REPLY TO THE

Data Empowerment and Protection Architecture – DRAFT FOR DISCUSSION

Submitted by

The Digital Future

November 29, 2020

Drafted by

Parvathi Bakshi, Divyanshu Dembi, Ieshan Misri, Arushi Mishra, Sharmita Sawant, Ashutosh Chandra, Pratyush Gupta, Himeesha Dhiliwal, Srika Agarwal, Jasleen Virk and Advait Shah.

TABLE OF CONTENT

ABOUT THE DIGITAL FUTURE

The Digital Future is an online platform for research and education on disruptive technology and its consequences. We undertake research and development of concepts such as artificial intelligence, blockchain and cryptocurrency. We also look at the growing field of technology regulatory framework such as cybersecurity and data protection.

The Digital Future has over 50 researchers working on various projects from producing informative, educative and thought-provoking articles to drafting primers on cybersecurity framework within India.

Contact Us:

Website: https://thedigitalfuture.in/
LinkedIn: https://www.linkedin.com/company/the-digital-future/?viewAsMember=true
Email: thedigitalfuture.blog@gmail.com
Instagram: https://www.instagram.com/the_digitalfuture/

Research Team for Draft DEPA Consultation

Parvathi Bakshi - Lawyer & Founder of The Digital Future
Advait Shah – LL.B. 2020-2023 | Jindal Global Law School
Arushi Mishra – B.A., LL.B 2016-2021 | Jindal Global Law School
Ashutosh Chandra – BBA., LL.B 2019-2024 | Jindal Global Law School
Divyanshu Dembi – LL.B. 2020-2023 | Jindal Global Law School
Himeesha Dhiliwal – BBA., LL.B 2018-2023 | Jindal Global Law School
Ieshan Misri – MAPP 2020 | Jindal School of Government and Public Policy
Jasleen Virk – LL.B. 2019-2022 | Jindal Global Law School
Pratyush Gupta – B.A.,LL.B. 2017-2022 | Jindal Global Law School
Sharmita Sawant – B.A., LL.B 2016-202 | Jindal Global Law School
Srika Agarwal – B.A., LL.B 2017-2022 | Jindal Global Law School

INTRODUCTION

The Data Empowerment and Protection Architecture framework ("DEPA") envisages a digitized financial ecosystem wherein individuals are empowered through regulatory, institutional and technology frameworks – to control their own data. This paradigm shift is premised on certain basic principles such as evolvable frameworks, privacy, open networks and citizen empowerment. Some of the key proposals we have identified in the Draft for Discussion ("Draft") includes introduction of (a) new consent institutions – Account Aggregator; (b) new governance institutions Sahamati; and (c) deploying new technology standards – ORGANS, Open Networks. Through these proposals amongst the others in the Draft, the DEPA framework intends to combine the public digital infrastructure along with private digital infrastructure in a manner that will benefit the various players in the ecosystem, especially the individual.

As such we have divided our comments into the following:

(a) Guiding Principles
(b) Executive Summary
(c) Chapter 3 – Introducing India's DEPA
(d) Chapter 4 – Building DEPA for the Financial Structure
(e) Chapter 5 – An Opportunity for the Ecosystem to Co-Create
(f) Comparison with International Policies

Before beginning the chapter-wise approach to our comments, we have summarized our guiding principles ("Guiding Principles") which may also be considered as our recommendations in addition to the guiding principles on pg. 11 of the Draft.

GUIDING PRINCIPLES

The guiding principles of DEPA[1] are a set of principles to guide the choices made regarding the design architecture of the DEPA framework. Read with other chapters within the executive summary, it can be inferred that many other relevant principles have been touched upon but not further developed. We have endeavoured to highlight certain guiding principles which go beyond the design of DEPA and also attempt to address other broader issues in the systemic changes proposed. Our Guiding Principles to drive the shift in the current system are quite simple:

The 3 As: Accessibility, Availability & Affordability

Financial products can enable increased prosperity however India has struggled to access affordable financial products[2]. This vast interconnectedness of all potential objects to each other, the efficiencies it entails, and the jobs that the creation of this infrastructure would bring, is but one part of the phenomenon that we call net connectedness[3]. In addition to the 4th guiding principle of DEPA[4], we recommend taking into consideration the availability factor. Taking the analogy of a pipe that connects all devices some of the following questions arise:

- Does an individual need the content that can be delivered through this pipe?
- Does she have the ability to utilise the content delivered?
- Does she have the ability to interact over the pipe?
- And the ability to pay for the content being received?
    - The cost of the device and
    - The cost of connecting the device.[5]

As financial exclusion is not only an existing reality but also a potential future reality, wherein more individuals may be excluded due to lack of the three As, cognizance of such questions are crucial to keep in mind while further developing DEPA. These questions which guide the

[1] Introducing India's Data Empowerment and Protection Architecture, Chapter 3, DEPA Book, pg. 30
[2] Financial Exclusion, DEPA Book, pg. 7
[3] Aloke Thakore, *Digital inclusion: Definitions and status in India*, Centre for Communication and Development Studies, (June 13, 2015) https://digitalequality.in/digital-inclusion-definitions-and-status-in-india/
[4] *Supra* note 1
[5] *Ibid*

mind through a virtual simulation of mass deployment will also highlight potential pockets of resistance from various lobbies.

Continuum

An underlying principle of the DEPA framework is that it will continue to remain an evolvable framework. In addition to continuous evolution, implementors should inspire to use technology in a manner that (a) doesn't result in further financial exclusion and (b) reduces chances of attrition. How can the proposed framework not only attract various stakeholders into the ecosystem but also continue to maintain the ecosystem at the grassroots level.

Empowering the Individual

To focus on empowering individual users of this platform on how to identify what is in their own best interest. Continuously ask the questions as to whether the technology is able to better inform an individual about the available services, quality and cost of services as well as their rights?

Information Asymmetry

To build a framework which reduces and better yet, negates the effect of information asymmetry. Identify those gaps in regulatory, institutional and technological architecture which results in information asymmetry. Digital India by means of digital inclusion aims to *"transform India into a digitally empowered society and knowledge economy"*[6] which is heavily enabled by technology – the chances of exclusion, due to lack of access and knowledge to digital platforms, are significantly higher[7]. Tackling information asymmetry will also create a "trickle-up" effect starting at the grass roots level.

Quality

Focus on not just empowering but also enabling other stakeholders within the ecosystem such as HIUs and HIPs to also improve their service outcomes. A shift to better quality is generally

[6] https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf
[7] https://digitalequality.in/digital-inclusion-definitions-and-status-in-india/ - look at the trai reports – see if there is something more recent.

resisted by incumbents, therefore incentivising service providers to not only join the ecosystem but also how to elevate their existing performance with the new technology proposed.

Pull over Push

The tendency of governments and policy makers has generally been to adopt frameworks and push them onto the population. While the intent of the policy and framework itself is good and meant to benefit the very population for which it was enacted, push tactics are often met with resistance by various lobbies. We recommend taking a *pull-based* approach which works on the behaviour of the population. The '*Nudge Theory*'[8] of behavioural economics provides tactics which policy makers and governments should adopt to nudge the behaviour of a population towards accepting policies while simultaneous building trust.

Technology

To use technology which is accessible by the economically disadvantaged such that a virtuous set of changes is brought about. To set down clear cut rules and guidelines for platform access, rules as to ownership of platforms, control of platform and engagement within the platform. This will also play an important role in assigning accountability.

