Rethinking Data Exchange & Delivery Models

Principles for Privacy Preserving Data Sharing in Digital Governance

31 March, 2021

By **Pallavi Bedi** and **Amber Sinha**

Edited and inputs by **Ambika Tandon**

Infographics and document design
by **Saumyaa Naidu** and **Akash Sheshadri**

The Centre for Internet and Society, India

Executive Summary

In 2020, reports of the government's proposal to create a social registry to update the Socio Economic Caste Census 2011 data started surfacing. Based on the limited information around these proposals in the public domain, it is imperative that adequate consideration be provided to develop such systems in a manner that protects the informational privacy of the individuals. Currently, the proposed Personal Data Protection Bill, 2019 is being deliberated by the Joint Parliamentary Committee and is expected to be tabled in the Monsoon Session of Parliament. The proposed data protection framework is a marked improvement over its predecessor, Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011. One substantial change in the context of welfare delivery is that the scope of the application of the proposed framework extends to the personal data processing by the government and its agencies.

The objective of the white paper is to examine the application of the proposed data protection provisions on such a welfare delivery model (data exchange and delivery model) and suggest ways to operationalise key provisions. The scope of this white paper is limited to examining the personal data implications of the model and the effective governance of such platforms in India. The paper relies on publicly available details of India's and other selected countries (Indonesia, Brazil, China, Malawi, Kenya, Estonia) digital infrastructure, proposals, schemes and legal frameworks in relation to welfare delivery in the country. International best practices around implementation of the principles of privacy and openness are analysed to suggest methods to operationalise these requirements in the context of the data exchange and delivery models and the proposed data protection framework of the country.

Based on the global experience of implementing data exchange and delivery models and the best practices for implementation of data protection provisions, following are some of the key recommendations (in addition to discussing ways to operationalise the data protection provisions) for such a platform in the Indian context:

- **Application of Data Protection Legislation:** Due to the sensitive processing of personal data accompanied with harms arising from unlawful surveillance, such a data exchange and delivery model should not be deployed without an overarching data protection legislation. It is vital that the application of the legislation extends to the model. The Data Protection Authority of India should be able to exercise its investigative, corrective and advisory powers over the functioning and management of the model.

- **Independent Regulator:** Oversight over the functioning of the platform should not be vested with the agency that is responsible for the maintenance of the platform to address potential conflict of interest issues. Additional sub - committees based on subject matter expertise for each individual scheme can be set up to assist the regulator, if required. The independent regulator should have strong investigative, corrective and advisory powers for effective oversight over the activities of the platform. Enforcement actions of the regulator should be transparent.

- **Governance:** The data fiduciary responsible for the management and operation of the data exchange and delivery platform should be clearly identified. The platform should have valid legislative backing. In case of involvement of private actors, additional safeguards related to the privacy and confidentiality of the data in the platform should be implemented.

- **Data Protection Authority of India and Platform:** There should be clear channels of communication between the data protection authority of India and the data fiduciaries managing and accessing the platform for guidance on data protection issues.

- **Grievance Redressal Mechanism:** An accessible grievance redressal mechanism should be set up at different points of the service delivery and their existence should be publicised through different mediums. As the platform can act as a single point of failure for multiple schemes, an integration of the redressal mechanisms across multiple schemes should be considered based on existing institutional structures. Multiple channels for receiving complaints must be set up for the citizen's convenience.

Introduction

Across the world, there has been a significant push towards harmonising information systems that enable effective service delivery of social welfare schemes. To function effectively, such information systems, or "social registries," contain sensitive personal data of citizens, and cover as much of the population as possible. In the absence of strong privacy and security measures, these social registries have been criticised for acting as tools for mass surveillance, while masquerading as monitoring and evaluation systems for poverty alleviation programmes; and have been seen as a possible threat to civil liberties. In addition, the one-stop nature of registries and their use for multiple welfare schemes magnifies their potential for exclusion.

