DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DSCI Feedback |Draft Non-Personal Data Committee Recommendations

Data Security Council of India (DSCI) is pleased to submit before the Non-Personal Data Committee, its submission on the draft recommendations put forth in the report by the Committee of Experts on Non-Personal Data Governance Framework. We appreciate the consultation and review undertaken by the Ministry of Electronics and Information Technology (MeitY). Public consultation is an integral step in continuing the discussion on creation of a framework for Non-Personal data in India. DSCI has conducted industry consultations to assess the likely impact on the Industry of the proposed recommendations and these have informed our assessment of the report.

We would like to commend the exercise undertaken by the committee to study and evaluate the data ecosystem in India. However, certain issues subsist within the framework proposed by the committee, we would urge the committee to revaluate the assertions and recommendations put forth in the report with respect to its interplay with the upcoming Personal Data Protection Law in India and other established regulations with respect to intellectual property rights and competition. The Draft report and recommendations, in our considered assessment, needs a revisit based on the contours of an emerging vibrant data economy, and India's Digital economy growth charter and also to ensure we further reinforce India's global position as a growing digital hub and innovation. With respect to specific recommendations in the report we request clear demarcation of sphere of applicability vis-a-vis the foundational concept of Non-Personal Data. In our submission we have highlighted the key concerns stemming from the above-mentioned factors and share with the committee our recommendations to them. The following are the key areas of concerns:

1. Objective and narrative of the report, w.r.t data utilisation
2. Requiring Individual's consent for Anonymisation and usage of Anonymised data
3. Definition of Non-Personal Data- Public, Private and Community
4. Sensitivity of Non-Personal Data and restrictions on data flows
5. Role of stakeholders- Data Custodians and Non-Personal Data Authority

Our submission is organised in 2 sections as follows:

We hope that our submissions would help the committee in further evaluating the recommendations of the report to create an effective, fair and accountable framework for data sharing in India.

Rama Vedashree

CEO

Data Security Council of India

I. Recommended principles for policy formulation on NPD in India

Context

Digitalization has led to large-scale and sweeping transformations across multiple aspects of businesses and governance alike. Providing unparalleled opportunities for value creation and facilitating data driven policy making. At the heart of this digitalisation is understanding and leveraging data for its innovation potential to service consumers and citizens

Enabling accountable exchange of data between the different stakeholders in the data ecosystem is important for realising the economic potential of democratised data usage and societal benefits that accrue from such equitable usage. The use and re-use of Non-Personal Data (NPD) to achieve the goals must take place in a framework that addresses legitimate commercial, privacy and security concerns. The framework should also take into consideration rapid changes in the marketplace, technologies and consumer and business preferences as well.

The role of the government in this process is to facilitate an ecosystem which enables the realisation of this goal and identification of priority sectors for harnessing economic and societal benefits in consultation with the industry.

Data Sharing Principles

Any framework envisioned to facilitate exchange of NPD should take the following principles into consideration. Each of these foundational principles, comes with a set of imperatives, which have been elaborated through the course of the present submission.

1. **Fairness:** The outcome of data sharing between entities should yield equitable benefits for all the stakeholders involved. Meeting the following **imperatives** would be necessary in achieving this end:
    - Protection of investment and assets
    - Access against compensation
    - Incentivisation of data sharing

2. **Accountability**: Data recipients should be accountable for the data which is received by them. Accountability could come in the form of:
    - The data recipient providing publicly available reports on what has been done with the data, and the results obtained from the use of the data. This will ensure accountability and build overall trust in the data sharing requirements. This will also increase the level of awareness of the value in data sharing.
    - The data recipient ensuring the ethical use of the shared data – e.g. not use the data for discriminatory purposes and eliminate unfair bias in the use of the data.
    - The data recipient needs to comply with data security standards which must be developed together with the industry.
    - Respect rights and IPR associated with data and use it for intended/stated purpose only

3. **Trust:** Trust is at the heart of any data sharing mechanism. A relationship of trust backed by a system of accountability and control, is essential to for equitable data sharing. The trust can be codified through:
    - Reliable and possibly standardised protocols
    - Traceability and clear identification of data sources
    - Impact assessment
    - Guard against disclosure of confidential data

4. **Cooperation:** The framework should be envisioned as a voluntary and collaborative effort between with the industry and the government.
    - Room for Self-regulation and Co-regulation
    - Encourage accountable International data transfers and collaboration