Transparency

To ensure transparency in not just governance framework but also in the institutional and technology frameworks. This includes ensuring a system of performance reviews and feedback to track the progress and viability of the various aspects of DEPA following full scale deployment. Also to have clear cut and accessible policies for the various layers of the DEPA framework. Transparency is a key step towards maintaining accountability, especially in a project of such scale where multiple institutions will potentially have overlapping jurisdiction. Further in the absence of a law on data protection as the Personal Data Protection Bill is yet to be passed and the Non-Personal Data Governance Framework is still in its nascent stage, transparency and accountability are key underlying principles.

[8] https://www.behavioraleconomics.com/resources/mini-encyclopedia-of-be/nudge/

EXECUTIVE SUMMARY

A. DATA SILOS

Data aggregation and centralisation is the key to financial inclusion in face of competitive interests of private players.

> *"Despite increasing digitisation and the tremendous value data could have for individuals to build trust with institutions, personal data (and particularly financial data) continues to remain in silos today" - DEPA.*

The argument being made is that there are too many isolated data silos with different private players that they keep isolated for their own benefit and that the data is stored in different formats which hampers effective usage of *all* the data simultaneously.

Shift to Decentralisation

DEPA will create new data silos by itself, in addition to the ones already existing with all the private players (banks, small finance institutions etc). So that will increase the number of private players vying for the individual's data. Moreover if the argument made for a centralised data silo is built on the premise that private players use various techniques to lock in data principals - how then will the data silos created by DEPA based entities which are also controlled by private players not suffer from the same issues, and be different? If the issue is with various data encryption or storing standards - a new centralised DEPA data silo only makes sense if we standardise the data collection and storage protocol in a way that either all other data silos become redundant or the DEPA seeded data silo is the most important and most easily accessible node. How does the framework envision to be central to all financial data operations and services? Making a central data silo that is linked to all other data silos also amplifies the vulnerability of such infrastructure, for a breach into such data would essentially mean being given access to a key of sorts to unlock all other data about an individual(s). ***Therefore the framework needs to adopt a de-centralised approach with very strong encryption standards.***

B. RISK OF INACTION

"Unless an evolvable, interoperable, and secure data sharing framework is implemented, newly generated data on Indians will at best remain in silos without benefiting individuals who urgently require it to access better services, and at worst be misused without individuals' knowledge and consent" - DEPA.

One central aspect of this section is about using machine learning models and algorithms for financial inclusion of people. There is extensive evidence that such machine models don't produce a highly accurate output - in this case creditworthiness ratings, due to the biases that consciously or unconsciously creep into the algorithms.

Credit Scoring Model: 2 scenarios

The main idea in the credit model is that an individual's financial history will be used to determine their credit worthiness. Therefore we must ask:

(a) Whether the individuals who opt into the DEPA framework will have all of their financial history automatically traced and analysed much like the Chinese social credit system (which has been proved to be exclusionary on multiple counts); or
(b) Will the financial services providers have to ask for the individual's consent for accessing their information at each instance of use.

If the latter is indeed the way forward - then determining in detail the metrics of such calculation, the measures the machine learning model would adopt and so on, are points that must play into the development of a credit scoring system.

Financial privacy is also privacy

Point (a) is a nightmare for individuals as it is akin to losing all control over their digital self (which many argue is not any different from your real self[9]) and having no privacy. The latter

[9] Anja Kovacks & Nayantara Ranganathan, *Data Sovereignty of whom?*, Data Governance Network policy brief - 3 (Nov. 20, 2020, 20:00), https://datagovernance.org/files/research/1605850788.pdf.

model is a better way in so far as individuals, with their consent, will share their data with the financial service providers.

Algorithms & Machine Learning

- On the question of the algorithms and machine learning models that will process this data to produce credit worthiness. Whether all financial history data will be automatically processed by these algorithms to keep updating the individual's credit worthiness, or will separate chunks of data be processed to produce credit worthiness every single time - has not been clarified.
- What standards will these machine learning models operate and what data sharing and data collection protocol they will use is also of utmost importance as it will affect actual real-world decisions of lending.
- Questions to be answered:
    - Who will store all this financial data?
    - Under what encryption standards will the data be secured?
    - Who will have access to such data?
    - Can the individual stop such data collection and still access the facilities?

Recommendation

These are all pertinent questions because in either scenario (a) or (b), the individual doesn't have any effective control or property rights over the data - the individual cannot either stop such data collection nor modify it if he wants to access the facilities of the DEPA framework. With reference to companies like Vanguard and Wealthfront (leaders in robo-advisory) they take a highly detailed and customised approach to each customer. We must understand therefore that within the objective credit scoring paradigm, there must be a subjective portion which will accommodate the individual's unique identity and provide them with tools for financial inclusion rather than excluding them because they failed to qualify under a generic credit scoring system.

Question: *Who* owns our data?

".....or to contribute data to research and better-designed machine learning models that benefits them" - DEPA.

Who owns our personal data? Who owns the data that we generate due to our activity on online platforms and services? Can we lay claim to such data as personal property?

- The idea of data as property is directly in question here. All the machine learning models and algorithms essentially *learn* from the data that is fed to them.
- The data that is used to train these models is the data generated by normal people like us. In this case - if my data is my property (which is the framework that DEPA operates within) then I should also be *paid* to give my data for the betterment of such models[10].
- It is essential to understand that without our personal data such models cannot work at all. If data is a resource and if this data that is being used is an individuals' personal data, then by that logic the individual themself should be compensated for it, and not in terms of the service because the framework isn't built on a quid pro quo principally. The DEPA document specifically says that, "a data fiduciary cannot make provision of goods or services or performance of a contract conditional on consent".

Bias in algorithms & machine learning models

The fact, that algorithms and machine learning models are not objective[11] and suffer from the same biases as humans, has been widely accepted worldwide by now. The challenge then is to imagine and employ such models that will minimise the risk of any bias seeping into them and also maximise accurate and welfare-based results for the individuals seeking this facility under DEPA.

[10] Livia Gershon, We All Work for Facebook, (Nov. 6, 2020, 6:40), https://longreads.com/2019/04/26/we-all-work-for-facebook/amp/.
[11] Robyn Caplan et al., Algorithmic Accountability: A primer 14-17 (2018).

Financial Exclusion

If these models suffer from any kind of bias (as most or arguably all of machine learning models do) - it will prove to be a fatal exclusionary process due to any unfair or incorrect assessment of the credit worthiness of that individual - ultimately resulting in denial of the microcredit facility to them.

Corrupted assessments

Machine learning models essentially build upon themselves (without any human intervention) and use prior data to produce future calculations. In such a context that we've just laid out - such vulnerabilities and wrongly done assessments will keep adding up and amplifying. For the unlucky individual whose credit rating was, say, calculated unfairly or erroneously - it means that their creditworthiness will keep declining as the models look at previous denial of services as a sign of low creditworthiness. Future requests of credit will use this information to further deny credit to this individual due to his low credit-worthiness - all in all circling into a nightmare for the individual with no sign of escape.

Recommendations

It is important to note that what this essentially means is that a few bad financial decisions can have a huge impact on an individual's loan taking capacity. And it is often those very individuals who by making bad financial decisions end up in an adverse situation that need such loans the most. This is not to say that we should go back to predatory loan sharks, but to encourage stricter and better standards of technology implementation by:

- Giving the data principals *more control* over when and how their financial data is collected and who collects it.
- Algorithms be first audited by independent and appropriate auditing agencies specialising in algorithmic ethics, bias etc. for lack of any kind of bias or error.
- The idea of digital footprints (financial history) be limited to the least possible data required to operate under the DEPA framework as according to Puttaswamy judgement[12] ("Puttaswamy").

