CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO NITI AAYOG ON THE DRAFT DISCUSSION PAPER ON THE DATA EMPOWERMENT AND PROTECTION ARCHITECTURE[1]

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in

[1] Authored by *Sangh Rakshita* and *Shashank Mohan*. Reviewed and edited by *Smitha Krishna Prasad*. Research support provided by *Anuj Dubey, Drishti Kaushik, Priyanshi Dixit, Shikhar Aggarwal, Vedangini Bisht, and Waleed Nazir Latoo*.

The Centre for Communication Governance is an academic research centre within the National Law University Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication policy and protect digital rights in India through rigorous academic research and capacity building.

We are grateful to the NITI Aayog for inviting public comments and suggestions on the Data Empowerment and Protection Architecture.

Introduction

The Data Empowerment and Protection Architecture ("DEPA") is a data sharing framework that is based on user consent.[2] According to the Draft Paper for Discussion ("Draft Paper"), by taking control and accessing their data history, users can leverage the value of their data and benefit from market services like financial credit and better health services.[3] DEPA is imagined as a digital solution, wherein users can access and share their data with different entities at the click of a button or in a paper-less fashion.

The framework will make use of new privately owned entities in the form of Consent Managers, to ensure that all data sharing via DEPA happens strictly with user consent. Consent Managers will use the Electronic Consent Framework ("ECF"),[4] proposed by the Ministry of Electronics and Information Technology ("MeitY"), as its technological architecture. The ECF ensures that consent is provided by the users after due intimation of details like - the data provider, data consumer, consent collector, and the types of data.[5]

[2] The Draft Paper uses the word 'users' to refer to data principals/ users/ consumers etc. This document uses the terms users or data principals interchangeably, to denote the same category of stakeholders.

[3] The DEPA framework is based on the Account Aggregator model as created by the RBI in 2016, 'Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016' <https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598> accessed 17 November 2020.

[4] Ministry of Electronics and Information Technology, 'Electronic Consent Framework, Technology Specifications, Version 1.1' <http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf> accessed 9 November 2020.

[5] ibid.

While the goal of achieving data empowerment and user autonomy over data is in line with the privacy rights as enunciated in *K.S. Puttaswamy vs. Union of India*,[6] ("Puttaswamy") the methods of achieving such empowerment have not been sufficiently detailed in the Draft Paper.

Firstly, the DEPA framework over-emphasises on the ability of user consent to translate into actual control and autonomy. Due to various reasons such as information asymmetry,[7] consent fatigue,[8] the advent of big data,[9] and cognitive biases,[10] users are unable to provide meaningful consent for data sharing transactions. These issues are further exacerbated when access to innovative market products, like cheap credit, are hinged upon the click of a button or digital convenience. Although the Draft Paper recognises this lacuna,[11] it doesn't sufficiently explain how users will be able to provide meaningful consent using the DEPA framework. The Draft Paper also states that the Personal Data Protection Bill, 2019 ("PDP Bill 2019") along with the proposed Data Protection Authority ("DPA") will play a strong role in the regulatory framework for DEPA. But this is contingent on the passing of the PDP Bill 2019 which continues to be in review before a joint parliamentary committee.[12]

[6] 'Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1 (Puttaswamy)' (*Privacy Law Library*) <https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors?searchuniqueid=549539> accessed 19 November 2020.

[7] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' [2013] GW Law Faculty Publications & Other Works <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications>.

[8] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 17 November 2020.

[9] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Columbia Business Law Review <https://osf.io/mu2kf> accessed 22 November 2020.

[10] Solove (n 7).

[11] The Draft Paper acknowledges that consent alone cannot be the only backstop to prevent data misuse.

[12] 'Derek O' Brien Raises Concern about Conduct of JPC on Data Protection Bill' *The Hindu* (New Delhi, 10 November 2020) <https://www.thehindu.com/news/national/derek-o-brien-raises-concern-about-conduct-of-jpc-on-data-protection-bill/article33061937.ece> accessed 24 November 2020.

Secondly, the Draft Paper proposes the use of Consent Managers[13] as a separate layer for collecting the consent of users for data sharing transactions. Consent Managers will be private entities, who will be data-blind but will be tasked with facilitating the consent transaction for transfers of data. Although the Draft Paper suggests that Consent Managers will be created and regulated by different sectoral regulators or by the DPA for unregulated sectors, it doesn't clarify the details of such a regulatory mechanism.[14] Other issues including the protection against metadata collection, consent fatigue due to multiple Consent Managers, and lack of proof of concept, which arise from the Consent Manager model, are not sufficiently mitigated for by the DEPA framework.

Lastly, the Draft Paper doesn't explore other models of data governance and data sharing which may provide for a higher degree of user control and enable the breaking of existing data silos. Some of these models are - data trusts, data cooperatives, data commons, and data collaboratives.[15] Although some of these models are theoretical and practical adoption has remained slow,[16] learning from these models might offer an opportunity to build a more robust user serving data governance and sharing model in India.

Our comments focus on the key challenges with the DEPA framework from a user privacy and security perspective. In the first section we discuss the nature of data and how increasing data flows via the DEPA framework, in absence of a data protection law, leads to higher risk of privacy violations. Subsequently, we explain how the DEPA framework places a disproportionate emphasis on the usefulness of user consent. Due to various reasons, users are not able to provide meaningful consent to data sharing transactions. In the next two sections we discuss the challenges with Consent Managers and the role of the Government in the DEPA structure. In our last section, we refer to some other

[13] Consent Managers are like Account Aggregators as created by the RBI in 2016, 'Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016' (n 3).

[14] The Personal Data Protection Bill, 2019 is currently under review before a Joint Parliamentary Committee, 'Derek O' Brien Raises Concern about Conduct of JPC on Data Protection Bill' (n 12).

[15] Mozilla Insights with Ana Brandusescu and Jonathan van Geus, 'Data for Empowerment' (2020) <https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/> accessed 20 November 2020.

[16] ibid.

models of data governance and sharing which might be useful to learn from, before putting the DEPA framework into application.