II. Key concerns and recommendations

A. Objectives and narrative

Data Enterprise

i. The Non-Personal Data Protection committee delves into the need and ways of unlocking data for creating economic, social, and public value. It recommends a framework for creating incentives for innovation and encouraging Indian start-ups, proposing a data-sharing framework to drive social, public, and economic good.

ii. To further supplement the committee's discourse, we would like to present our assessment of data utilisation and value creation by digital enterprises (referred to as a 'Data Enterprise'). A Data Enterprise evolves from identification of problem statements and ideas to solve them. While doing so, it deals with various use cases, solved with existing or newly designed algorithms. The data led entrepreneurial activities often rely on the platform to collect information and organize it in the form of data structures. The adoption of this platform by end consumers eventually leads to the formation of the data lake or store. In most cases, the way the platform is deployed plays a vital role in the success of data enterprise design.

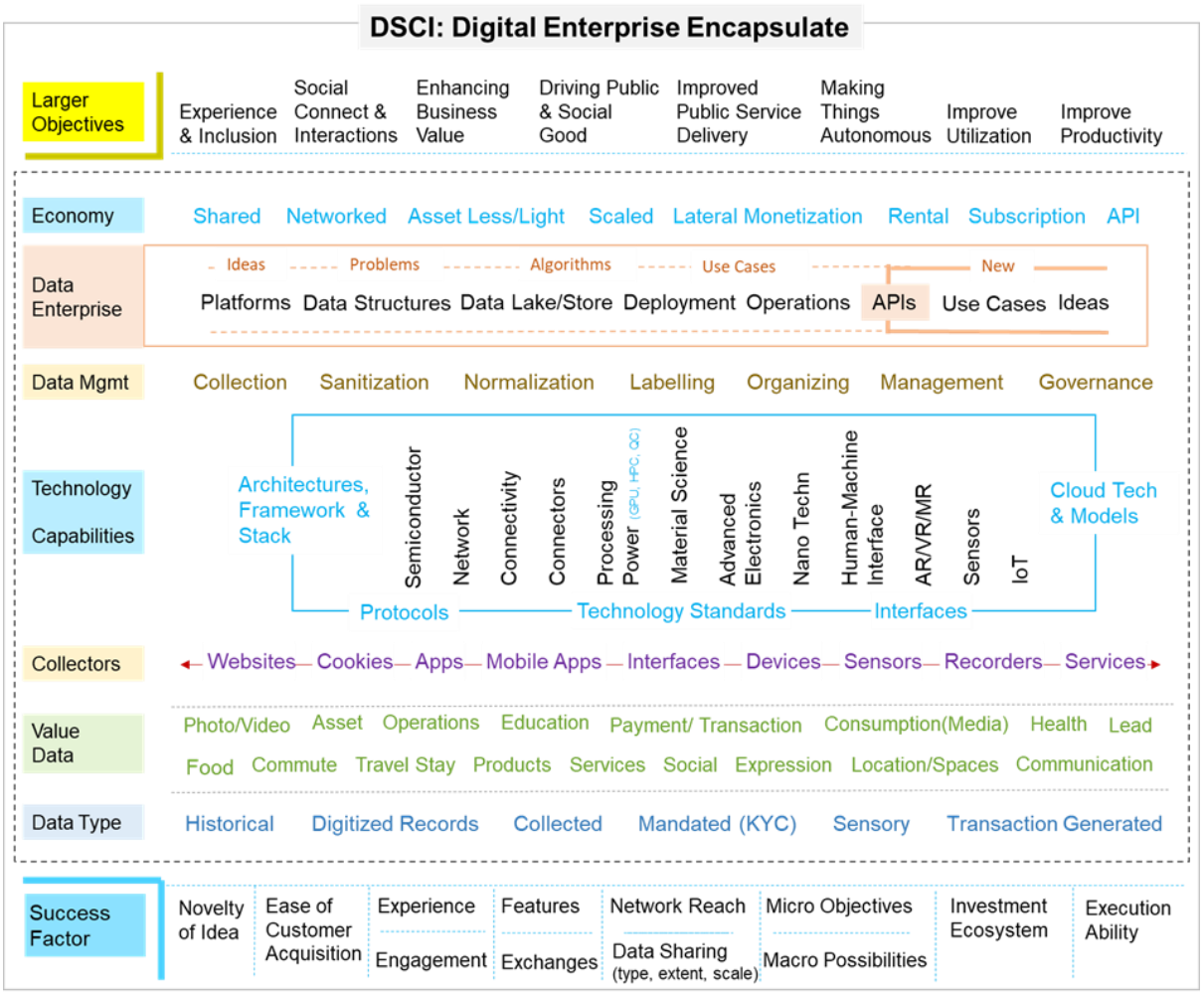

Fig. 1 Anatomy of a Data Enterprise

iii. At the heart of a Data Enterprise is Digitization, which makes economic value creation nimble. It unleashes possibilities for shared use by optimizing the utilization of assets. Due to ubiquitous connectivity and the ability to offer a standard set of services to millions of customers, it provides the impetus to scale up in a short period. It can also work on the principle of lateral monetization by focusing on acquiring and serving customers in the early stage. It finds ways of monetization that is not heavy on the consumer. The services offered are very affordable or sometimes free as the network provides other avenues of monetization. Moreover, these economic drivers heavily rely on rental and subscription, reducing the entry barriers. The data economy thrives on one innovation fuelling others. Increasing reliance on APIs to expand business value creation give testimony to it.