[12] Justice K.S Puttaswamy v. Union of India, AIR 2017 SC 4161

C. A GLOBAL CHALLENGE

"Other countries have responded to these challenges by implementing efforts to improve data protection and consent-based sharing (such as Open Banking in the UK or General Data Protection Regulation (GDPR) in the EU), which India can learn from. However, these approaches have not addressed the issue in a manner that is fully relevant to India's scale and diversity, and to our objectives around accelerating financial inclusion, economic growth, and data democracy" - DEPA

- What is essentially meant by this statement? Does it mean that the data privacy models developed in western countries aren't to be implemented in India and there is a different way to go about the privacy issues?
- The document notes that the incentives of private companies (who want to maximise data collection while minimising the data principal's control over their data) are opposite to the incentives of the data principal (to maximise privacy and autonomy over their data).
- How will DEPA ensure that the incentives of the market forces and the individual are aligned? Especially because the India stack model is a platform for private players to use and do business on.
- In such a scenario, not just with respect to just the consent aggregators but also to all other private entities that will participate under the DEPA infrastructure - how will DEPA ensure that the incentives always stay aligned?

Building trust with institutions

A central idea of the DEPA document is to build trust between individuals and small businesses and the money lending corporations. However it is essential to unpack that there is essentially no trust building happening through the DEPA infrastructure which is data centric not identity centric. Usually lending, as a function of trust in physical sense is about the specific individual and NOT their monetary capabilities. So by that logic the idea of building trust by DEPA is illusionary because there is no human contact and the trust, if any, is between the data of an individual and the data processing machine models. And as we know, algorithms don't deal in emotions.

CHAPTER 3 - INTRODUCING INDIA'S DATA EMPOWERMENT AND PROTECTION ARCHITECTURE

A. LEGAL & REGULATORY FRAMEWORK

One of the main lenses the DEPA document uses to argue for greater personal data collection (mostly financial for now but subject to be expanded to all areas of service[13]) is to label such collection of data as 'empowering'. The idea of empowerment is linked to the idea of greater accessibility of financial services in the market i.e. microcredit and instant small loans. However the idea of empowerment is used to dilute the idea of data privacy time and again by suggesting that the ONLY way forward is to use data as a resource and give up control over it. That posturing is wrong. The generation of data in increasing volumes is neither inevitable nor natural, and that its commercialisation is not necessarily desirable, is, thus, overlooked[14] in most policies.

Property rights-based framework for personal data

When you have a right to something, it is not an abstract thing. It means that you have the faculties to be able to enforce those rights as well because without that - you don't have a right, you only have the illusion of it.

What does it mean to have a property right over something?

1. You have exclusive ownership rights to it;
2. No other person or association of people can use it without your permission;
3. No others can derive any benefit without your permission;
4. You can transfer the property when YOU want; and
5. You will be compensated for the property and you should not be forced to give it up.

[13] Ispirit, India Stack: Towards a presence-less, paperless, and cashless service delivery, (Nov. 6, 2020, 6:00), https://drive.google.com/file/d/0B8eAaE2o9Uh8d3JsX3pNeVNCSVVoRU45VTJLTlFfZlBweHRN/view
[14] Anja Kovacks & Nayantara Ranganathan, *Data Sovereignty of whom?*, Data Governance Network policy brief - 3 (Nov. 20, 2020, 20:00), https://datagovernance.org/files/research/1605850788.pdf.

All these ideas only make sense when we assume *free choice* without any coercion or any conditions that makes the choice severely constrained. We know that the privacy policy agreements that we assent to when we sign up for all applications are mandatory to be assented to for using the services of the application. In this condition - the user doesn't have a free choice, because the only way that they can access the application is if they give up their personal data. So by making their services contingent on collection of personal data - the individuals do not have a free choice and thus by extension do not have any claim to the personal data being collected by these applications. This is the status quo where data principals do not have any property rights either over the data that they've wilfully submitted OR the data that they generate by the virtue of their activities on the application. A classic example of how such conundrums seep into government provided benefits is Aadhar. The government still maintains that Aadhar is a voluntary program, however by making Aadhar mandatory for almost all government services, the state has forced the people who are entirely dependent on these services to sign up for Aadhar. We must look closely at how even after NOT making enrolment for Aadhar as mandatory for everyone - they've created a bypass[15] to achieve the same outcome by making deliverance of services contingent on Aadhar thus eliminating any free choice for the people.

Proposal - A 3 step model:

You can only realise property rights over personal data if you can:

1. *Access any service/application irrespective of giving control of your personal data to the service providers/application.*
2. *If you can have the faculty to know, at all times, what is the complete personal data that the application/service has collected on you.*
3. *If you can, at any time, take back, in part or in whole, your personal data.*

The DEPA framework has taken a progressive step by introducing the concept of consent in data transactions for financial purposes, however it suffers from the same problem of illusion

[15] Reetika Khera, Dissent on Aadhar (2019)

of data control (and largely - data ownership). By making all or at least most microcredit and small loans facilities available subject to data principals' consent to have ALL of their financial decisions and spending monitored and collected as financial data - the framework essentially removes the concept of free choice completely. Because the logic is that if you are a small time businessman and you want microcredit or a small loan - the only way you can avail this facility is by letting go of any and all control over your financial data. Therefore by the 3-step model laid out earlier:

1. DEPA framework fails on the first account by the analysis as given above.
2. DEPA framework is silent on this point. Data principals should know the full of their personal information that such services and platforms have collected.
3. This right, even if given under DEPA, is essentially a non-right - because the people who need the microcredit and loans cannot avail of these facilities without giving up all rights over their financial data, and since the people who need it cannot get it any other way - they do not have the right to take back their data and still continue to avail the services of the state/free market. [see the similarity with the Aadhar model of creeping data control]

Recommendations

By this analysis we can conclude that the DEPA framework essentially strips the data principal of any property rights over their personal data. The framing of 'control' of personal data by the data principal by virtue of asking for consent is also illusory at best. Consent is not meaningful if you have no other choice BUT to consent to the request to be able to avail any state benefits. Therefore the recommendation is to employ the 3-step model as detailed above in the metrics and give as much control and ownership to the data principal while providing the same level of services.

Information Property rights

Legal roots of Information Property rights

The Supreme Court in *Puttaswamy*, recognized the right to privacy as a fundamental right under Article 21 of the Constitution of India.[16] Moreover the judgement went into details of how "informational privacy" is an important component of the right to privacy. Thus, an individual has the right to control over dissemination of material which forms any part of the personal data. It is ideally accepted that personal data of a person is owned by that person.[17] This right is also protected under SDPI Rules, the IPC and the Information Technology Act, 2000. An argument can be made in certain cases that there could be multiple claims of ownership over the same data. For example, when a person takes out loans or invests, the credit and investment history, and other details could be said to belong to various entities, such as the investor, fund manager, custodian, trustee, internet companies, website traffic tracking agencies, etc.

Information Property Rights and DEPA Framework

As the framework of DEPA is based on consent-based transaction of data for availing and providing financial services. In such a case, the need to understand how property rights on data being transacted will be or should be allocated arises in order to understand who technically is the owner of such data and to what extent. All the entities involved have very different rights and obligations with respect to such data and the concerned rules are either inept or defragmented.