Executive Summary

DEPA is a data sharing framework, which will allow users to port their data from one entity (information providers) to another (information users), to access better market services such as – access to credit and better healthcare. Although innovative data governance and sharing frameworks need to be considered to empower users in the data economy, the DEPA framework as recommended by the NITI Aayog, poses a few challenges.

Firstly, in the absence of a comprehensive data protection legislation in India, expanding data flows, may lead to privacy risks of data breaches. Other than stating that it will function under the broad framework of the Personal Data Protection Bill, 2019 (which has its own challenges) and different sectoral regulators, the Draft Paper by NITI Aayog does not explain how such risks will be mitigated. Secondly, the DEPA framework presumes that reliance on user consent will lead to empowerment. It is now well established that due to various challenges like information asymmetry, consent fatigue, and the advent of big data, meaningful user consent is difficult to achieve. The Draft Paper does not explain how these challenges will be overcome.

Thirdly, the Draft Paper recommends the institutionalisation of Consent Managers – a new form of private entity to manage the consent and data sharing transactions in the data economy. It suggests that each sector may provide for its own set of Consent Managers. Such entities pose various challenges to the privacy rights of users – they will collect large amounts of metadata which may cause privacy risks, multiple Consent Managers for different sectors may lead to consent fatigue, and the DEPA framework may help them bypass certain protections laid out in the Personal Data Protection Bill, 2019. The Draft Paper doesn't sufficiently consider these challenges arising out of the Consent Manager model.

Lastly, the Draft Paper doesn't engage with other types of data governance models such as data trusts, data cooperatives, data commons, and data collaboratives that seek to achieve data empowerment, to make its own suggestions more robust.

1. Nature of Data

DEPA is envisaged as an interoperable and secure data sharing framework that will empower individuals and small businesses by giving them practical means to access, control, and selectively share their data. One of the aims is to allow users to improve their experiences with products in relevant sectors, for example via ease of access to new financial products and services, contribution of data to research, and better-designed machine learning models that benefit them.[17] However, several concerns regarding data protection and privacy that stem from the very nature of data (discussed below), remain unaddressed in the Draft Paper. These concerns are exacerbated by the absence of a comprehensive data protection law in India.

A. Expanding Data Flows

As a data sharing framework, DEPA operates on the principle of data and platform interoperability where personal data can be re-used for multiple purposes with the consent of the data principal. Although enhancing access to and sharing of data may lead to social and economic benefits, this leads to expansion of data flows which carries the risk of privacy violation.[18]

Data Breach

Data, by nature, is non-rivalrous and can be easily duplicated.[19] Thus, expanding data flows can increase the risk of privacy breaches.[20] Large-scale data breaches, i.e. data breaches involving more than 10 million records, have become frequent and data breaches have increased with the collection, processing and sharing of large volumes of

[17] NITI Aayog, 'Data Empowerment and Protection Architecture (DEPA)' (2020) <https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf> accessed 10 November 2020.

[18] OECD, 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies, Chp 4 Risks and Challenges of Data Access and Sharing' (OECD iLibrary 2019) <https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en#endnotea4z12> accessed 19 November 2020.

[19] Charles I. Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data', *Stanford Graduate School of Business* (2019) <https://www.gsb.stanford.edu/faculty-research/working-papers/nonrivalry-economics-data> accessed 20 November 2020.

[20] OECD (n 18).

personal data.[21] Increased data sharing between institutions, platforms, businesses and sectors, facilitated by DEPA, will lead to definite expansion in data flows. This increase in data flows also increases the risk of data breaches. At present, due to the absence of a comprehensive data protection legislation, data principals have limited[22] protection and remedies against such breaches.

DEPA attempts to provide a secure and user consent based data sharing platform between Information Providers ("IPs") and Information Users ("IUs"). The accountability of IPs and IUs who operate at the two ends of DEPA is ambiguous. While the Draft Paper does not provide any clarification in this regard, the absence of a comprehensive data protection law means that there are no enforceable data protection measures available with users against IUs and IPs.

The PDP Bill 2019, which was placed before a Joint Parliamentary Committee in December 2019,[23] might require substantial time for its implementation after it becomes a law.[24] Even if the PDP Bill 2019 comes into effect in its current form, there are several concerns regarding the protections and remedies available in the case of a data breach. In the event of a data breach, data fiduciaries only need to inform the DPA, if the breach is likely to cause any harm.[25] Depending on the severity of the harm and the need for mitigation, the DPA will decide whether the data fiduciary needs to inform the data principal/s about the breach.[26] Data principals do not have quick redressal options for complaints of data breach under the PDP Bill 2019. Clause 32 of the PDP Bill 2019 provides the procedure for grievance redressal by data fiduciaries. A data principal

[21] OECD, 'Digital Economy Outlook' (2017) <https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en> accessed 23 November 2020.

[22] Sec. 43A and related rules of the Information Technology Act, 2000 do provide limited protection to users for information security breaches, but its scope (limited to body corporates) and implementation has been limited.

[23] The Personal Data Protection Bill 2019.

[24] Although the PDP Bill 2019, does not provide specific dates and timelines for implementation, a staggered implementation approach maybe required for complete implementation of the governance and regulatory frameworks under the PDP Bill 2019.

[25] 'The Personal Data Protection Bill, 2019' <https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf> accessed 23 November 2020 cl 25(1).

[26] ibid cl 25(5).

needs to necessarily lodge a complaint with the data fiduciary and can approach the DPA only upon completion of 30 days from the date of complaint if they are not satisfied with the redressal provided by the data fiduciary.[27]

User Control

Data access and sharing transfers data from one context to another. This change of context can often mean that the privacy assumptions and expectations arising in relation to the initial use of data are no longer relevant or applicable to subsequent uses of data, making it difficult for existing rights and obligations to be upheld.[28]

Once individuals provide their data and give their consent for their re-use and sharing the data also moves outside their control. Data principals then lose their capability to control how their data is re-used. As a result, there remains a risk that a third party may use data differently from what individuals consent to while agreeing to data sharing and data re-use.[29] The case of Cambridge Analytica illustrates this risk where the personal data of Facebook users was used for a commercially motivated political campaign. This occurred despite Facebook's prohibition on selling and transferring data "to any ad network, data broker or other advertising or monetisation-related service".[30]

Though DEPA relies on sharing of data based on the effective choice and consent of data principals, the overemphasis on consent is flawed and ineffective (see section 2). Providing meaningful consent for sharing derived or inferred data (as the DEPA framework provides for) might be even more difficult, as users would not be in a position to assess the potential privacy risks of sharing such data.