iv. For the success of the data enterprise, the novelty of the idea is an essential factor. However, what matters is the ease of acquiring the customers and the kind of experience it offers to the consumer. The features offered should instigate engagement and exchanges for consumers. The reach of the network plays an important role as well. The type, extent, and scale of data it collects and can share would add to it. The execution ability matters a lot to make the enterprise dynamic, fast-moving, scalable, and innovative. It demands proportionate investment that, too, at the right time.

v. The success of digitization and innovation that it unleashed gives more significant fillip to solve the problems at a broader level. It serves the purpose of including the population that remained isolated from the development processes. It enhances social connections and interactions for the free flow of information, ideas, and opportunities. Apart from driving business value, it drives public and social good. It promises to improve the delivery of public services. It makes things autonomous, removing the scope of inefficiency and discretionary interventions. It improves the utilization of the assets and investments and makes the economic activities productive

vi. Data Security Council of India's encapsulation of data enterprise, as illustrated in Figure 1, provides broader and nuanced contexts to the policy deliberation around data, for both personal and non-personal data.

NPD Committee Paper sees Data in Isolation

vii. DSCI believes that the data collected and generated should not be seen in isolation. The foundation of solid but innovative ideas gives birth to data enterprises. They deploy many creative ways for easy onboarding and acquisition of customers. They come up with new features and provide great experiences to their customers. They set up platforms, beef up the underlying technology stack, and experiment with various deployment strategies. They painstakingly build operations to reach a critical mass and often take significant business and investment risks to become viable The Non-Personal Committee paper, while focusing on data, doesn't take into what leads to the creation of data, which would not only create severe IPR issues but also make the digital business environment significantly uncertain.

viii. Data Security Council of India has attempted to provide the key data definitions considering the objectives furthering innovation, social, and the public good, namely, 'Public Interest Data,' 'Innovation Interest Data,' and 'Competition Interest Data.' The figure below depicts the definition of the data.