With social registries becoming the norm[1], it is pivotal to devise methodologies that lead to the creation of privacy-respecting information systems, and this white paper is an attempt to do that. The research objective of the white paper is to locate the proposal of creating a welfare delivery model based on a social registry within the existing and proposed data protection framework of India. The white paper suggests ways in which the provisions of the framework may be operationalised while taking into consideration key challenges that arise in the Indian context. In doing so, it will examine existing initiatives in the Indian context, relevant literature, and examples of similar platforms from other jurisdictions. The primary question of whether such a platform is necessary in the Indian context and the alternatives to such a platform is out of scope for the paper including subjects such as design of eligibility criteria for social welfare programmes, and their management. The scope of this white paper is limited to the question of effective governance and personal data protection implications of the use of such platforms in India.

The terminology[2] used to refer to these integrated information systems is dependent on the nature of the system, their function, population coverage etc. Since the objective of the white paper is merely to identify the personal data protections provided to data principals of those systems, the relevance of the type of integrated information system for the purposes of the white paper is negligible. Hence, this whitepaper will use the term "data exchange and delivery models" to refer to the information systems instead.

To set the context, this paper compiles the publicly available details of proposals, schemes and legal frameworks in relation to welfare delivery in the country. A comparative research of the data exchange and delivery models of the selected countries[3] has been conducted which includes a technical analysis of the architectural designs of these models and the underlying

[1] Phillippe Leite Tina George Karippacheril, Changqing Sun, Theresa Jonesand Kathy Lindert, "Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool", July 2017, http://documents.worldbank.org/curated/en/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf

[2] Refer to annexure

[3] Indonesia, Malawi, Kenya, China, Brazil, Estonia . These countries were selected to represent diversity in the regulatory frameworks and architectural designs of the registries.

legal and governance frameworks that enables lawful implementation of the welfare delivery. International best practices around implementation of the principles of privacy and openness are analysed to suggest methods to operationalise these requirements in the context of the data exchange and delivery models and the proposed data protection framework of the country.

Data Exchange Platforms in India

Context Setting

A timeline of relevant events starting from the establishment of the Unique Identification Authority of India in 2009 to the notification of the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020 has been provided in the chart below:

Timeline of Events

2009

Establishment of UIDAI

The UIDAI was established to issue Aadhaar numbers to persons residing in India. Seeding of Aadhaar with the beneficiary data has been made compulsory under certain welfare schemes, including the Pradhan Mantri Kisan Samman Nidhi Yojana.

2011

Carrying out of SECC

The Central Government conducted a comprehensive Socio-Economic and Caste Census ("SECC") in India, to replace the existing below-the-poverty line list to identify beneficiaries for government welfare programmes.

2016

Recommendation for Social Registry

The SECC report was published in 2015, and an Expert Committee ("Committee") was constituted. The Committee recommended that SECC data should be used as the basis for the creation of a social registry comprising information about the beneficiaries of the social security programme of the government.

2018

Strategy Paper on National Health Stack

The Niti Aayog released a strategy and consultation paper on the National Health Stack. It envisages the creation of a unique ID for registered beneficiaries in the system — a 'Digital Health ID'.

March 2020

Release of Whitepaper on the National Open Digital Ecosystem (NODE)

MEITY released a white paper seeking comments on the National Open Digital Ecosystem (NODE). It describes the evolution of government technology in a three step process; automation and digitisation of public records, end to end service delivery, and 'shared, interoperable digital delivery platform.'

Also, several news reports described the government's plans to create a "single, searchable Aadhaar-seeded database, or 'multiple harmonised and integrated databases' that use Aadhaar numbers to integrate religion, caste, income, property, education, marital status, employment, disability and family-tree data of every single citizen."

August 2020

Notification of Aadhaar Authentication for Good Governance

In August 2020, Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020 were notified. As per the rules, the Central Government has permitted the voluntary use of Aadhaar authentication by requesting entities for "usage of digital platforms to ensure good governance" and "prevention of dissipation of social welfare benefits."