[27] ibid cl 32, the DPA can also take suo motu cognizance of a data breach (cl 53).

[28] 'Helen Nissenbaum' <https://nissenbaum.tech.cornell.edu/> accessed 23 November 2020; OECD Expert Workshop, 'Enhanced Access to Data - Reconciling Risks and Benefits of Data Re-Use' <http://www.oecd.org/digital/ieconomy/expert-workshop-enhanced-access-to-data-reconciling-risks-and-benefits-of-data-re-use.htm> accessed 23 November 2020.

[29] OECD (n 18).

[30] ibid.

B. Derived and Inferred Data

The Draft Paper indicates that the DEPA framework will apply to both personal and derived data. It defines derived data to mean raw data which is manipulated or analysed by a company's proprietary algorithms, indexes, or models to generate useful information. It further characterises derived data as data with masked personally identifiable information which could reveal confidential data of a company. Derived data is extrapolated and inferred from existing data about an individual using data analytics tools - the individual is often not aware of such extrapolation.[31] Data principals cannot reasonably consent to use of data they don't know exists or understand implications of its use.[32]

The PDP Bill 2019 includes inferences drawn from collection of personal data for the purpose of profiling within the definition of personal data.[33] It also includes data about or relating to a natural person, who is indirectly identifiable, under the definition of personal data.[34] As per the report of the Committee of Experts on The Non-Personal Data Governance framework ("NPD Framework"), inferred/derived data is categorised as private non-personal data.[35] The definition of private non-personal data is vague and there seems to be an overlap between the definition of personal data (as per the PDP Bill 2019) and non-personal data, which needs to be resolved[36] for further clarity.[37] This

[31] Alda Yuan, 'Derived Data: A Novel Privacy Concern in the Age of Advanced Biotechnology and Genome Sequencing' [2018] Yale Law & Policy Review <https://ylpr.yale.edu/inter_alia/derived-data-novel-privacy-concern-age-advanced-biotechnology-and-genome-sequencing> accessed 23 November 2020.

[32] ibid.

[33] 'The Personal Data Protection Bill, 2019' (n 25) cl 3(28).

[34] ibid.

[35] Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework 2020' <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf> accessed 22 November 2020.

[36] Jhalak Kakkar and others, 'CCG's Comments to MeitY on the Report by the Committee of Experts on the Non-Personal Data Governance Framework' (2020) <https://ccgdelhi.org/wp-content/uploads/2020/09/CCG-NLU-Comments-to-MeitY-on-the-Report-by-the-Committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>.

[37] 'Report by the Committee of Experts on Non-Personal Data Governance Framework 2020' (n 35).

raises the concern of regulation of DEPA as the data could fall under both the PDP Bill 2019 and the NPD Framework, adding to regulatory uncertainty.

Concerns regarding privacy breaches and profiling conducted using derived data shared via DEPA also make it essential that the framework be clearly laid out before implementation. Developments in big data and Artificial Intelligence along with the increasing availability of diverse and voluminous data sets, and the capacity to link these different data sets, have made it easier to identify individuals by combining seemingly non-personal or anonymised data about them.[38] Additionally, DEPA brings privacy risks related to automated decision making to the forefront. Even the PDP Bill 2019 does not provide for redressal of privacy harms that may arise due to automated decision making.[39] It gives no right to object to such automated processes and the corresponding profiling of individuals and provides for no scrutiny against opaque decision making process of algorithms.[40]

2. Overemphasis on Consent

A. The Consent Model is Flawed

As per the Draft Paper, data sharing will be operationalised by a new type of private entity called “Consent Managers” - an institutional mechanism to manage people’s consent for data sharing. Consent Managers will directly obtain consent from data principals to allow data sharing between IPs and IUs. The Draft Paper envisages that individuals will provide consent as per the ECF. DEPA operates on the traditional permission-based ‘Notice and Consent’ model of data sharing. It seeks to provide data

[38] President’s Council of Advisors on Science and Technology, ‘Big Data and Privacy: A Technological Perspective’ (2014) Report to the President <https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf> accessed 21 November 2020.

[39] Anirudh Burman, ‘Will India’s Proposed Data Protection Law Protect Privacy and Promote Growth?’ (*Carnegie India*, 9 March 2020) <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217> accessed 23 November 2020.

[40] ‘India’s Privacy Law Needs to Incorporate Rights against the Machine’ (*MediaNama*, 28 May 2020) <https://www.medianama.com/2020/05/223-indias-privacy-law-needs-to-incorporate-rights-against-the-machine/> accessed 23 November 2020.

principals with a notice about the IUs' request for data and then obtains consent specific to the duration and purpose of data sharing, elements of data to be shared, and possible third-party sharing.[41]

While the 'Notice and Consent' model forms the core of most privacy regulation, there is increasing consensus among experts that the model is flawed and is not sufficiently equipped to protect user privacy.[42] DEPA assumes that individuals are the best judges of the correct use of their data. However, this assumption is erroneous as individuals cannot exercise consent effectively to make choices due to lack of understanding of how their data will be used.[43] This lack of understanding stems from information asymmetries,[44] cognitive biases,[45] consent fatigue[46] and technological advancements like big data analytics.[47]

B. Information Asymmetry

The 'Notice and Consent' based privacy self-management framework of DEPA functions on the premise that by incentivising the sharing of data with better access to services, users will be empowered in the data economy. It disregards that users are at the disadvantaged end of information asymmetry and might not be fully aware of what they are consenting to. Information asymmetry is a result of amalgamation of various factors discussed below.

[41] 'DEPA' (n 17).

[42] Katherine Kemp, 'Big Data, Financial Inclusion and Privacy for the Poor' (*Dvara Research Blog*) <https://www.dvara.com/blog/2017/08/22/big-data-financial-inclusion-and-privacy-for-the-poor/> accessed 10 November 2020.