Silence/overlooking of information property rights

It can very well be argued that collection, processing, and dissemination of personal data by data fiduciaries, with the consent of relevant data principals, or as may be permitted by law,

[16] https://indiankanoon.org/doc/91938676/
[17] https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621

and compiling such personal data into meaningful databases, is a result of skill and labour, and thus such databases could be considered property. However, **to give ownership rights over it to the data fiduciaries, which either undermines or overrides the rights of the relevant data principals, may not be reasonably accepted** as any use or misuse of this data may have real life consequences for data principles. Data fiduciary may claim a copyright in the databases, but the rights on the personal data itself must belong to the data principal. In this regard both the PDP bill and DEPA framework are either ambiguous or silent.

Space for possible misuse of Consent model

Under Transfer of Property Act, 1882 'receivable or an actionable claim' is recognized as intangible property. As such a receivable as an actionable claim provides its holder the right to receive back or recover money or goods from a debtor. This claim may also be transferred or assigned by the holder of the receivable to a third party. By same logic, as conceived under DEPA framework, if a data principal provides his or her consent to a particular consent manager for the usage of his or her personal data, such consent may permit further transfer of such personal data by the original data fiduciary to a data processor or to a third-party data fiduciary.

Ideally the data principal also has the right to withdraw such consent. It is possible that the data principals may be able to even transfer their right to grant or withdraw consent on their behalf for the usage of their personal data to a third party for a specific period. Such transfer may be for 'valuable consideration' yet the third party with such a right may be entitled to further transfer it to other third parties, in a manner akin to the transfer of receivables.

Monetization and possible commercialization of Consent

It is also not implausible that at some point the data principals grant consent managers, for a consideration, the right to give consent on their behalf to third party data fiduciaries. In such a case, the consent managers would be able to monetise the consent received from the data

principals by selling or transferring the consent to third party data fiduciaries within that particular time period.[18]

Recommendations

- ➢ Providing guidelines for information property rights which not just explain in detail the extent and nature of these rights but also clearly demarcate the rights of data fiduciary and their obligations with regards to usage and processing of such data must be drafted and incorporated within the ambit of Personal Data Protection bill and DEPA Framework itself.
- ➢ The addition of a Section detailing the nature and extent of 'Information property rights' in Personal Data Protection bill and a separate chapter dealing with the 'information property rights' in contest of the 'consent model' envisaged in proposed DEPA framework.

Standards for Non-Personal Data and Data Anonymization

Definition of Personal Data:

"*(28) "**personal data**" means 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;"*

As per the Report by the Committee of Experts on Non-Personal Data Protection Framework, the present definition of Non-Personal Data is:

"When the data is not 'Personal Data' (as defined under the PDP Bill), or the data is without any Personally Identifiable Information (PII), it is considered Non-Personal Data.

[18] https://www.mondaq.com/india/privacy-protection/978012/exploring-property-rights-in-personal-data#_ftn3

- *Firstly, data that never related to an identified or identifiable natural person, such as data on weather conditions, data from sensors installed on industrial machines, data from public infrastructures, and so on.*
- *Secondly, data which were initially personal data, but were later made anonymous. Data which are aggregated and to which certain data-transformation techniques are applied, to the extent that individual-specific events are no longer identifiable, can be qualified as anonymous data."*

Recommendation

On the issue of no singular definition of non-personal data, we recommend the adoption and support of the Committee of Experts, that has divided non-personal data into three categories namely, (a) public non-personal data, (b) community non-personal data and (c) private non-personal data[19].

Note: *Anonymisation has an important role within the context of personal and non-personal data as it is a tool for converting personal data to make it non-personal data. The risk posed is however, that anonymised data can be re-identified. Hence, introducing an element of sensitivity to non-personal data can prevent non-personal data from posing substantial risk.*

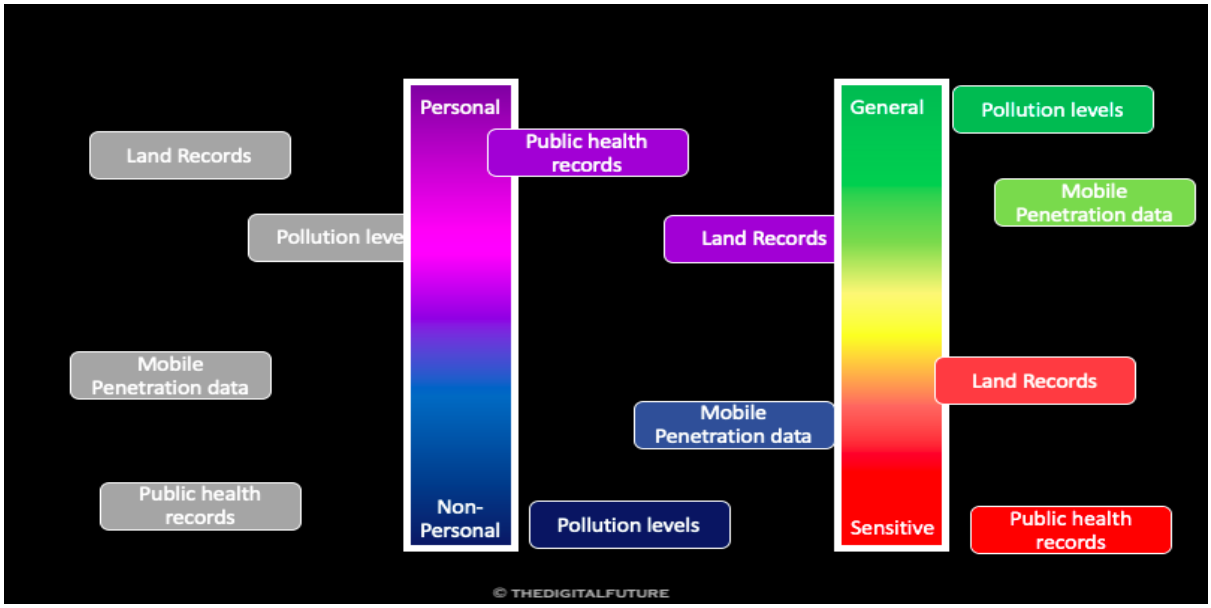
Sensitivity

In addition to the 3 categories of non personal data, the Committee of Experts also recommended that, 'sensitivity' should also be read with non-personal data and not just personal data. The former can also be subject to 'sensitivity' as illustrated in the Report, situations may arise where non-personal data which arises from personal data, will also be subject to some level of sensitivity due to the nature of underlying personal data. For e.g. Anonymised data collected by a research body for a genetic study of a communities susceptibility to cancer, can be categorised as 'sensitive non-personal data' as the underlying health and genetic data is defined as 'sensitive personal data'.

[19] Committee of Experts, Report on Non-Personal Data Protection Framework, pg. 14-15

Recommendation

Therefore, we highlight the importance of inserting a sensitivity spectrum or filter even when dealing with non-personal data. Data processors and controllers, will have to take into account that non-personal data too can pose significant risk to national security, financial sector, strategic interests of the country a communities safety and so on.



Consent

We note that the DEPA framework does take into cognizance the importance of adopting an approach which is in line with the PDP Bill, however the same cognizance should also account for non-personal data. 'Consent' as defined in Section 11 of the PDP Bill is with respect to 'personal data' and has been restated in the DEPA Framework as 'free, informed, specific, clear and revocable', with respect to 'personal data'.