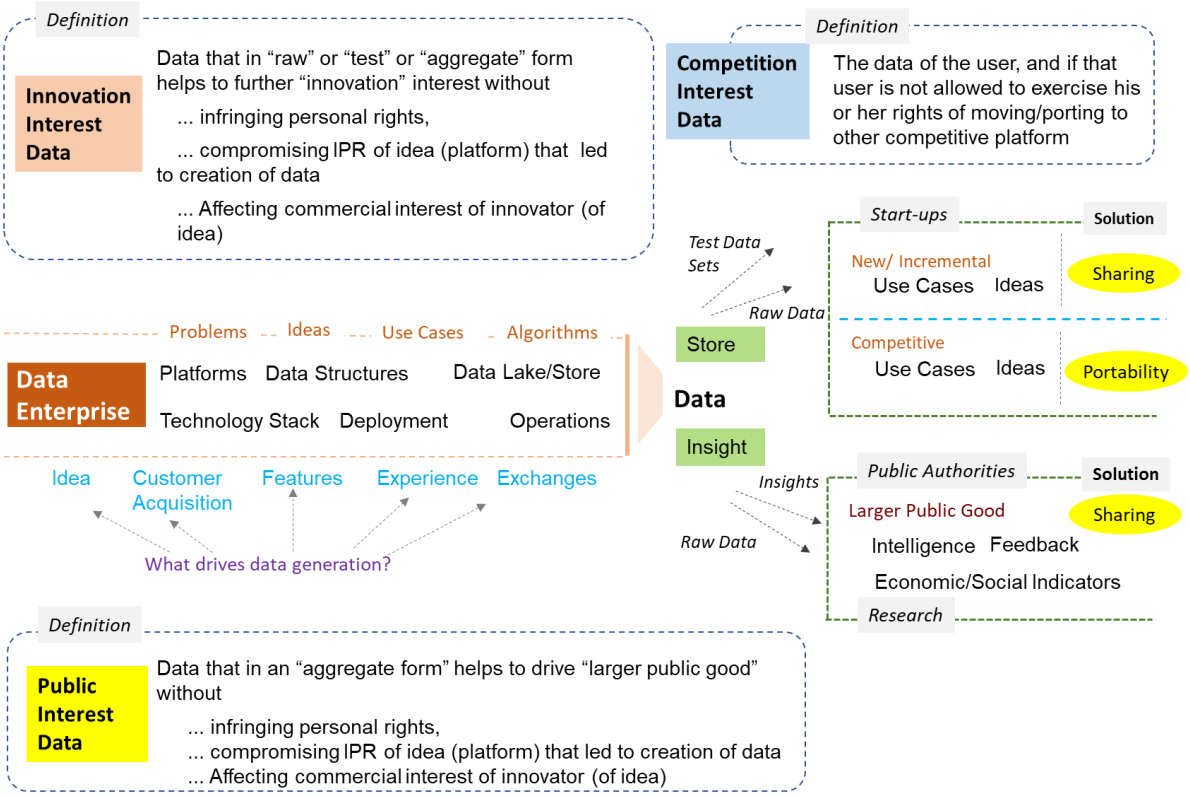

Figure 2. Defining 'Public Interest Data,' 'Innovation Interest Data,' and 'Competition Interest Data.'

ix. DSCI strongly believes that any framework laid down for sharing or governing non-personal data should not: (i) Infringe personal rights (ii) Compromise the IPR of idea or platform that led to the creation of data or (iii) Affect the commercial interest of innovation or the idea.

x. DSCI also recommends factoring these while devising the framework for data sharing. Moreover, it believes sharing shouldn't be a blanket instrument. For example, an original innovator may share data only for incremental innovation, ideally in the form of test data. In some cases, it may share raw data if the situation demands. Sharing of the raw data should be discouraged for innovation purposes as much as possible. The innovator should be allowed to exercise its rights associated with data while taking such decisions.

xi. For the competition interest, portability should be promoted as an instrument. The consumers should be allowed to port their data from one platform to another in an easy way.

xii. For larger public good, sharing of inferences or aggregated intelligence is recommended. In some cases, the raw data may be shared without hampering the original innovator's IPR and commercial interest.

B. Individual's consent for Anonymisation

i. Report recommends that the consent of data principals should be obtained for anonymization and usage of the anonymized data, while obtaining their consent for processing their personal data, and that appropriate standards of anonymisation would be defined to prevent or minimize the risks of re-identification.

ii. This assertion has been attributed to the assumption that personal data that is anonymised should continue to be viewed as non-personal data of the principal, due to an ever-present risk of re-identification of personal data from anonymized data. It's a globally established principle that on

the identifiability spectrum of personal data, anonymisation represents the highest level of de-identification. Justice Srikrishna committee report, echoes this understanding and advocates an approach where the standard of anonymisation considered adequate to guard against risk of re-identification should be prescribed by the Data Protection Authority.[1] It also articulates that while the possibility of identification must be eliminated for a data set to be exempted from the rigours of regulation, '*any absolute standard requiring the elimination of every risk including extremely remote risks of re-identification may be too high a barrier and may have the effect of minimal privacy gains at the cost of greater benefits from the use of such data sets'*.

iii. The Personal Data Protection Bill, 2019 (PDP Bill) subscribes to this view of the committee and lays down that anonymisation has to be an irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility standard set by the Data Protection Authority.[2] PDP bill also prescribes punishments for any attempts to re-identify personal data. Therefore, if the NPD regulations also stipulate standards for anonymization, there is a possibility of conflict / overlap in the event these regulations are not harmonized. This may lead to uncertainty for businesses and increased compliance costs.