Existing Regulatory Frameworks

The current data protection framework of India consists of the requirements mentioned under Section 43A of the Information Technology Act, 2000 (**IT Act**) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**SPDI Rules**). These requirements are applicable only to those organizations that fall within the restrictive definition of body corporates, i.e. organisations engaged in commercial or professional activities[4], which excludes government agencies.

After unanimously holding the existence of a fundamental right to privacy under the Indian constitution, the lead judgment in Puttaswamy v. Union of India[5] held that a law that limits the right to privacy of the individual will have to "withstand the touchstone of permissible restrictions on fundamental rights." A threefold requirement consisting of the legality of law in question, a defined legitimate state aim and proportionality of the objects and means adopted to achieve the aim had been laid down.

Subsequent to the declaration of right to privacy as a fundamental right, the five judge bench [6] had to determine whether the Aadhaar Act posed a reasonable restriction on the privacy of individuals based on the proportionality test set by the nine judge bench of the Supreme Court. Based on the proportionality test, the Supreme Court struck down the provision of the Aadhaar Act that enabled government entities, body corporates and individuals to use the Aadhaar number for establishing the identity of an individual for *any purpose* based on a contract. As a result, private entities are barred from using Aadhaar based authentication services to curb potential commercial exploitation of an individual's biometric and demographic information by private entities. Any future database linkages with the Aadhaar database will have to stand the scrutiny of the reasonableness standard set in the Puttaswamy judgment.

The Personal Data Protection Bill, 2019 (**Bill**), which is an improvement over the current data protection framework, has been sent to a joint parliamentary committee for further deliberations. The Bill has requirements addressing many of the globally accepted privacy principles i.e. notice, choice and consent, purpose limitation, storage limitation, collection limitation, data security and privacy by design. Extending the application of the requirements under the legislation to government agencies is a noteworthy improvement from the current data protection framework.

The term data fiduciary and data processor have been introduced where the former is used to represent persons or entities which determine the purpose and means of processing

[4] Section 43A Information Technology Act, 2000
[5] K.S. Puttaswamy (Retd) v Union of India (2018) 10 SCC 1
[6] (2019) 1 SCC 1

personal data and the latter is used to represent those persons or entities that process personal data on behalf of the data fiduciary. Personal data has been defined to include data that can directly or indirectly identify a natural person whether online or offline including a combination of features with any other information. For the purposes of this white paper, it is important to note that official identifiers[7] such as Aadhaar numbers have been classified as sensitive personal data.

Conditions necessary to use consent as a lawful ground of processing have been clearly laid out. For the purposes of this white paper, it is important to note that the State can process personal data without consent for the purposes of providing any service or benefit to the data principal from the State only if such functions of the State have been authorised by law[8]. The Bill provides the data principal with the right to access, correct, delete and 'port' their personal data from the data fiduciary.

The Bill calls for constituting an independent Data Protection Authority (**DPA**) which is tasked with specific investigatory, corrective and advisory powers to ensure compliance with the provisions of the Act. The DPA also has the power to classify data fiduciaries as significant data fiduciaries based on the volume of data being processed, sensitivity of the data, risk of harm to the data principal, turnover of the data fiduciary, use of new technologies for processing and other factors that can result in harm to the data principal. These significant data fiduciaries have additional obligations of appointing data protection officers, conducting data protection impact assessments, maintaining records and carrying out annual audits by independent auditors. Since the application of the Bill extends to personal data processing by government agencies, it would be reasonable to assume that the DPA's investigative, corrective, advisory powers along with the power to classify data fiduciaries as significant data fiduciaries would extend to the data exchange and delivery model. At this point, it would be difficult to accurately predict if this model will be classified as a significant data fiduciary.

The Bill requires all data fiduciaries to prepare a privacy by design policy comprising details of their privacy governance program. The policy can be submitted to the DPA for certification subject to the regulations made by the DPA. In the event of a personal data breach, the data fiduciary is required to inform the DPA in the manner prescribed and inform the data principal on the guidance of the DPA.