Recommendation

The consent architecture should not only account for 'non-personal data' but also for the process of anonymisation itself.

- at the time of collection of data;
- at the time of anonymisation of personal data; and
- at the time of usage of anonymised non-personal data.

B. INSTITUTIONAL ARCHITECTURE

Business Models for Consent Managers

For an ecosystem to flourish, a viable business model is quintessential. DEPA, while refraining from setting out parameters and boundaries, lays out multiple business modelS in alternative. It envisages Consent Managers as data agnostic transaction facilitators, who charge a nominal or no fee for the transaction. Among others, it hypotheses models wherein (1) consent managers act as independent body charging a fee, or (2) the role of consent manager is performed by the in-house team of the data users itself, or (3) the independent Consent Manager additionally offer data privacy and security services to the data users.

Antitrust and Anti-Competitive Concerns

While the revenue models might have been developed to balance the best interest of the data principle, data user and Consent Manager, they overlook antitrust concerns that are co-found with such business models. During the Net-neutrality debate, we saw Internet Service Providers (**"**ISP**"**) more than willing and happy to prioritise and throttle data speed and bandwidth for websites of certain blue-chip companies. A preferential product model was developed wherein, through private contracts, these giants could ensure their data would be prioritised over their competitors. In this product model, a new and relatively small competitor would have faced marginalisation and ultimately elimination from the market at the behest of private contracts. Similarly, in light of the fact that the new data privacy architecture under the Personal Data Protection Bill is said to place additional heavy responsibility over new and relatively small competitors, an adverse and unregulated revenue model of Consent Manager could end up facilitating exclusion and elimination of competitors for existing tech giants and new Consent Managers.

While the Consent Managers are said to be data agnostic, they are well capable of performing analysis of the transaction and figuring out the parties at either end of the transaction. This data could be utilised in the revenue model to prioritise and de-prioritise requests for certain parties over others. This factual matrix is further problematised if the Consent Managers choose to

charge different fee for facilitating transaction for established industry giants, by charging higher fee for facilitating fee to facilitate transaction for industry newcomers in the disguised argument of frequency of transactions.

Lack of prohibition on such private contracts can further lead to exclusion of new consent managers by depriving them of opportunity to build a viable business framework. While it could be argued that that is an issue covered under Competition Act, 2002, there are two facts that need to be kept in mind: (1) the existing anti-trust policy of India and (2) the nature of transaction being undertaken by Consent Managers. The Competition Act, 2002, while being well capable of dealing with allegations of abuse by a single dominant player, has often been found incapable of dealing with cases of collective dominance[20]. Further, Consent Managers are tasked with the responsibility to facilitate transaction concerning highly sensitive data, any adverse practice adopted will directly affect the success of the DEPA ecosystem.

Recommendations

We recommend:

(a) Outright prohibition on possibility of private contract between the data users and Consent Managers.
(b) A price band to be charged by a Consent Manager to be laid out by a regulatory body, after due consultation and representation of all the stakeholders.
(c) Formulation of full-fledged regulations regulating activities and behaviour of Consent Managers.

Scope of work under 'Additional Services'

There has to be unadulterated clarity about the task to be performed by the Consent Managers under their power to provide with 'additional services' mentioned under the heading of Business Models for Consent Managers in DEPA. The lack of defined scope of work or a hazily describe scope of work of the 'additional services' would leads to uncontrolled development

[20] Ashok Kumar Vallabhaneni v. Geetha SP Entertainment LLP, 2019 SCC OnLine CCI 27.

of services provided leading to complexity, chaos, multiplicity of work and sometimes even biases.

Recommendation

We recommended that in light of the undefined work under the heading of 'additional services' be defined with respect to:

(a) Sectors that Consent Managers can cater to;
(b) The position of the Consent Managers allowed to provide those additional services;
(c) The extent and definite scope of work that can be undertaken by the Consent Managers with respect to data privacy and security; and
(d) Any other detail which the specialising and drafting committee may seem fit.

Clarifications sought:

1. To what extent can competing consent managers be interoperable? We are unable to understand how consent managers can be interoperable, as their role is to streamline consent and data request flows between information providers, information users and consent giving user/data subject. Clarity is sought with respect to:

    1.1. meaning of interoperability with respect to multiple consent managers;
    1.2. examples of interoperability with respect to multiple consent managers.

2. There seems to be a conflict with the role of the consent/account aggregator. It is stated on pg. 35 that "**the data itself is not necessarily streamed through the servers where the account is hosted**" and on pg. 43, it is stated that "t**he data that flows through the AA is encrypted**".

    2.1. The first point of contention is that these two statements are contradictory to the extent that one states data does not necessarily flow through the aggregator and the other states that it does indeed flow through the aggregator but it is encrypted. Clarity is sought in this aspect.

2.2. The model proposed is that consent and account aggregators will only direct the request for consent and granting of consent. No data itself is presumed to flow through the aggregator (as depicted in diagrams on pg. 34 & 43). Clarity is sought as to what is this "data" that is referred to on pg. 35 and 43 statements emboldened above.

Recommendation

In light of the unclear role of consent and account aggregator with respect to 'flow of data', we recommend that the definition of "data" being referred to while explaining the aggregator model be defined.

CHAPTER 4 - BUILDING DEPA FOR THE FINANCIAL STRUCTURE: THE ACCOUNT AGGREGATOR MODEL

The Account Aggregators ("AA") system proposed to be used under DEPA for facilitating transmission of data from a Financial Information Provider ("FIP") to a Financial Information User ("FIU") appears to be entering uncharted waters, with very little established mechanism of its actual working. At the outlook, there appears to be some blatant issues that are likely to arise once the system is set to operationalise.

REGULATORY FRAMEWORK

RBI as the regulator

The Reserve Bank of India ("RBI") being the sole regulator in this framework provides RBI with unbridled power to oversee the functioning of the AAs. While RBI regulating the AA operations when the data is financial appears to be something that might work, however, since the idea is to extend DEPA to the healthcare and telecom sector,[21] it appears that the RBI might not be best suited to be a regulatory body in such a scenario. Furthermore, regulatory oversights are not foreign to regulatory bodies like the RBI, and in that scenario, bestowing upon the RBI the power to regulate all AAs allowed to operate in the field, is again slightly worrisome. There is also a technological dimension to this ecosystem of AAs, and while the cyber and security needs of the RBI are met by ReBIT, we think that a more nuanced and targeted technological structure is required to address the concerns that might arise in the functioning and regulating of the AAs.

Recommendation

We recommend that a separate regulatory body be established to solely serve the purpose of regulating the AA ecosystem. This body should have the requisite technology and expertise to function effectively as a regulator of the AAs. Since the focus here is on the intersection

[21] DEPA, p5

between data and technology, the regulatory body should have expertise in this field, and accordingly establish best practices suitable for their functioning.[22] This has been further discussed in the subsequent recommendations for 'self-regulating authorities', herein below.

Self-Regulating Authorities

It has been suggested that self-regulatory authorities be set up to look out for data subject interests and design sector specific sharing guidelines. In fact, a financial sector self-regulatory authority has been set up called 'Sahamati'. We understand that AAs have been granted legality vide RBI **Master Direction DNBR.PD.009/03.10.119/2016-17, called the Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.** However Sahamati, is a private company, set up to organise, manage and design the account aggregator framework.