iv. The report makes the assertion that additional consent of the principal for anonymisation and use of anonymisation would act as a safeguard against re-identification of personal data. Assuming that anonymised non-personal data referred to in this instance of the report is processed from the underlying personal data collected using consent as a ground of processing under PDP Bill, it's a established principle of data protection that; processing of personal data in order to fully anonymize it is "compatible with the purpose for which the personal data is initially collected" and therefore does not require an additional legal basis, such as consent, specifically for the act of anonymising. This position has been re-affirmed by distinguished long standing data protection regulators such the UK Information Commissioner's Office[3].

Recommendations

i. The requirement to obtain the individual's consent for anonymizing data or using anonymized data should be removed. Organizations should be permitted to anonymize data without the need for obtaining consent of the individual. A consent obligation would also mean that consent can be withdrawn. However, in order to give effect to this ability to withdraw consent, it would require the re-identification of the individual in the anonymized dataset. Doing so would defeat the whole purpose of the anonymization in the first place.
ii. Privacy safeguards and anonymisation standards should flow through the Personal Data Protection Bill, 2019 and the procedure laid therein.
iii. Irrespective of the de-identification method used, we encourage the practice of informing data principal's that their data will be de-identified and may be processed for additional purposes. This would help the principal make an informed decision.

C. Definition of Non-Personal Data

Definitions

i. The Committee recognises that NPD can be defined in multiple ways. Therefore, it has adopted the approach of defining categories of NPD - (i) public, (ii) private, and (iii) community NPD. But due to nature of their definition these categories could have significant overlaps in practice.

[1] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Page 30.
[2] *Ibid.*
[3] Anonymisation: Code of practice, Ico.org.uk. Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf (last accessed: 11 September 2020).

ii. NPD collected or generated by the government / agency of the government will amount to public NPD as per the Report with the exception of data that is explicitly treated as confidential under any law. However, confidentiality obligations in the commercial context are largely driven by contractual obligations. Without a clarification that information that is contractually confidential is an exception to public NPD, any information provided to any government department or agency in the course of collaboration with the government by a private entity or individual is also at risk of being categorized as public NPD. Several Public sector entities are also independent commercial enterprises.

iii. The Report defines private NPD to mean NPD collected or produced by persons or entities other than the governments, the source or subject of which relates to assets and processes that are privately-owned by such persons or entities, and includes those aspects of derived and observed data that result from private effort, insights involving application of algorithms or proprietary knowledge, and data included in a global dataset and which is collected in foreign jurisdictions. This would mean that all Indian data custodians, including those collecting NPD of foreign individuals, and all foreign data custodians collecting NPD of Indians would be subject to these regulations.

iv. Therefore, the presence of Indian NPD in a dataset will invoke applicability of the NPD regulations, even for datasets created by foreign entities which largely contain NPD of foreign individuals. This would also act as a strong deterrent for several service providers that operate at a global level, or even smaller players from offering their services to customers/ users based in India, since even any incidental collection of NPD of users in India is likely to subject the entire dataset(s) of such organisations to the proposed requirements and obligations.

v. The Report further defines a community as any group of people that are bound by a common interest / purpose, and involved in social and/or economic interactions such as a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community. It goes on to define community NPD as NPD about inanimate and animate things or phenomena – whether natural, social or artefactual, whose source or subject pertains to a community of natural persons. It excludes private NPD and qualifies that only raw/factual data without processing or derived insights is considered community NPD. However, the examples of community NPD presented in the Report include datasets collected by the municipal corporations and public electric utilities which should have been considered as public NPD. The examples also include information collected by private players such as ride-hailing companies. While the Report qualifies that in such cases, the raw/factual data without processing /derived insights will be characterized as community data, it would still be considered as private NPD going by the definition in the Report. Thus, there is considerable ambiguity and potential for overlap in the categorization of community data.

vi. Further, just as there can be an infinite number of NPD data sets, there can be an even greater number of communities since each data set could result in interest from multiple communities. However, it may not be necessary and also practically not possible to give rights to all such communities. There can also be several subsets of communities, within any given 'community' as defined. Without identifying a community, it would not be possible to identify the rights that such communities should exercise as not all communities can be equal or enjoy equal rights. The obvious overlaps amongst different 'communities', would invariably lead to disputes over the manner in which NPD of those communities are to be handled. Moreover, this would also lead to contesting claims from different bodies/ organisations over the right to be the 'data trustee' of any given community.

vii. The lack of clear guidelines with respect to the definition can lead to undue interference with established business practices and create uncertainty since there is no practical definition for any business to implement. Notably the idea of regulating community data was introduced into mainstream discourse on data regulation by the Committee headed by Justice B.N. Srikrishna. However, even this reference was in the limited context of potential collective privacy harms.