[7] Section 3(36), Personal Data Protection Bill,2019
[8] Section 12(a), Personal Data Protection Bill, 2019

Challenges and Concerns with Social Registries

The Ministry of Rural Development had proposed the idea of creating a national social registry based on the SECC with the objective of ensuring better management of the social protection schemes in the country[9]. Documents obtained through the Right to Information Act [10] indicate that the data collection is not limited to potential welfare beneficiaries, but may be extended to all households in the country. Establishing a registry with the sole purpose of enabling efficient service delivery of benefits under welfare programs can be considered a legitimate state objective. However, in the absence of a framework with clear governance structures, data access protocols and grievance redressal systems, these systems can end up causing the citizens more harm than good. These harms can range from risks associated with the possibility of unauthorised access to personal data and exclusion errors to mass surveillance on the general population. Few of the concerns are as follows:

Function Creep

A key prerequisite is deciding the clear and specific purpose before initiating plans to design the system. In the absence of clear and documented purpose the potential for function creep is extremely high, especially in the absence of a data protection legislation[11].

Exclusion Errors

Since these systems are intended to integrate the registration process for multiple welfare programs, improper data collection methods can exacerbate the exclusion issues as any mistake can exclude the citizen from receiving services of multiple schemes. Data collection solely on the bases of on demand registrations or census based surveys have proven to be untrustworthy[12]. As most of the welfare programs target households based on income, frequent updation of these records to account for the ever changing statuses of family has to be built into the design of the registry.

[9] Kumar Sambhav Shrivastava “Exclusive: Documents show Modi Govt Building 360 Degree database to track every Indian “ Huffpost, March 17, 2020 https://www.huffingtonpost.in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462

[10] National Social Registry with respect to Socio economic and caste census 2011 , Ministry of Rural development https://ia903102.us.archive.org/14/items/social_registry/social_registry.pdf

[11] Vijayta Lalwani, “Delhi BJP is gathering data on welfare scheme beneficiaries for 2019 polls”, *Scroll.in*, January 10, 2019 https://scroll.in/article/908215/delhi-bjp-is-gathering-data-on-welfare-scheme-beneficiaries-for-2019-polls-is-it-a-cause-for-worry

[12] Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary registries Australian Government, Department of Foreign affairs and trade (October 2017) https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf

Technology Gaps

Apart from acting as a single window for registration purposes, the data in these registries is also relied on for eligibility determination and subsequent service delivery. Any failures in the operational or administrative aspects of the registry can bar the citizen from receiving what is rightfully theirs. Brazil's Cadastro Unico database faced connectivity issues in certain parts of the country that could have impacted service delivery as the entire system was managed online[13]. In India, the technology failures of the Aadhaar based authentication procedures due to biometric authentication issues, server and connectivity issues resulted in the failure of ration delivery[14]in some cases. Before moving the entire system online, a detailed understanding of not just the technology options at the Centre but the availability of similar options at the exact point of service delivery is necessary. Authentication based on an offline card based option could be one way to address technology gaps.

Lack of Redress

Most of the challenges of social registries correspond to the registry acting as a single point of failure for the implementation of social welfare schemes. Harm mitigation strategies of other countries that have implemented any form of an integrated registry have highlighted the importance of grievance redressal systems. In the absence of an effective and accessible redressal system, the entire objective of the registry of enabling efficient delivery of welfare schemes will be rendered moot. Due to the automated nature of the proposed service delivery system, human interface at point of delivery is highly essential to ensure that the system remains citizen friendly[15].

[13] Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary registries Australian Government, Department of Foreign affairs and trade (October 2017) https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf

[14] Reetika Khera, "Impact of Aadhaar on welfare programs" 52 *Economic and Political Weekly* (2017)

[15] Schemes to systems| The Solutions State: Complementing Digital and Human Resources, World Bank, March 15, 2019, https://www.worldbank.org/en/news/feature/2019/03/15/schemes-to-systems-digital-human-resources

Global Experience

Overview

There are four arrangements[16] for managing and operating social registries which are being employed by different countries, namely, (i) Managed and operated by a central social agency (for eg. Azerbaijan, Chile, Turkey), (ii) Managed by Central Social Agency with separate operating agency (for e.g, Brazil, Mali and Montenegro); (iii) Managed and Operated by other central agency (for e.g. Indonesia's UDB); and (iv) Managed and operated by specific program (for e.g. Pakistan).