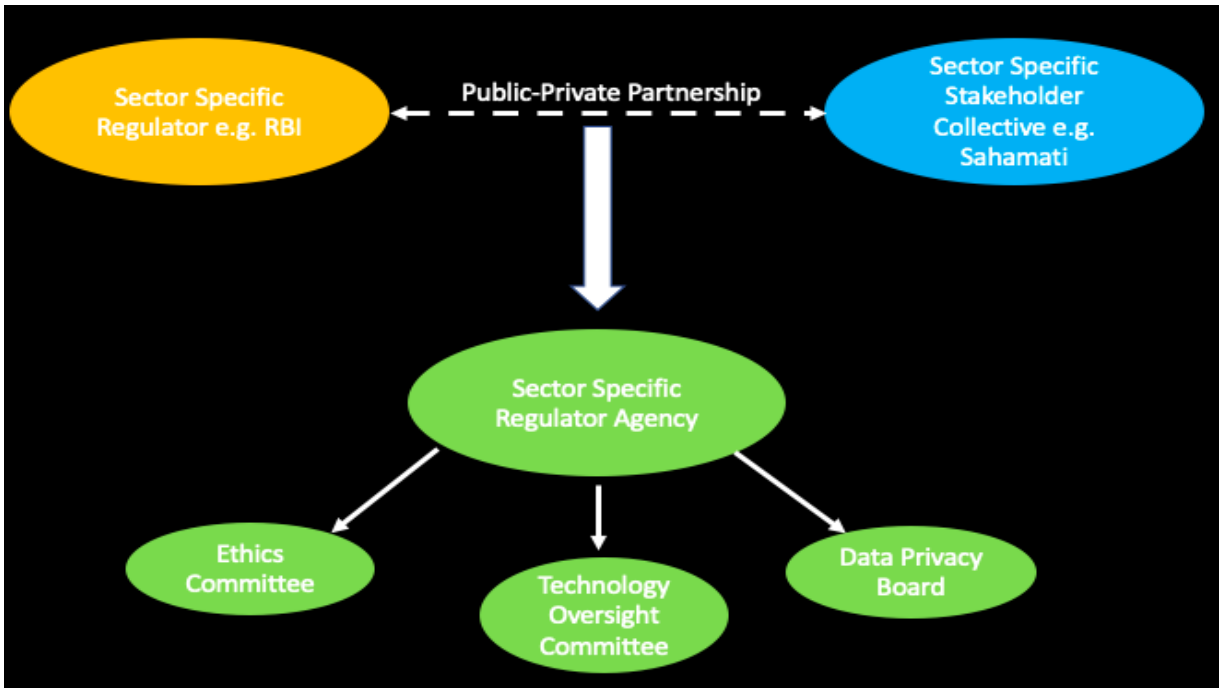
1. 'Sahamati' has defined itself a 'Self-organised Collective', and it has granted itself the authority to 'Develop and Run the Central Registry' - Please clarify as to how a not-for-profit private company can deem itself to have such authority.
2. It has identified itself as a 'certification authority' on common minimum compliance on privacy, security, and API standards.[23] - How will this certification hold credibility when in a court of law, in the event a dispute regarding breach of obligations by an account aggregator?

We understand that, there is no suitable existing government agency which can take on the role of monitoring the account aggregators from the perspective of data subject interests, stakeholder interests and privacy. However, we also do not recommend wholly leaving up regulation to self-regulatory authorities which are especially established under the Companies Act, 2013 as a private limited company. Keeping in mind the guiding principles of accountability and transparency, a private company is not the most stable body for regulating an entire ecosystem. Further we understand that other sectors will also have their own aggregators and subsequent self-regulating authorities.

[22] https://www.medianama.com/2018/11/223-exclusive-rbi-issues-in-principle-licenses-to-5-account-aggregators/
[23] 'About Sahmati' https://sahamati.org.in/about/#

Recommendation

We recommend that a private company cannot solely be the monitoring or regulating agency in charge of the account aggregator ecosystem. We would recommend an entity or agency be established as a part of a public private partnership, with which institutional and regulatory oversight can be assigned to. Rather than discrediting Sahamati entirely, we would suggest a scenario where Sahamati can provide the appropriate input for establishing an entity/agency. This entity or agency, should embody the guiding principles mentioned in this paper while taking charge of the management and supervision of account aggregators. As the RBI is the authority regulating AA (Non banking financial companies) we recommend that the RBI, would be the appropriate financial regulator with which the public-private partnership could be entered into. Respectively for the other sectors, we can look to the relevant governing authorities therein, such as the National Health Authority which is working on a National Digital Health Mission.



Financial Information Users

There have been no clear guidelines passed regarding the storing, processing and consuming the data that FIU's receive from the aggregator. RBI should create guidelines for specific parties involved in the transaction. Guidelines should also set a bar for minimum level for security protocol to be followed by the parties involved for assurance in case of a data breach. This should be at the utmost priority after the infamous Aadhaar data leak.

Recommendations

Obligations of the FIU's: All FIU's must undertake certain transparent and accountability protocols:

(a) Certain security safeguards should be established such as data encryption to prevent misuse of data; and

(b) Establishment of grievance redressal mechanisms to address concerns of FIUs, FIPs, and individuals.

Institutional coordination

Only 20 percent of people in India have access to the internet at least occasionally while a mere 14 percent own a smartphone.[24] Additionally, the use of resources available to them is quite bleak too. For a smoother implementation, there is a need for greater awareness among data principals, their rights and the consequences of sharing or not sharing data, the availability of consent management services etc.

Recommendation

We recommend adopting the awareness programs imparting knowledge about the use of this service and technology in languages specific to the state, village or city so as to not be in a position where they happen to consent to data sharing without knowing the consequences, both positive and negative. Additionally, in light of security of data and avoid misuse of information, we further recommend the use of digital signatures to guarantee integrity of access permissions

[24] https://www.thehindu.com/business/how-many-indians-have-internet/article17668272.ece

given by the consenting individuals. This would avoid security issues/breaches and rather maintain transparency while making it fully legal under the Information Technology Act, 2000.

Lack of Standardised Pricing

AAs are allowed to charge FIUs and the data owner for facilitating the transmission of information. Although during the initial rollout, there seems to be no chargers for FIPs, they may be allowed to have a nominal charge. There is no standard on how AAs can charge for such data transmission, and although initially that might not seem like an issue, once there are enough players in the AA ecosystem, not having a price bracket and giving AAs the full power to establish their charges might cause issues.

Recommendation

We recommended that a certain base price and price bracket be created to address this issue, so that AAs do not get unchecked power to impose charges. Further, we also recommend that more light be shed on the definition of nominal charges in terms of the FIPs.

CHAPTER 5: AN OPPORTUNITY FOR THE ECOSYSTEM TO CO-CREATE

As DEPA itself has stated "An opportunity for co-creation". The document states that multiple "market players" will have the opportunity to build on this platform. It also mentions that rather than following a private player versus public entities system, the DEPA will accommodate a "Relay Race" model where these "market players" will work in harmony for collective progress.