[43] Rishab Bailey and others, 'Disclosures in Privacy Policies: Does "Notice and Consent" Work?' [2018] SSRN Electronic Journal 44 <https://www.ssrn.com/abstract=3328289> accessed 10 November 2020.

[44] Gordon Hull, '"Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data"' [2015] Ethics and Information Technology Journal.

[45] Solove (n 7).

[46] Bart Schermer, Custers, Bart and Van Der Hof, Simon, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology.

[47] Solon Barocas and Helen Nissenbaum, 'On Notice: The Trouble with Notice and Consent' 7.

First, users often do not read privacy notices,[48] which are long and difficult to comprehend.[49] Even if they read, they have poor understanding of the implications of these policies. For instance, in a survey conducted to assess the privacy policies of five popular online services in India from the perspective of access and readability, findings suggest that consumers barely understood the terms of the notice before giving their consent.[50]

The complex terms in which privacy policies are formulated is a leading cause of this asymmetry, though proposals to simplify and shorten these notices have also been criticised.[51] The criticism arises from the fact that often when policies are simplified or shortened, important details are left out, as a result of which individuals are not fully aware of the consequences (under the terms of contract or otherwise) of agreeing to share their personal information .[52] While DEPA aims to simplify complex notices, it raises concerns about enabling effective choice. If DEPA relies on obtaining consent in an oversimplified form, for example by clicking a button or signing a paper form, it will not provide for a solution which meaningfully empowers users.[53]

Secondly, privacy warnings are harder to comprehend as they are abstract. Daniel Solove explains this in the following words: “While smoking warnings may be effective because cancer and death are such concrete and terrible consequences, privacy warnings are more difficult to translate into visceral terms because the consequences are much more abstract.”[54] Consent is often given keeping in mind the short term benefits like accessing a website without much consideration to the long term

[48] ibid.

[49] Solove (n 7); Katherine Kemp (n 42).

[50] Bailey and others (n 43).

[51] M Ryan Calo, ‘Against Notice Skepticism in Privacy (and Elsewhere)’ (2012) 87 Notre Dame Law Review.

[52] Solove (n 7).

[53] Rohan Jahagirdar and Praneeth Bodduluri, ‘Digital Economy: India’s Account Aggregator System Is Plagued by Privacy and Safety Issues’ (2020) 55 Economic and Political Weekly <https://www.epw.in/engage/article/digital-economy-indias-account-aggregator-system> accessed 19 November 2020.

[54] Solove (n 7).

cumulative effect of aggregated privacy harm.[55] Even if the notice informs users about the possible future use of the data being shared, an increasing body[56] of research points out to cognitive biases, problems of self-control, and immediate gratification that might impede informed and rational decision making.[57] These biases make an individual take skewed decisions based on immediate impact without taking into account or fully understanding the cumulative risks of data sharing.

Thirdly, technological advancements like big data and data mining have made it possible to draw inferences from seemingly innocuous and unrelated bits of data about a user.[58] Thus, users are at a disadvantage as they are unaware of the ways in which their data can be used in future and its implications. For instance, customers can be offered customised prices or interest rates based on profiles built using their prior purchasing history, social media activity, income, location and neighbourhood, habits and friends.[59] For example, predictions have been made about an individual's personal life like marital status, religion, lifestyle and interests from a list of apps uploaded on their smartphone.[60]

Information asymmetry is structural, and cannot fully be remedied by supplying individuals with more information about sites' privacy policies.[61] Research highlights that more nuanced consent does not necessarily mean better informed consent. For instance in clinical trials it was "unlikely that the informed consent procedure could adequately

[55] Alessandro Acquisti, 'Privacy in Electronic Commerce and the Economics of Immediate Gratification', *Proceedings of the 5th ACM conference on Electronic commerce - EC '04* (ACM Press 2004) <http://portal.acm.org/citation.cfm?doid=988772.988777> accessed 10 November 2020.

[56] Solove (n 7).

[57] Vrinda Bhandari and Renuka Sane, 'Towards a Privacy Framework for India in the Age of the Internet' 58 <https://www.nipfp.org.in/media/medialibrary/2016/11/WP_2016_179.pdf> accessed 19 November 2020.

[58] Wachter and Mittelstadt (n 9).

[59] Katherine Kemp and Ross P. Buckley, 'Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model' (2017) 18 Georgetown Journal of International Affairs.

[60] Suranga Seneviratne and others, 'Predicting User Traits from a Snapshot of Apps Installed on a Smartphone' (2014) 18 ACM SIGMOBILE Mobile Computing and Communications Review 1.

[61] Gordon Hull (n 44).

predict and therefore inform the patient supplying the biological sample of unforeseen future research efforts."[62]

Ultimately, the impediment to exercising effective consent is inbuilt in the 'take it or leave it' model of privacy policies. Users either accept all the terms and conditions outlined in the policy or refuse to accept it and be denied access to the service.[63] Users do not have bargaining and negotiating power to allow only some uses of data being shared and still have access to services.[64] While DEPA aims to reduce the amount of data shared in each instance, it is still based on the same 'all or nothing' model, albeit in an incremental manner, where users cannot exercise a meaningful choice for the fear of losing out on the incentivised benefits like better access to financial or healthcare services.

C. Consent Fatigue

While DEPA aims to achieve granularity and unbundling of consent by seeking user approval before data is shared each time, it overlooks the problem of consent fatigue completely. Consent fatigue is a result of excessive time spent on reading and understanding complex consent notices.[65] Users become desensitised to privacy harms due to overload of and overexposure to information which makes the act of giving consent meaningless.[66] The Justice B.N. Srikrishna Committee Report ("Srikrishna Committee") recognised that consumers suffered fatigue due to excessive consent requirements which desensitised them to privacy harms.[67]

[62] Danielle Hornstein and others, 'More Nuanced Informed Consent Is Not Necessarily Better Informed Consent' (2015) 15 The American Journal of Bioethics 51 <http://www.tandfonline.com/doi/full/10.1080/15265161.2015.1062167> accessed 9 November 2020.