For the purposes of analysis, the social registries of Indonesia, Malawi, Kenya, Estonia, Brazil and China were examined. These countries were selected to represent the diverse architectural, regulatory and data collection frameworks currently implemented. Furthermore, the selection of countries was also dependent on the availability of reliable publicly available information regarding functioning of these registries. Key questions related to the architecture of the information management systems, role of openness in the design of the systems and regulatory frameworks around privacy were assessed to determine if a similar system can be implemented in the Indian context.

Lessons Learned

Database Management

The option of choosing between centralised and decentralised systems is heavily dependent on the nature of institutional structures in place i.e. the nature of centralized oversight of the social protection programs, if any, and the ability of the local government to maintain their own databases in addition to implementing service delivery. In China, local governments manage their own registries in a decentralised manner, despite a centralised accumulation of data[17]. The lack of coordination between the local government in determining the thresholds for targeting leads to differential treatment across different districts[18]. Estonia's X-Road is the

[16] Phillippe Leite Tina George Karippacheril, Changqing Sun, Theresa Jonesand Kathy Lindert, "Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool", July 2017, http://documents.worldbank.org/curated/en/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf

[17] Phillippe Leite Tina George Karippacheril, Changqing Sun, Theresa Jonesand Kathy Lindert, "Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool", July 2017, http://documents.worldbank.org/curated/en/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf

[18] Nanak Kakwani et al , "Evaluating the effectiveness of the rural minimum living standard guarantee(Dibao) programme in China". *University of Manchester Global Development Institute,* August 2016 https://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/GDI/GDI_WP1822_Wang.pdf

truest to the form of decentralization as there is no centralised accumulation of data and X road merely provides the interoperability needed for the agencies to function[19]. However, the socio-economic and demographic conditions[20] necessary for the successful implementation of a data exchange layer like X-Road may be difficult to duplicate in the Indian context. The other option is to centralise the control of the registry while delegating the implementation to the local level of the government similar to the system in Brazil, where the responsibilities are shared between the federal government, states, federal districts and municipalities[21].

Considering the multiple welfare schemes and the number of beneficiaries across the country, a decentralised delivery model may be adopted in India. Under such a mechanism, the State Government authorities and the district level officers will be responsible for linking the welfare schemes with the delivery exchange model at the local level and an agency/department at the central level will be responsible for overseeing the overall effective implementation of the delivery exchange model. However, an in-depth analysis of the existing technical capabilities at the Centre and State level is essential before implementing the system. Possibility of implementation of different models based on technical capacity at State level should not be ruled out.

Oversight

In Brazil[22] there is a division between the Ministry of Social and Agrarian Development and the Public bank wherein the former is the host managing agency and the latter has been hired via a performance contract to act as the operating agency.
It has been suggested that the agency responsible for managing the registry be independent from the individual agencies that actually manage the social welfare programs. [23] Apart from the fact that independence can lead to better oversight, the agencies that are responsible for managing the individual social welfare programs might not have the technical or subject matter expertise needed to manage and coordinate the programs. [24] Kenya's Social Protection Secretariat was established to "facilitate the integration, coordination and harmonization of