Willingness of Private Players to Adopt the Framework in their Daily Functioning

As such, the word "opportunity" has to be stressed on in this section of the document for the purpose of analysis. Even though the document mentions that private players will play a role in the framework, this document fails to mention any incentive that would result in private players willing to play a pivotal role in the incorporation of the framework. Moreover, in the same regard, the document does not explicitly mention what "different market players" will consist of. Usage of sentences such as "All players in the ecosystem could work to build awareness around informed consent"[25] only seems to showcase that the document itself is not very clear in this regard. The organisations that can be potentially included seem to fall under a very broad category of "financial institutions" and the lack of classifications of the same on the basis of private and public do not pose a picture of a clear road that the framework could follow.

It is not clear why private financial institutions would want to adopt the framework in the first place. The composition of hiring an account aggregator, setting up the framework and other costs included in the application of the framework might not make DEPA a viable opportunity for financial institutions. To add, data from the past can only go so far to convince financial institutions of the investment of their money. Collateral may still be the largest factor that might affect financial opportunities even for MSMEs.

[25] Page number 15| Co Creation| DEPA Document

Hidden Fees

The hidden fees issue only seems to increase the cost of issuing a loan for the bank. Page number 43 of the document mentions "Financial information providers have committed to provide free service today could charge a nominal fee in the future." However, private players may not follow the same. If the hidden fee increased by hiring of consent managers or transferring data is borne by a financial institution, then the financial institution itself may be demotivated to offer any loans and on basis of data ordered by them. If it is borne by customers however, it would be interesting to consider how the financial institutions would act against the provisions mentioned inside the document by increasing a debt on customers.

Recommendation

Subsidies for private institutions for implementing the framework can be a method to make private institutions adopt it. A notification can be released containing the exact composition of "market players" and the institutions that the framework will directly impact for clarity.

Usage of Technology and Digital Methods by MSMEs

Analysing the facts mentioned in DEPA, it can be understood that the document aims to "empower" individual or small businesses through the usage of their data-based background by financial institutions to provide them credit. While the intention behind the framework may seem usable as it is documented by several studies that a major roadblock in the growth of MSMEs in India is the lack of credit provided to them, a problem that can be identified promptly is the lack of architecture for implementing the same.

Even if individuals are discounted and only MSMEs are considered, it is to be noted that the majority of the MSMEs today lack a digital channel. In a survey conducted by Boston Consulting Group in 2018[26], 87 percent of merchants found conducting their transactions digitally unattractive and 77 percent of merchants lacked clarity on methods for digital payments. If this survey is to be considered, it raises concern for the data generated by MSMEs.

[26] "Indian needs its MSMEs to go cashless: Report" | The Economic Times | https://economictimes.indiatimes.com/small-biz/sme-sector/india-needs-its-msmes-to-go-cashless-report/articleshow/59233358.cms?from=mdr

The non-usage of digital methods often results in lack of transparency and further, for the purpose of DEPA, lack of sufficient data generated that can be used. It is to be understood that whatever data is generated may come under scrutiny because the other transactions may not result in substantial digital data that can be monitored by financial institutions. And when there is absence of data (data relating to cash transactions) that is associated with significant workings of the business, a half-baked picture will be difficult to be considered by financial institutions.

Adaptability to Technology

As stated by the survey, 77 percent of the merchants lacked clarity on digital methods to be used. If this is taken in perspective, it can be safely said that business owners in India are not very adept with technology in general. To supplement this, a Yes Bank Survey in 2019 stated that only 5% MSMEs have actually embraced digital technology completely[27]. This may have changed over the course of last year, but not likely to a degree very a majority would be comfortable using technology. If so, it would be very difficult for business owners to adopt the idea of data empowerment and how it would benefit them in general.

The primary purpose of the framework being the idea of individuals benefiting from the data they produced, actual implementation needs the populace to understand how the framework would actually work. With the prevailing knowledge of technology in general, this will pose as a huge roadblock for DEPA and the idea with which it was formed may not be very effective. This point will also be strengthened by the lack of access to the internet and devices for the production of data, and the considerable number of individuals and business owners without access to the same.

Verification Process

[27] "Only 5% MSMEs have fully embraced digital technology, says Yes Bank survey" | Financial Express | https://www.financialexpress.com/industry/sme/only-5-msmes-have-fully-embraced-digital-technology-says-yes-bank-survey/1447985/

The obvious contention that one may make against this point is that MSMEs do keep their own book of accounts to monitor every past transaction. Even if that were practical, there is no third party in this case verifying the data generated by MSMEs in non-digital form. For instance, recording transactions on UPI services guarantees a reader of the authenticity of the transaction made because it is made through that particular service.

Recommendations

There is no particular recommendation that can be made in this regard, it's rather an obstacle that can only be resolved through deep penetration of technology in businesses and understanding of the same. A framework cannot be used efficiently if it is made and then the supported technology and knowledge is attempted to be inculcated. The framework has to be rather developed on the existing technology in the market and MSME sector in India has not come to adopt it yet.

SPEED AS A MAJOR CHALLENGE TO INTERNET QUALITY

Lack of inadequate internet speed will pose an obstacle in the successful proliferation of the DEPA Framework.

"*The Indian Standard of more than* 512kbps *for broadband is significantly less than many countries that demand a download speed of above 1 to 2Mbps for the service to be classified as broadband. A recent investigation by the Digital Empowerment Foundation found that in many villages, speeds are half of what has been assured as part of the NOFN."*[28]

TRAI report reflects that smartphones which have wireless connections are widely used. Presently, India has approx. 684 million mobile internet subscribers whereas, the wireless internet subscribers, which have high quality speed connection by virtue of Wi-Fi or Wi-Max, comprise just approx.0.64 million as of July 2020 statistics noted by TRAI. *Figure below.* [29]

VIII. Broadband (≥ 512 Kbps download)

- As per the reports received from 345 operators in the month of July, 2020, the number of broadband subscribers increased from 698.23 million at the end of June-20 to 705.40 million at the end of July-20 with a monthly growth rate of 1.03%. Segment-wise broadband subscribers and their monthly growth rates are as below: -

Segment–wise Broadband Subscribers and Monthly Growth Rate in the month of July, 2020

Segment	Broadband subscribers (in million)		Monthly growth rate in the month of July-20
	As on 30th June, 2020	As on 31st July, 2020	
Wired subscribers	19.82	20.13	1.56%
Mobile devices users (Phones and dongles)	677.79	684.64	1.01%
Fixed Wireless subscribers (Wi-Fi, Wi-Max, Point-to-Point Radio & VSAT)	0.63	0.64	1.76%
Total	**698.23**	**705.40**	**1.03%**

Smartphones being the device of choice for accessing the internet become a bone of contention because the problem of speed persists over wireless networks which have a speed that is less

[28] Aloke Thakore, Digital inclusion: Definitions and status in India, Centre for Communication and Development Studies, (June 13, 2015) https://digitalequality.in/digital-inclusion-definitions-and-status-in-india/
[29] TELECOM REGULATORY AUTHORITY OF INDIA, New Delhi, 12th October, 2020 (Press Release No.84/2020) at page 12; https://www.trai.gov.in/sites/default/files/PR_No.84of2020.pdf

than the standardised meaningful speed i.e. 512 Kbps as confirmed by TRAI. Moreover, access to certain government websites and more utilitarian purposes require high speeds and large screen devices. This coupled with lack of access, awareness and affordability problems hinder the implementation of the current DEPA model.