[63] 'Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector (Part–1)' (*Dvara Research Blog*) <https://www.dvara.com/blog/2020/01/06/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-1/> accessed 10 November 2020.

[64] Katherine Kemp and Ross P. Buckley (n 59).

[65] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' [2008] A Journal of Law and Policy for the Information Society.

[66] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection' 17; Schermer, Custers, Bart and Van Der Hof, Simon (n 46).

[67] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' (n 8).

DEPA seeks to establish sectoral consent managers which will require granular consent from users at each instance of data sharing. The Draft Paper does not take into account the adverse impact on users and the resultant consent fatigue that will ensue from proliferation of consent requests from multiple sectoral consent managers.

D. Personal Data Protection Bill, 2019 and Consent

The PDP Bill 2019 relies heavily on consent as a ground for processing of personal data.[68] However, it incorporates several essential data protection principles including data minimisation, purpose limitation, privacy by design, data audits, to ensure robust data protection.[69] The Draft Paper not only relies on consent as the only ground for sharing data, it also does not sufficiently incorporate and emphasise on necessary data protection principles as covered under the PDP Bill 2019. The Draft Paper suggests that consent will not be the only backstop and tools will be developed to prevent over-consent or lack of informed consent, and bring accountability to data controllers. The Draft Paper suggests that a data governance working group led by Sahamati will work with other regulators like the RBI and the proposed DPA for strong data governance in the DEPA framework. However, the Draft Paper does not provide details on how these concerns will be addressed and does not clearly specify the role of the Sahamti in developing these solutions. We recommend that in its current state DEPA framework should not be implemented before the PDP Bill 2019 is enacted and duly implemented. Alternatively we suggest that data protection principles in line with the PDP Bill 2019 should be incorporated in the DEPA framework.

E. Different Standards of Consent

The PDP Bill 2019 provides for different standards of consent for different categories of data like the requirement of 'explicit' consent to process sensitive personal data.[70] In addition to the requirements of processing personal data on the basis of consent of the

[68] 'The Personal Data Protection Bill, 2019' (n 25) cl 11.
[69] ibid, cls 4-10, 22, 29.
[70] ibid, cls 11, 34.

data principal, Clause 11 has some subjective requirements as well. These include: information to data principals regarding *purposes for operations in processing that may have significant consequences for the data principal*; clear and meaningful consent which has not been inferred from conduct; and specific consent with regard *to the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing*.

The DEPA framework does not provide for different standards of consent which may apply to different types of personal data. We recommend that DEPA should not precede the implementation of the PDP Bill 2019 which necessarily requires operationalisation of different standards of consent. Alternatively DEPA should incorporate processes by which different standards of consent mentioned in the PDP Bill 2019 can be effective.

3. Consent Managers

To enable the seamless flow of data from IPs to IUs, based on user consent, the Draft Paper proposes a new type of private institution called — Consent Managers. The primary function of Consent Managers is to allow users to access and share data. The DRAFT Paper claims that these new types of institutions will ensure that individual data rights around privacy and portability are duly protected. In this model of consent management, the flow of consent (i.e. the transaction between users and Consent Managers for providing consent) will be separate from the actual flow of data. Once user consent is obtained, data could flow directly from the IPs to the IUs. The DEPA framework envisages Consent Managers to be data blind in nature. The Draft Paper uses the example of RBI's Account Aggregator model[71] as a Consent Manager.

For the regulation of Consent Managers, the Draft Paper recommends the creation of a self-regulatory organisation, which would be a non-profit collective of - Consent Managers, data providers, and consumers. Similar to the non-profit collective called Sahamati,[72] active in the financial sector.

The PDP Bill 2019 also introduced a new entity in the form of 'Consent Managers'.[73] It defined Consent Managers as data fiduciaries that enabled data principals to gain, withdraw, review and manage their consent through an accessible, transparent, and interoperable platform.[74] According to the PDP Bill 2019, the DPA is empowered to grant and lay down conditions for the registration of Consent Managers.[75] The PDP Bill 2019 provides an option to data principals to exercise their rights of - access, correction and erasure, and portability using the services of a Consent Manager.[76]

[71] 'Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016' (n 3).
[72] 'Sahamati - Collective of the Account Aggregator Ecosystem' (*Sahamati*) <https://sahamati.org.in/> accessed 17 November 2020.
[73] 'The Personal Data Protection Bill, 2019' (n 25), cl 23(5).
[74] ibid, cl 23(5).
[75] ibid, cls 23(5), 94(2)(h).
[76] ibid, cl 21(1), ch V.

The role and function of Consent Managers as proposed under the DEPA framework and under the PDP Bill 2019 is broadly similar, barring a couple of differences. While the PDP Bill 2019 provides that the DPA lays down conditions for the operation of Consent Managers, the Draft Paper recommends that either sectoral regulators, or in certain sectors a self-regulatory approach, be adopted. The PDP Bill 2019, also designates Consent Managers as data fiduciaries,[77] thereby placing all obligations[78] of data fiduciaries on them. The DEPA framework doesn't expressly state whether Consent Managers are data fiduciaries as per the PDP Bill 2019.

As the PDP Bill 2019 will be an overarching central legislation, the Consent Manager framework under DEPA will need to be in compliance with provisions laid down therein.

The concept of Consent Managers, both under the PDP Bill 2019 and the DEPA framework is akin to third-party centralised consent dashboards as recommended by the Srikrishna Committee.[79] The Srikrishna Committee recommended the institutionalisation of consent dashboards to mitigate the challenge of consent fatigue.[80] However, the Srikrishna Committee warned that if consent dashboards were not carefully conceptualised and not made adequately simple, they could become 'expensive white elephants'.[81] The DEPA framework does not lay down how Consent Managers were conceptualised or why they are the most appropriate tools for consent management in India's demographic context.

Challenges with the Consent Manager Model

i. Metadata collection

Although the Draft Paper proposes that Consent Managers will be 'data blind', it does not clarify whether Consent Managers will retain the related metadata of the data

[77] ibid, cl 23(5).

[78] Obligations on data fiduciaries such as purpose limitation, collection limitation; and transparency requirements like privacy by design, security safeguards, and data breach notifications, chs II, VI, ibid.