Recommendations

i. Any framework for governance of NPD should provide sufficient and clear guidelines for data classification that would enable businesses to implement the classification. Given the complexity involving community data, it is advisable to remove the concept from any policy regarding NPD. As and when required, specific communities can be identified based on policy objectives and the government and the relevant sectoral regulators can still seek appropriate NPD as required by such policy.

ii. Foreign data sets should be excluded from the NPD framework since the object of the framework is to unlock the value of data related to India. It also needs to be clarified that information that is treated as confidential contractually is a valid exception to public NPD.

D. Sensitivity of Non-Personal Data and restrictions on data flows

i. The Committee has recommended that NPD should inherit the sensitivity characteristic of the underlying personal data from which it is derived. Accordingly, there would be 3 categories of NPD - (i) general NPD, (ii) sensitive NPD and (iii) critical NPD, derived from personal data, sensitive personal data and critical personal data respectively.

ii. The Report provides that general NPD may be stored and processed globally, however; Sensitive NPD can be transferred overseas but must be stored in India. Critical NPD can only be stored and processed in India. It further states that NPD may be sensitive based on (i) national security or strategic interests such as vital infrastructure; (ii) business sensitivity or confidentiality; or (iii) risk of collective harm. The Report envisages that the NPD regulation will continue to apply to the regulation of community NPD and public NPD transferred overseas. Businesses that transfer community NPD or public NPD overseas will be responsible for complying with data sharing requirements.

iii. The scope of sensitivity of NPD under the Report is very broad. It could depend on dynamic factors such as national / security or strategic interest and risk of collective harm, which leads to uncertainty around the classification and treatment of such data. The inheritance of sensitivity from personal data could also involve a large compliance burden since the current draft of the PDP Bill envisages that the government has the ability to expand the scope of sensitive and critical personal data. Further, given that NPD implies that it is already no longer relatable to the data subject, there is inherently neither a need to categorise such data as ‘sensitive’ or ‘critical NPD nor to regulate them as such.

iv. This would also lead to several ambiguities regarding the treatment of any given data set, given that any data set is bound to include several data points. For instance, given that the sexual orientation of a data subject is considered ‘sensitive personal data’ under the PDP Bill, any dataset on purchases made by users for a given product, which includes gender/ sexual orientation of the individual as one of the data points, would likely, unduly subject the entire dataset as ‘sensitive NPD’.

Recommendations

i. Localization requirements should not be included in the NPD framework. The Committee should clarify whether there are other objectives to defining NPD as sensitive or critical and consider removing the concept from the NPD framework entirely.

E. Data Businesses & Mandatory Data Sharing of Proprietary Data

i. The Report introduces the concept of "Data Businesses", i.e., organizations that are collecting, storing, processing, or otherwise managing data and meet thresholds of data specified by NPDA from time to time. Data Businesses would be required to submit meta-data about the data user and community from which data is collected, with details such as classification, closest schema, volume, etc. based on a directory of data classification and schema published by the NPDA. Indian citizens and organizations may access such metadata. Subsequently, they may request for underlying data for the following - sovereign purposes such as national security, legal purpose, core public interest such as research and innovation, better delivery of public services or economic purposes such as encouraging competition.

ii. However, the Report does not provide details of how the sharing mechanism would work and has left it to the NPDA to certify rules and technology framework for data sharing. While the Report considers certain checks and balances to sharing, they seem to be largely from the perspective of data safety and do not consider the rights of the Data Businesses.

iii. In contrast, the Open Data License (ODL) issued pursuant to the NDSAP considers several protective measures such as rightful attribution, disclaimer of warranty for errors and omissions etc., and if the conditions are violated, the license to open data would terminate. The ODL also excludes inter alia data that is subject to intellectual property rights and sensitive data (as defined under law). The Report does not consider any such protective measures.