For Banking services, successful transactions will require high speed and optimal user interface both of which need computer literacy and financial backing. One major concern with respect to banking related transactions online is the issue of refresh button which happens when the net connectivity is low due to a reduced speed wherein when the individual clicks on the refresh page while the transaction has been in progress for a long time, it may happen that the money has been debited from the account but has not reached the receiving portal making is a failed transaction. Usually in such cases, the money refunds by itself within a period of 14 days but there is no guarantee that the money will return in the bank account. Certainly, new users are bound to become anxious as lack of human agency in this entire process makes it harder for consumers to trust the online system.

As already outlined by the central government, it was the goal of National Telecom Policy 2012 ("NTP") to achieve the target of providing reliable broadband connections by the year 2015 which have a minimum speed of 2 Mbps and ensure availability of high speeds which have at least 100 Mbps speed in order to give high quality internet access to rural areas. NTP revised the aforementioned speed limits to a minimum of 512 Kbps and then subsequently to 2 Mbps though TRAI allows 512 Kbps as a meaningful standard of internet speed. However, these targets have not been achieved and India still has a long way to go.

Recommendation:

It is evident that the issue of accessibility will not be resolved by just providing an internet connection and a technological interface such as a mobile phone if the same lacks efficient performance in terms of adequate speed and ability to connect with 4G and 5G internet networks in order to conduct secure financial transactions proposed by DEPA which require a desired bandwidth speed. The setting up of these networks (with a minimum speed of 512 Kbps) in rural areas becomes an important goal to be achieved before the implementation of the DEPA framework.

COMPARISON WITH INTERNATIONAL POLICIES

The need to consider international policies is reflected in the draft itself:

"Although learnings from global data security approaches have been captured in India's draft Data Protection Law, replicating other nations' data sharing strategies would not go far enough to achieve India's objectives: those of ***individual empowerment and financial inclusion through data****, of encouraging a vibrant* ***data democracy,*** *and of building an environment for* ***businesses to thrive based on legitimate and high value use cases for data sharing****." - DEPA*

France's National Strategy on Artificial Intelligence policy

DEPA: *Data sharing For data sharing to evolve to support emerging needs, the framework needs to engage the right experts and stakeholder communities on data sharing policy and regulation through institutions, upgrade APIs appropriately, and move forward on a continuum as technology evolves.*

Recommendations

State's role as a trusted third party to the economic players' pool of data. - In order to incorporate the exceptional magnitude of size and diversity India has to grapple with, while encouraging economic growth, a consent-based sharing approach should be preferred. Such is highlighted in the DEPA draft's reliance on a framework of institutional accountability and regulation, with a consent-based sharing approach at its core. However, the specifics of this framework remains unclear.

France's position on this permits data circulation between stakeholders which are controlled by elementary data protection rules, like the current Privacy Bill in India and ensuring citizen's control over their personal data. This is structured to maximise economic and social utility because the application of regulations differs within the public and private sector as well as

across priority areas such as health, transport and environment. The alternate data protection and governance model suited for the private sector is based on the ideals of transparency, cooperation and sharing. Through division of models into priority areas France's model avoids stretching data policy too thin. The private sector's governing model allows the State to act as a third party for data sharing between private to private body as well which helps in ensuring accountability and avoiding exploitation of data.

Ecological economy - In the draft's emphasis on innovative technology and balancing free market needs, sustainability goals have been lost. France's policy lays grounds for an ecological economy. It advocates for a greener AI value chain and a task force dedicated to assessing the environmental impact of smart digital solutions. The customer also plays a role in ensuring a greener and sustainable future under this policy. The draft's constant reminder of the need for private innovative solutions should be coupled with considerations of environmental impact.

European Union's Regulation on the Free Flow of Non-Personal Data

Factor to be kept in mind while assessing policy: *EU, like other countries that have established data protection or sharing frameworks, have already had much of their population become economically wealthy prior to becoming 'data-rich'.*

Recommendation

Free flow of non-personal data being a prerequisite for a competitive economy. - This regulation protects free flow of non-personal data, unlike the GDPR which governs free flow of personal data. This regulation considers data localisation restrictions as an impediment on a competitive economy and has thus limited them severely. India cannot follow suit in this case as the cons of restricting control of free flow of non-personal data by public authorities, outweigh the pros of economic growth of the private sector. However, India could encourage cloud service providers to develop independent self-regulatory codes of conduct for easier portability of data. This could imply trust in the private sector and limit public authorities' supervisory role to a reasonable extent.

UK's Open Banking Standards

Uk's Open Banking Standard is a regulatory-driven initiate to facilitate more competition between the financial service providers. It should be noted that the standards are formulated and regulated jointly by the Financial Conduct Authority and Competition & Markets Authority.

Recommendation

Overarching Competition Law concerns of Data Portability - Open Banking Standards were formulated with an overall aim of promoting competition in the banking services industry by facilitating the creation of innovative finance services. Consumers are given a choice and greater control over whom they want to choose to manage their own money. As stated in the guiding principles, the main focus of this regulation is - "individual empowerment and financial inclusion through data and of encouraging a vibrant and competitive data democracy….". While the UK focuses more on competition, this regulation's focus is on financial inclusion. But, that does not mean that the thriving competition concerns should remain unaddressed. The Net-Neutrality debate focused on how Internet Service Providers were working in tandem with few corporations to eliminate competition by subsidizing data. The same can be applied in the case of Consent managers to not only eliminate competition for certain favoured competition for certain favoured corporations by adopting strategic pricing pricing structures. In the UK, data storing regulations are in place as per the GDPR which was already implemented before the rolling out of Open Banking Standards. The simultaneous implementation of Data Protection Act and this regulation in India has the potential of these issues going unnoticed.

Australian Consumer Data Right

Treasury Laws Amendment (Consumer Data Right) Act, 2019 ("CDR") became operational in Australia from February 2020. It is implemented with phases. First, focusing implementation in the financial sector and then extending it to telecommunication and energy. It is to be noted that this Act only makes provisions as to the portability of "sensitive information", while all other forms of information are already regulated by the Privacy Act.

Recommendation

Guiding principle of Evolvability - This principle stresses on evolutions of the regulations and the flexibility that the authorities enjoy in making due changes with the changing landscape of the society and forthcoming technological advancements. On the similar lines, Australian legislation left the room for the implementation of CDR open to various sectors and scenarios. But rather than leaving the future plans vague and unspecified, the Australian Government has taken measures and published Suggestion Papers discussing at lengths how the CDR will function in sectors like energy and telecommunication. This has helped in demystifying the process of the data portability as well as taken into consideration the sector specific needs of the consumers and businesses. India should take into consideration this factor to bring in some stability, certainty to the regulations. India's open banking gateways like KYC and UPI experienced a slow start due to consumer stigma coupled with misinformation. Clearly laying down the future endeavours along with the current approach would be beneficial to combat this stigma.

QUALIFICATIONS

The thoughts and views expressed in this reply are meant to be viewed pragmatically. The research team does not purport to be experts in the field of privacy, economics or regulation but rather we are a team of thinkers, action takers and concerned citizens who wish to provide useful observations and comments.

We represent a portion of society made up of majorly law students who have a deep interest in public policy, technology disruption and privacy. As younger millennials who will be inheriting property and wealth in the near future, we have expressed our opinions to a proposed new system that we will be the guinea pigs for.

With utmost respect to the teams of highly qualified individuals that have put their effort into the DEPA project, we hope that we were able to provide some useful insight for the framework.

Disclaimer: In no way do the opinions reflected in this document represent the opinions of Jindal Global Law School or any of the institutions we are working/interning with. The opinions expressed are purely personal opinions of each researcher.

Thank you

The Digital Future