[79] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' (n 8), ch 3.

[80] ibid.

[81] ibid.

transaction(s) or not. The DEPA framework relies on the ECF for its technology architecture. The ECF uses a consent artifact that is a machine-readable electronic document which specifies the parameters and scope of data sharing for a particular transaction. The consent artifact contains, *inter alia*, information about entities involved in the transaction, the type of data, purpose of the transaction, duration of the storage with the IU, frequency of access, and consent and data flow logs.[82] Additionally, for transactions to be auditable, such logs of information as contained in consent artifacts become necessary. All this information, in addition to any other non-content data collected by Consent Managers such as - date, time, IP address, location, and network particulars, in context of a transaction, may be treated as transaction metadata.[83] Access to such metadata about an individual, might provide Consent Managers with the capability to conduct profiling and gather information which may be considered personal in nature.[84] Metadata provides essential context to digital records and is considered to be inextricably linked to the actual content.[85] Due to this reason, access to metadata can be considered as crucial to the privacy of an individual as the underlying content itself.[86]

ii. Multiple Consent Managers

The Draft Paper proposes the creation and regulation of Consent Managers for each sector separately. It proposes that Consent Managers for regulated sectors, like the financial sector, be created by the respective regulators (for example the Account Aggregator[87] model created by the RBI). For unregulated sectors, the Draft Paper proposes that the DPA manage and certify the creation of Consent Managers. This

[82] 'Electronic Consent Framework, Technology Specifications, Version 1.1' (n 4).

[83] ibid.

[84] Natasha Lomas, 'Stanford Quantifies the Privacy-Stripping Power of Metadata' *TechCrunch* (17 May 2016) <https://social.techcrunch.com/2016/05/17/stanford-quantifies-the-privacy-stripping-power-of-metadata/> accessed 18 November 2020.

[85] Bryce Clayton Newell, 'Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs', *iConference 2014 Proceedings* (iSchools 2014) <https://www.ideals.illinois.edu/handle/2142/47299> accessed 18 November 2020.

[86] ibid; Jonathan Mayer, Patrick Mutchler and John C Mitchell, 'Evaluating the Privacy Properties of Telephone Metadata' (2016) 113 Proceedings of the National Academy of Sciences 5536 <http://www.pnas.org/lookup/doi/10.1073/pnas.1508081113> accessed 18 November 2020.

[87] 'Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016' (n 3).

model of multiple Consent Managers raises concerns of user desensitisation and consent fatigue.

The Srikrishna Committee had recommended the institution of consent dashboards precisely for the reason to mitigate the risk of consent fatigue.[88] But creating multiple Consent Managers across various sectors might have the opposite effect and may lead to user desensitisation with respect to informed consent. The added layer of notice and consent operationalised by the Consent Manager coupled with consent fatigue arising out of multiple Consent Managers and numerous transactions could lead to devaluation of consent.[89] If a regular Indian user will have to navigate multiple Consent Managers, for what could be numerous transactions, there is a fair chance that they may not make an informed decision before providing their consent for data sharing.

iii. Consent Managers and Purpose and Collection Limitation

The PDP Bill 2019 incorporates two essential data protection principles[90] in the form of purpose limitation[91] and collection limitation.[92] These principles restrict data fiduciaries from collecting and processing personal data of data principals, beyond what is necessary.[93] Using the Consent Manager model, data fiduciaries might be able to by-pass purpose and collection limitation requirements, as laid down by the PDP Bill 2019.[94]

For example, if an e-commerce provider wishes to collect the credit and banking history of a user (which it cannot collect in lieu of providing e-commerce services due to purpose limitation), it may request for such information using the Consent Manager model. Users may consent to the sharing of such data under the DEPA model due to a plethora of

[88] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' (n 8).

[89] Jahagirdar and Bodduluri (n 53).

[90] Planning Commission, 'Report of the Group of Experts on Privacy Constituted by the Planning Commission of India, Chaired by Justice A P Shah' (2012) <https://www.dsci.in/sites/default/files/documents/resource_centre/Report%20of%20the%20Group%20of%20Experts%20on%20Privacy%20constituted%20by%20Planning%20Commission%20of%20India.pdf> accessed 19 November 2020.

[91] 'The Personal Data Protection Bill, 2019' (n 25), cl 5.

[92] ibid, cl 6.

[93] This is based on the principles of Notice and Consent, ibid, cls 7, 11.

[94] Jahagirdar and Bodduluri (n 53).

reasons —consent fatigue, information asymmetry, or desensitisation to privacy risks (see section 2). Once the e-commerce provider gets access to a user's credit and banking history, it might combine this with data collected on its own and target such users with certain products and services with attractive financing options. This would essentially render the protections of purpose and collection limitation futile. The Draft Paper does not consider or explain frameworks for the mitigation of such risks.

iv. Information Providers/ Users as Consent Managers

Although the Draft Paper states that Consent Managers will be independent entities, it doesn’t clarify whether they could be subsidiaries or owned by IPs or IUs. For example, in the Account Aggregator model, Jio Information Solutions Limited[95] has gotten an in-principle approval from the RBI to operate its own Account Aggregator.[96] If permitted, this might lead to data mining, profiling, and targeting, impacting the privacy of users. As discussed (see paragraph i)), Consent Managers will have access to detailed metadata of each transaction that they administer. Combining this detailed metadata with information already available with IPs and IUs, may lead to the risk of user profiling and targeting without the knowledge of the users. To avoid such risks, it is essential that Consent Managers be considered data fiduciaries as per PDP Bill 2019,[97] which is not expressly stated by the DEPA framework.

v. Incentives for Information Providers

Another risk to the success of the Consent Manager model is the lack of incentives for IPs to share data.[98] Especially if sharing such data will impact the revenue or business of an IP or the data sharing request is by a direct competitor.[99] For example, if a bank is requested for data on the banking history of an individual to assess their credit

[95] Sahamati, ‘Account Aggregators in India’ <https://sahamati.org.in/account-aggregators-in-india/> accessed 19 November 2020.

[96] Jio is one of India’s largest mobile network providers, ‘Reliance Jio’ <https://www.jio.com/en-in/jio-life> accessed 30 November 2020.