[19] Uuno Vallner, "Secure data exchange platform. Principles and implementation X-Road", *Scoop4c.eu* (December 12, 2017) https://scoop4c.eu/sites/default/files/2018-03/Overview-of-Secure%20Data-Exchange-X-Road-6.pdf
[20] Meelis Kitsing, "An Evaluation of E-Government in Estonia."*Oxford Internet Institute Blogs*, September 2010 http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/IPP2010_Kitsing_1_Paper_0.pdf
[21] Unified registry, World without poverty, (2015) https://wwp.org.br/en/social-policy/unified-registry/
[22] Phillippe Leite Tina George Karippacheril, Changqing Sun, Theresa Jonesand Kathy Lindert, "Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool", July 2017, http://documents.worldbank.org/curated/en/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf
[23] Valentine Barca and Richard Chichir, "Single registries and integrated MISs: De-mystifying data and information management concepts", *Oxford Policy Management*, (May 2014) https://www.opml.co.uk/files/2018-05/barca-chirchir-2014-data-information-management-social-protection.pdf?noredirect=1
[24] Supporting Social Protection Systems, Directorate-General for International Cooperation and Development European Commission (September 2015) https://europa.eu/capacity4dev/public-employment-social-protection/documents/concept-paper-supporting-social-protection-systems-devco-2015-0

social protection programmes in Kenya"[25] and is tasked with performing certain core functions despite being housed under the Ministry of Labour, Social Security and Services which is responsible for fulfilling the social protection mandates. [26] It is recommended that a similar authority be set up with clear indication of its technical and subject matter expertise to perform the core functions required to maintain a registry.

Role of Openness

There is a higher emphasis on open standards and open source code in Malawi[27], Kenya[28], Estonia[29]. The high costs of making changes in proprietary software and the ever-present risk of vendor lock in make the flexibility and autonomous system management offered by open source software a better choice.

[25] "About us", Social Protection Secretariat ,last accessed August 30, 2020 https://www.socialprotection.or.ke/about-sps/social-protection-secretariat

[26] "Introduction to Social Protection", Social Protection Secretariat, last accessed August 30, 2020 https://www.socialprotection.or.ke/about-sps/introduction-to-social-protection

[27] Kathy Lindert et al. "Rapid Social registry assessment: Malawi's Unified Beneficiary Registry " *World Bank*, November 2018, http://documents.worldbank.org/curated/en/363391542398737774/pdf/132144-NWP-P162379-Rapid-Social-Registry.pdf

[28] Program appraisal document on a proposed credit to the Republic of Kenya for a national safety net program for results, World Bank, June 26, 2013, documents.worldbank.org/curated/en/500691468273333320/pdf/782940KE0PAD0I00Box0377356B00OUO090.pdf

[29] Helen Margetts and Andre Naumann, "Government as a platform: What can Estonia show the world?" *Oxford Internet Institute,* February 28, 2017 https://www.politics.ox.ac.uk/materials/publications/16061/government-as-a-platform.pdf

Data Protection Frameworks

Kenya, Brazil and Estonia have specific data protection laws which include provisions related to data sharing, security measures, privacy notice etc. In Brazil[30], electronic access to the database is provided to those public or private institutions that are legally responsible for the implementation of the social protection schemes. Institutions that are not involved in the implementation of the schemes, but require access to the database need to submit a formal enquiry to the Ministry of Social Development. In Indonesia[31], to obtain access to the database ministries or local governments send written requests to the Ministry of Social Affairs detailing the type of data needed. Data that is considered sensitive is only shared with other government institutions upon request.

The application of People's Republic of China Cybersecurity law (CSL) extends to network operators and businesses operating in critical sectors. The definition of network operators is wide enough to include all businesses that operate a computer network. In addition to cybersecurity provisions, privacy principles such as notice, purpose limitation, right of the individual to be informed and correct their data have been included. However, details regarding the nature of application of the provisions of CSL to the Dibao registry are not publicly available. Additional details regarding any specific data access and sharing protocols independent of CSL are not publicly available either.