iv. Compulsory sharing of NPD without taking sufficient safeguards to protect Data Businesses from the liability arising out of such sharing is problematic. The Report also does not touch upon such accountability principles that are necessary pursuant to data sharing, which may further disincentivise companies from investing or carrying out business in India. Bad actors can deploy methods to re-identify individuals and breach privacy and use it for irresponsible activities without accountability.

v. The Report provides that when there is a value addition to data, private companies can charge for the NPD that it shares depending on the level of the value addition. For non-trivial value additions, NPD sharing may be mandated but subject to fair, reasonable and non-discriminatory (FRAND) based remuneration, for an increased value addition the charges will be determined by market forces, and for "high value add" NPD, the private companies will have full discretion. While the Committee recommends affixing costs proportionate to the value addition, there is a lack of clarity on what would constitute "non-trivial", "increased" and "high" value additions.

vi. Further, sharing of data by businesses may possibly erode the value of such data. It will have adverse business and cost consequences to established businesses operating in India. Mandating open access to data ignores the significant cost incurred by businesses to collect such large amounts of data. Furthermore, the powers of NPDA to mandate data sharing can be misused in ways to undermine confidentiality and integrity of NPD.

vii. Mandating compulsory sharing of NPD for private organisations, is in fact creating compulsory licensing provisions for copyright through a new legislation. India already has a comprehensive Copyright Act, 1957. A new legislation for this subject matter is therefore not required. Also, any incremental laws on compulsory licensing etc, should be continued to be covered under Copyright Act, 1957.

Recommendations

i. Private NPD should not be brought within the ambit of mandatory sharing. Self-regulation by industry/ voluntary sharing is a much more appropriate mechanism when it comes to NPD owned by private businesses. A proposal on this front is to incentivise data portability so that data

subjects/principals are in complete control of their data and can take it out of an entity / transfer from one entity for use in different use cases, thereby meeting/ supporting the needs of start-ups etc. The Account Aggregator framework, for e.g., is a regulation that enables entrepreneurs and users to leverage existing data to help create new datasets.

ii. Over the years, private companies, organisations and institutions have voluntarily shared large volumes of data sets available for processing and use by the public without any intervention or compulsion from the state to disclose them to maximize their potential benefit for the public. These organizations have internal checks and balances to determine the sensitivity of datasets owned by them and to ensure that their own proprietary interests are not compromised when making decisions on sharing. It is not possible for governments to replicate these checks without accessing proprietary information and tools belonging to these organizations which they may not wish to share.

iii. The government can instead consider incentivizing the sharing of NPD sets by private parties by various policies and programs. The NPD law must also provide detailed guidelines for framing data sharing requests to ensure that these are reasoned and specific, and do not impose onerous obligations on private companies to routinely transfer large quantities of NPD. There is also a need to protect and shield the Data businesses against any liability that may arise as a consequence of sharing of NPD beyond the indemnification against vulnerabilities that the Report contemplates for adhering to standards.

F. Roles and stakeholders in the NPD Ecosystem

NPD Authority

i. The Committee has proposed setting up a new NPD Authority (NPDA) to administer the provisions of the proposed NPD law. This appears to be based on the Committee's belief that (i) the regulatory authority would need specialised knowledge and the ability to keep pace with evolving technologies, (ii) the nature of tasks and focus of the authority would be different from existing regulators. Yet, the Report does not clarify how the NPDA would be better equipped to deal with these tasks as opposed to an existing regulator. It only says that the NPDA will have some members with "relevant industry experience". NPD is an umbrella set of data that can comprise of data from any number of industries. Not all of them can find representation in the constitution of the NPDA, and the Report provides no guidance regarding which industry would be the relevant industry or what experience would be considered as relevant experience. Hence, it is unclear how the NPDA would have any advantage over existing sectoral regulators in respect of keeping pace with technology.

ii. Most sectoral regulators are best placed to assess the best interests of each sector, be it economic, social or security related interests. They are qualified to understand the problems and the practical difficulties in each sector. In respect of the tasks and focus of the NPDA, while the Committee envisages that the NPDA will have an enabling role in addition to an enforcing role, i.e. enabling data sharing requests, proactively addressing market failures such as information asymmetry, enabling competition and level playing field etc., these tasks can also be performed by relevant sectoral authorities.