[97] ‘The Personal Data Protection Bill, 2019’ (n 25), cl 23(5).

[98] Jahagirdar and Bodduluri (n 53).

[99] ibid.

worthiness for a loan approval, the bank will not be incentivised to share such data if they offer loan services themselves. Similarly, this could also lead to large conglomerates, who offer services pan-industry, to lock-in consumers in their own ecosystem, based on requests they receive for data sharing under the DEPA.

vi. No proof of concept

The DEPA framework does not offer any proof of concept of the Consent Manager model. Even the Account Aggregator model instituted by the RBI in 2016, has only 7 applicants yet.[100] Since Consent Managers will be privately owned entities, what will be their business model for sustenance? The DEPA framework recommends that Consent Managers may facilitate data exchanges by charging a 'nominal fee' to IUs rather than data principals/ users. The framework also recommends that IPs may charge a service fee in the future. The success and sustenance of Consent Managers thus depends on the volume of transactions along with the capacity and inclination of IUs to pay for access to data.

The DEPA framework also operates on the principle of reciprocity, that is - IUs will need to adopt technology standards required to become IPs too. But the enforcement of this mandate might be difficult unless incorporated into law or enforced by a regulator.

The Draft Paper must clarify how the Consent Manager model is the best possible way of empowering users or data principals in India's data sharing economy. It must also engage with other models of data governance, sharing and empowerment being explored globally such as - Open Data Institute's[101] Data Trusts project or Mozilla's Data Futures initiative.[102]

[100] There are 4 AAs with an operating license and 3 with an in-principle license, Sahamati, 'Account Aggregators in India' (n 95).

[101] 'R&D: Can Data Trusts Increase or Help Data Sharing? – The ODI' <https://theodi.org/project/data-trusts/> accessed 19 November 2020.

[102] 'Data Futures - Research to Shift Power through Data Governance' (*Mozilla Foundation*) <https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/> accessed 19 November 2020.

4. Government entities as Information Users and Providers

A. As Information Users

While the DEPA framework has been designed with the objective of making it easier for data principals/ users to access products and services (for example, financial, health and telecom), it is not clear whether government agencies could become IUs under DEPA. Governments have sufficient powers under law to perform targeted surveillance and intercept digital communication in India for reasons of law enforcement.[103] Additionally, the PDP Bill 2019 gives wide powers to both Central and State Governments[104] to process data without the consent of data principals for law enforcement purposes. The PDP Bill 2019 also empowers the Central Government to request data fiduciaries for any non-personal data for the purposes of service delivery or policy making.[105] But it remains unclear whether governments could request access to data as IUs making use of the DEPA framework for reasons beyond law enforcement and in lieu of providing certain services to users.

The relationship between a citizen and the State is not of equals and in several situations the imbalance of power between them would affect the validity of consent given for sharing of data.[106] Therefore, consent becomes even more meaningless when the State requests for certain personal data. Privacy is also a fundamental right[107] enjoyed by citizens against the State and it is well settled law in India that fundamental rights cannot be waived by citizens.[108] Any State actions to collect personal data of citizens, by means of contract (using consent as a metric), would only be legitimate if sufficient safeguards are provided to protect the right to privacy and the social/ public interest in data collection outweighs the particular aspect of privacy.[109]

[103] The Information Technology Act 2000, s 69.

[104] ‘The Personal Data Protection Bill, 2019’ (n 25), cls 35, 36.

[105] ibid, cl 91.

[106] ‘A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna’ (n 8).

[107] ‘Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1 (Puttaswamy)’ (n 6).

[108] R.F. Nariman, J., ibid.

[109] ibid.

The DEPA framework must clarify that its main purpose is to help provide users timely and quality services. Government agencies must not use this architecture to gain access to data about citizens, purely based on consent.

B. As Information Providerss

The DEPA framework envisages government agencies/ departments to become IPs in the form of Government Information Providers ("GIP"). It states that the first government department to become a GIP will be GST. This raises several privacy risks —firstly, the State collects large amounts of personal data from citizens to not just provide services and benefits, but to also perform its regulatory functions.[110] Secondly, such data is shared by citizens with the expectation that it is essential for the State to perform its functions and under the influence of a skewed balance of power (as noted earlier).[111] Thirdly, the State is under an obligation to protect such data and the privacy right attached to it as informational privacy is a fundamental right enjoyed by citizens.[112] Lastly, as users are not the best judges of their privacy rights, sharing such data based on consent with private entities may have a significant impact on the privacy rights of citizens.

[110] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' (n 8).
[111] ibid.
[112] 'Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1 (Puttaswamy)' (n 6).

5. Different Approaches to Data Governance and Data Sharing

As data becomes increasingly valuable to both business and governments alike, it is essential to move away from a regime where the controllers of data are the sole decision makers on its use and governance.[113] To bring back meaningful autonomy in the hands of users, data governance models that empower them to make better decisions and fix the imbalance of power between users and data processors will need to be developed .

This is essentially what the DEPA framework sets out to achieve. But the pertinent question is how can a data governance or data sharing model empower users while ensuring privacy, security, and a transition in the power balance.[114]

To tackle these challenges in our data economy, recent scholarship on data governance has proposed the concept of data stewardship.[115] Data stewardship is a model wherein an intermediary navigates consent and decision-making on behalf of users.[116] Data stewards are also responsible for ensuring data is able to generate societal value, and maintain the security standards and quality of datasets.[117] Data stewards function on behalf of users, typically in a fiduciary capacity or with an implied guidance towards achieving a determined societal goal.[118] The data stewardship model empowers users without placing the entire onus on a single individual to make decisions of the governance of their data.

There are various models of data stewardship, but these are primarily in theory, without large scale instances of practical application.[119] It will be useful to consider some of these

[113] Siddharth Manohar, Astha Kapoor and Aditi Ramesh, 'Understanding Data Stewardship: Taxonomy and Use Cases' (Aapti Institute) <https://uploads.strikinglycdn.com/files/64aa4010-6c11-4d6f-8463-efaed964d7d9/Understanding%20Data%20Stewardship%20-%20Aapti%20Institute.pdf> accessed 20 November 2020.

