaves the standard of "irreversibility" to be defined by the data protection authority. At the same time, the Committee Report on the non-personal data framework recommends that appropriate standards of anonymization be defined to prevent and minimize the risk of re-identification. It is not clear which entity would define such standards. Is it the data protection authority in line with its role to define "irreversibility" under the PDPB or is it the new non-personal data authority that would be set up by the non-personal data framework? However India defines a standard for anonymization, such a standard should be consistent across India's digital and data ecosystem.

In order to avoid organizations becoming totally overwhelmed with a whole set of new, confusing and potentially inconsistent data concepts and rules, CIPL recommends that MeitY support the Joint Parliamentary Committee in passing comprehensive privacy legislation in India via the PDPB and the yet to be established Data Protection Authority in clarifying the scope of the new rules.

Following this, MeitY should further consider the recommendations it is proposing in the non-personal data framework. It should do this via a multi-stakeholder process with industry to ensure that any framework for data sharing can:

(1) unleash the value and power of data while also being practical, realistic and supportive of innovation and investment in the data economy by individual organizations; and

(2) enable a flexible and pragmatic approach for sharing data that protects individual rights and other company rights, including intellectual property rights and business proprietary information.

Taking such an approach will also provide India with the benefit of understanding how the sharing of personal data sets or mixed data sets (consisting of personal and non-personal data) is taking place under the PDPB and can inform any subsequent dedicated framework for data sharing.

2. Data Localization Rules

One major point of concern within the PDPB is India's proposed rules restricting the transfer of sensitive and critical personal data outside of India. CIPL has previously argued against the inclusion of such provisions in the PDPB.[2] These broad localization rules are also included in the non-personal data framework and will raise many issues for organizations.[3] These include:

(1) prohibiting the use of technology relying on distribution of data, including cloud computing, data analytics and AI and machine learning applications;

(2) imposing the creation of redundant storage systems;

(3) increasing costs to prohibitive levels for local and foreign small and medium enterprises;

(4) compromising data security, by preventing the partitioning of sensitive data sets across global servers, which can provide an additional layer of protection against hackers as well as business continuity in the case of natural disasters; and

(5) creating complex conflict of laws situations.

In addition, localization rules may result in the *de facto* prohibition of sharing of data across borders for important scientific health research activities, including to fight against the COVID-19 pandemic. Such rules may also impact the need to share financial information across borders by organizations to comply with their obligations to prevent financial crimes (e.g. Know-Your-Customer and Anti-Money Laundering obligations) or to prevent fraud in the use of their services.

For India to maintain its ability to play a leading role in the global digital economy and continue to flourish as a global center of innovation and trade for both Indian and multinational organizations, it is imperative that the PDPB and any future data sharing framework include interoperable rules on

data transfers. In its recent paper on "Enabling Accountable Data Transfers from India to the United States under India's Proposed Personal Data Protection Bill,"[4] CIPL puts forward several options to govern cross-border flows of data under the PDPB. These include less trade-restrictive solutions that can addresses relevant concerns driving a desire for personal data to remain in India while preventing unnecessary barriers to data transfers.

3. The Role of Consent

As mentioned above, the non-personal data framework introduces a new requirement to obtain a separate consent from individuals to anonymize data. Such an approach runs counter to the goals and incentives of anonymization, which are:

(1) to protect individuals by removing personal identifiers associated with data; and

(2) to enable data to be used and shared more broadly, especially for social good and societal benefit.

Under the non-personal data framework, the expert Committee recommends that the data principal should provide consent for anonymization and usage of this anonymized data while providing consent for the collection and usage of his/her personal data. This would require data fiduciaries to have a process in place to gather consent and enable the withdrawal of such consent. Facilitating the withdrawal of consent would require re-identification of a data principal within an anonymized dataset. It is unclear how this would work in practice given that the purpose of anonymization is to remove personal identifiers from the data set. Data principals would also be presented with a whole barrage of additional consent requests, leading to consent fatigue. Individuals may also refuse consent to anonymize data at the outset due to an inability to foresee the potential future beneficial uses of such data which may hinder important research activities. Furthermore, if an organization is required to obtain and manage additional consents to anonymize data, many businesses may shy away from engaging in beneficial data uses enabled by anonymization for fear of being in non-compliance with the non-personal data framework or for fear of individuals subsequently withdrawing consent, which may significantly impact research efforts. CIPL recommends that the rules on consent in the framework align with those included in the PDPB and also that anonymization be defined in the framework and the PDPB to reflect the more realistic standard of reasonable anonymization coupled with procedural, legal and administrative safeguards applicable to the organization. The definition should also account for the need to re-identify data in certain circumstances for the benefit of individuals rather than view it solely as a risk to privacy.