iii. Further, under the Competition Act it is the duty of CCI to eliminate anti-competitive practices and promote competition and addressing monopolistic or exploitative practices resulting from lack of access to NPD is a subset duty, though the CCI may not be able to follow a proactive approach in this regard, currently. However, the CCI has a wealth of experience in dealing with anti-competitive practices and if the CCI were to perform the role of proactively identifying market harms, this experience could be put to use more effectively than, if this role is performed by a new regulator.

iv. Moreover, the NPD that is the subject of regulation may already be regulated by existing sectoral regulators that have been introduced keeping in mind the specific requirements of each sector such as the Reserve Bank of India, the Department of Telecommunications (DoT) and TRAI, Ministry of Defence (MoD), the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority of India etc. Similarly, e-commerce data is proposed to be regulated by an e-commerce regulator under the Draft E-commerce Policy being developed by the Department for Promotion of Industry and Internal Trade. Currently the technology sector may witness over regulation with at least four regulators Data Protection Authority (DPA), the E-Commerce Regulator, and the Central Consumer Protection Authority and now the proposed Non-Personal Data Authority (NPDA). Overregulation undermines innovation and leads to conflict especially in cases of overlap of issues and jurisdiction.

Example - the DPA under Section 50 of the PDP Bill is expected to regulate non-personal data, which is similar to the role of NPDA. The role of CCI is to address market failures and its role can be strengthened to address antitrust conduct in this sector. Therefore, the role of NPDA is mere duplication of the scope of work of these existing/proposed regulators. Creation of another regulator will not only lead to overregulation but also confusion thereby delaying the process for the companies who are looking to use the anonymised data.

v. The Committee has maintained that the sectoral regulators may make additional regulations in a horizontal fashion. This can result in over regulation and conflicts and the Report does not address how to resolve such issues. Also, the report does not address situations wherein there is an overlap between DPA and NPDA or for that reason specific sectoral regulators, which may lead to conflict.

Data Custodians

vi. The Report introduces the concept of a data custodian, whose role is similar to that of data fiduciary under the PDP Bill. It is imperative that such categorisation should not include data processors as defined under the PDP Bill. In most instances, data processors process data (personal data and NPD) based on contractual arrangements with their clients (data fiduciaries/ data collectors) who provide access to such data for limited purposes defined therein. Data processors are contractually restricted from accessing or processing the data for purposes beyond the scope of such arrangements.

vii. The report states that the Data custodians must collect, store, process and use NPD in the best interest of the data principal. Data custodians have a duty of care, in respect of community NPD, to the concerned community. Such duty of care will be specified in the proposed NPD law and will include anonymisation requirements, protocols for data sharing etc.

viii. The Report provides that 'duty of care' must be operationalised through the best interest standard in order to prevent harms to communities and individuals from processing NPD. Businesses may make data sharing requests to the data custodian. If the data custodian refuses to share the data, the request can be made to the NPDA and if the NPDA determines that the request is genuine and beneficial it can require the data custodian to share the raw/factual data. Equating the obligations of a data fiduciary under the PDP Bill which relates to protection of personally identifiable data to that of obligations of entities that process NPD is not justified since the nature of data being processed is different. Further, the standard for ensuring the "best interest" of the data principal is presently unclear, and the Committee has recommended that this be detailed in the NPD regulation.

ix. The best interest standard in administrative law or trust law requires acting in a manner to benefit the person concerned, and not just ensuring that no negative impact is felt by the principal. While this may work for personal data protection, it may not work in the context of NPD where the context is to unlock the value.

Recommendations

i. From an implementation point of view and in order to maximise efficiency to achieve the objectives outlined by the Committee, it is recommended to follow a sectoral approach instead of setting up a separate NPDA. Depending on the need for regulating NPD in a particular sector, the existing sectoral regulators, if any, or the relevant government department or ministry can issue appropriate rules and regulations.

ii. Data custodians should not be treated on the same footing as data fiduciaries. They should not be imposed with an obligation to act in the "best interest" of the data principal. Especially in the case of community NPD where there could be multiple communities involved, posing a fiduciary obligation on data custodians would unfairly burden them.

iii. The concept of Data Custodians should not include the data processing industry in India, that processes vast amounts of data under contractual obligations, especially with respect to foreign citizens data. Given that such data does not relate to Indian citizens, or communities within India, the industry is concerned that mandatory storage or sharing of such data within India could lend Indian data processors in breach of statutory obligations in other jurisdictions, as well as their contractual obligations with their clients.