[114] Due to the DEPA framework's over-emphasis on consent, meaningful autonomy and control over data sharing or data flow might not be achieved. The DEPA framework also doesn't acknowledge the power imbalances and information asymmetries between users and data processors, which may not get solved by relying completely on user consent.

[115] Manohar, Kapoor and Ramesh (n 113); 'Data for Empowerment' (n 15).

[116] Manohar, Kapoor and Ramesh (n 113).

[117] ibid.

[118] 'Data for Empowerment' (n 15).

[119] ibid.

models while developing a new data governance or data sharing architecture. Some of the popular data stewardship models are:[120]

A. Data Trusts

Recently, data trusts have been recognised by several scholars as a promising model of data stewardship. A data trust is a legal relationship where a trustee stewards or navigates data rights for the benefit of the user or a group of users (in the form of beneficiaries). In this model, the trustee is bound by law to act in a fiduciary duty for the sole benefit of the users (predetermined conditions, decided while entering into the trust relationship).

This model is promising as trustees may be in a better position (due to their knowledge or expertise) to make decisions on behalf of users, and are bound by law to act in the best interest of the users as well.

B. Data Cooperatives

A data cooperative is a legal construct to facilitate the pooling of data contributed to by individuals or organisations for the economic, social, or cultural benefit of a group. The entity that holds the data is often co-owned and democratically controlled by its members.

C. Data Commons

Data commons is a concept, where data is pooled and shared as if a common resource. A data commons is based on a high level of community ownership and is often associated with a public good. Such a model may address the power imbalances in the data economy, by democratizing access to and availability of data.

[120] ibid.

D. Data Collaborative

In a data collaborative, private sector data is generally combined to help assist in public sector decision making. Data in a collaborative could be shared strictly between partners, with an independent third party who manages access to the data, or publicly online.

As noted earlier, though these models are mostly theoretical and might need adaptation for India's unique demographic and legal landscape, it may be beneficial to explore these models before proposing a comprehensive data sharing framework. Currently the Draft Paper does not lay down how the DEPA framework or the Consent Manager model may be the best suited solution for a new data sharing or data governance architecture. Adapting a model which may be suited for the financial sector (which is a highly regulated sector with a powerful regulator), may not be the best solution for all other sectors. This may be even more challenging without the enactment of a data protection legislation and a regulator in the form of the DPA.

6. Different Timelines for DEPA and the PDP Bill 2019

DEPA must address data protection and privacy concerns that flow from its proposed data sharing mechanism. In Puttaswamy the Supreme Court while reaffirming the right to privacy as a fundamental right elaborated on both the positive and negative obligations of the State.[121] As a data governance framework DEPA fails to fulfill its foremost requirement of providing privacy protections before enabling expansion of data flows in the hands of State and non-State actors. It is proposed that DEPA will comply with the requirements of the PDP Bill 2019, however the timelines for implementation of PDPB and DEPA do not coincide.

DEPA is envisaged to operationalise much before the PDP Bill 2019 becomes a law and is duly implemented. The absence of a robust data protection law makes data sharing as per DEPA, which involves both private and public entities, at risk of violating the mandate established by *Puttaswamy.*

Thus, the implementation of DEPA should not precede that of a comprehensive data protection law. In the alternative, if the DEPA framework is implemented, it must incorporate all data protection principles adopted by the PDP Bill 2019.

[121] 'Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1 (Puttaswamy)' (n 6).

Conclusion

In Puttaswamy, the Supreme Court clarified that communicational and informational privacy were important subsets of the overall right to privacy of an individual.[122] The Court also laid down that control and autonomy were essential facets of the right to privacy[123] and such a right needs to be protected from both State and non-State actors.[124]

India's draft data protection bill, the PDP Bill 2019, doesn't provide sufficient provisions for operationalising user control and autonomy. The PDP Bill 2019 has a number of exceptions for processing of personal data without the consent of the user, gives wide powers to the government for processing data without intimating users, and does not institute an independent regulator for fair adjudication.

Recently, the government has also proposed a non-personal data framework which proposes the creation of various new stakeholders in India's data economy for example, data custodians, data trustees, and a new regulatory structure in the form of a Non-Personal Data Regulatory Authority.[125]

With the PDP Bill 2019 and the NPD Framework, India's data governance model is fairly complex and still does not provide for institutionalising user control or autonomy over the processing of their data. The introduction of DEPA further complicates this complex structure. Though the DEPA framework states that it will be in compliance with the PDP Bill 2019, the timelines for the two frameworks do not coincide. The PDP Bill 2019 is currently pending review before a joint parliamentary committee, but the Draft Paper states that the public launch of the DEPA framework will be sometime in the end of 2020. The Draft Paper does not clarify how the DEPA framework will be in compliance with

[122] ibid Dr D Y Chandrachud, J., [142].

[123] ibid, Dr D Y Chandrachud, J., [141], [142], [168].

[124] ibid, Dr D Y Chandrachud, J., [185.

[125] MeiTY, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' <https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf> accessed 14 September 2020.

India's data protection law before the PDP Bill 2019 is passed as law by India's parliament.[126]

To fix the current challenges in the data economy, wherein users do not have a choice but to give consent to the data collection practices of various online services,[127] a data governance framework needs to empower users while giving them meaningful choice and autonomy. Although the DEPA framework attempts to do this, it over-emphasises on the usefulness of consent to empower users (see section 2). It doesn't engage or acknowledge various other models of data governance being devised in global scholarship which also attempt at empowering the average users.[128]

Lastly, the usefulness of a public consultation on a data sharing or governance model that is already in existence in the financial sector[129] and is touted to go live soon becomes moot. The government must conduct public consultations on policy proposals at the nascent stage of development for meaningful feedback. Additionally, the DRAFT paper acknowledges the efforts of an independent think tank, without demonstrating if the NITI Aayog consulted with other stakeholders before finalising the DEPA framework.

[126] The DEPA framework does not incorporate a number of data protection principles in the PDP Bill, 2019 such as purpose limitation and collection limitation.

[127] 'Data for Empowerment' (n 15).

[128] ibid.

[129] 'Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016' (n 3).