4. Mandatory Data Sharing

CIPL believes that any data sharing framework should promote and incentivize voluntary sharing arrangements (and understand their sufficiency and effectiveness for accountable data sharing) over compulsory data sharing schemes. We have recently seen an increase in data sharing between organizations and governments, particularly in the context of the COVID-19 pandemic. For example, Google is currently making available COVID-19 Community Mobility Reports[5] to aid public health authorities globally in making critical decisions to fight the pandemic. Similarly, Vodafone is providing several European governments with heat maps showing how population movements have changed before and after the imposition of containment measures.[6] This data sharing is not mandatory but organizations understand the value to wider society in sharing data. India could begin by promoting government to business data sharing to lead by example and to demonstrate the benefits to India's

economy (and recovery post-COVID) of such sharing. The government should consider, in parallel, the impacts of mandatory data sharing on India's economy and work on an accountable data sharing framework that also considers other company rights. This would mitigate the negative impact that forced data sharing may have on organizations' willingness to do business in India and on intellectual property rights and business proprietary information. Moreover, appropriate guardrails to ensure data cannot be requested by other companies or government bodies in ways that enable misuse must be considered. The independence of the non-personal data authority must also be considered and measures put in place to avoid any abuse of power to obtain data. Furthermore, any new data authority must work closely together with the data protection authority, to be established under the PDPB, and the Competition Commission of India to ensure a consistent regulatory environment.

Finally, the creation of a new category of "Data Business" and the proposal to create a scale to share private data ranging from raw and factual data sharing for no remuneration to remuneration based sharing depending on value-add to the data are highly confusing concepts. CIPL recommends against adopting such an approach and instead focusing on creating an accountable data sharing framework that facilitates the responsible transfer of data across borders, voluntary data sharing mechanisms within India and across borders, and the contractual freedom of parties to enter into data sharing partnerships, subject to any existing legal frameworks on unfair pricing, non-discrimination laws, etc. Of course, there will be instances where mandatory data sharing is necessary in the public interest or for very specific national security purposes. Such narrow scenarios should be considered but should not form the basis of India's entire data sharing ecosystem.

5. Health Data Management Framework

In August 2015, the Prime Minister of India announced the Government's National Digital Health Mission, which is an initiative to digitize the entire healthcare ecosystem of India. Following this, the National Health Authority released the Health Data Management Policy. The Policy sets out a framework for the secure processing of personal and sensitive personal data of individuals who are part of India's digital health ecosystem. This framework introduces yet another set of comprehensive rules that are applicable to the collection and use of data in India.

The non-personal data framework recommends considering the health sector as a pilot use-case for the framework. As with the PDPB, there is a risk that the Health Data Management Framework may overlap and create inconsistency with the non-personal data framework which would lead to further uncertainty for organizations. Any future data sharing framework must ensure that it can work in tandem with other existing data frameworks and specify how conflicts of law are to be resolved, where possible.

II. CONCLUSION

CIPL is grateful for the opportunity to comment on the Ministry of Electronics and Information Technology's Report by the Committee of Experts on a Non-Personal Data Framework. We look forward to further opportunities for dialogue on accountable data sharing or other privacy and data protection matters.

If you would like to discuss any of the comments in this paper or require additional information, please contact Markus Heyder, mheyder@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

References

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] See CIPL Comments on the Indian Ministry of Electronics and Information Technology's Draft Data Protection Bill 2018, 26 September 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_indian_ministry_of_electronics_and_information_technology%E2%80%99s_draft_data_protection_bill_2018.pdf; and CIPL Response to the Indian Joint Parliamentary Committee on the Personal Data Protection Bill 2019, 21 February 2020 available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_indian_joint_parliamentary_committee_on_the_personal_data_protection_bill_2019__21_february_2020_.pdf.

[3] Of course, CIPL recognizes that there may be specific situations related to state and national security activities whereby keeping certain narrow categories of data in India may be justified, but these should be narrowly defined to prevent unjustified barriers to digital trade.

[4] CIPL White Paper on "Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill", August 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-dsci_report_on_enabling_accountable_data_transfers_from_india_to_the_united_states_under_indias_proposed_pdpb__8_september_2020_.pdf.

[5] COVID-19 Community Mobility Reports, Google, available at https://www.google.com/covid19/mobility/.

[6] Reiter, J., "Correct use of telco data can help in this crisis", Vodafone Group, 27 March 2020, available at https://www.vodafone.com/covid19/news/correct-use-of-telco-data-can-help-in-this-crisis.