[30] Unified registry, World without poverty, (2015) https://wwp.org.br/en/social-policy/unified-registry/

[31] Adama Bah, Fransiska E. Mardiananingsih and Laura Wijaya, "An evaluation of the use of the unified database for social protection programmes by local governments in Indonesia", *TNP2K,* March 2014, https://ia800507.us.archive.org/27/items/Working-paper-6-an-evaluation-of-the-use-of-the-unified-database/Working%20Paper%206%20%28English%29.pdf

Data Collection Strategies

Population coverage is an important aspect of creating a consolidated database and deciding the method of data collection. The adoption of a particular method is dependent on accuracy of the existing databases[32] of the social protection schemes in the country along with the coverage offered by the proposed databases. Once data is collected, adequate protocols that address the nature of updating this data is essential. Countries with social registries with on demand data collection approaches have marginally lower coverage rates[33]. In Indonesia, the data collection through household surveys had significantly improved in 2011 from the earlier versions as the data from the surveys was being validated using local knowledge among communities and other data sources such as Village Potential Statistics 2010, Data Collection of social protection programmes (PPLS, 2008) database and others.

In Kenya and Chile, data collection is primarily a result of linkages between existing databases using the national ID numbers. Existing MISs of different welfare schemes will need to be examined to determine if a similar model can be implemented in India. The most crucial element for this data collection strategy is the ID that will be used to link the databases. To prevent exclusion errors, the coverage of the ID across the country through an independent audit needs to be examined.

In India, it is important to consider if Aadhaar number can be relied on to link multiple databases for the purpose of service delivery. Despite a high population coverage (based on the number provided by UIDAI), authentication failures as a result of machine errors, incorrect details in the database or technical constraints from the beneficiary's side have resulted in exclusion of individuals[34] from receiving much needed benefits of the social protection schemes. Efficiency of measures such as the offline verification[35] or alternative modes of identification in case of authentication failures[36] in ensuring higher rates of inclusion needs to be examined. In case of lack of improvement in the inclusion rates, newer strategies to address the technical failures before initiating the process of database linking for the purpose of welfare delivery needs to be tested and subsequently implemented.

The Aadhaar project derives its legal validity from the Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016 (**Aadhaar Act**). The court in K.S

[32] Designing and implementing social transfer programmes , Economic Policy Research Institute (2006) http://epri.org.za/wp-content/uploads/2016/07/Designing-and-Implementing-Social-Transfer-Programmes-EPRI.pdf

[33] Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary registries Australian Government, Department of Foreign affairs and trade (October 2017) https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf

[34] Swetha Totapally, Petra Sonderegger, Priti Rao, Jasper Gosselt, Gaurav Gupta "State of Aadhaar Report 2019" *State of Aadhaar* (2019) https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf?utm_source=download_report&utm_medium=button_dr_2019

[35] Section 2(pa) r/w 4(3) r/w 8A of the Aadhaar Act

[36] Office Memorandum No. D26011/04/2017-DBT Cabinet Secretariat (DBT Mission), December 19, 2017 https://dbtbharat.gov.in/data/om/Office%20Memorandum_Aadhaar.pdf

Puttaswamy vs. Union of India[37] upheld the constitutional validity of the Aadhaar Act after striking down provisions that didn't comply with the proportionality standard for reasonably restricting the privacy of the individual. Despite the clear direction of the Supreme Court on the conditions for mandatory linking of Aadhaar i.e. existence of law, a legitimate state interest and compliance with the proportionality test, there is a lack of consistency[38] in practice. Due to the dissonance in law and practice, the clear mandate around the use of Aadhaar is still unclear. The privacy and cybersecurity risks as a result of such dissonance should discourage developing the delivery exchange model based on Aadhaar as the unique identifier till there is more clarity.

[37] (2019) 1 SCC 1

[38] NH web desk, "Odisha makes Aadhaar mandatory for pension, 11 lakh pensioners could lose benefits", *National Herald,* August 12, 2020
https://www.nationalheraldindia.com/india/odisha-makes-aadhar-mandatory-for-pension-11-lakh-pensioners-could-lose-benefits
ANI, "Mandatory to submit Aadhaar card number for covid -19 testing in Rajasthan", *Livemint,* July 26, 2020
https://www.livemint.com/news/india/mandatory-to-submit-aadhaar-card-number-for-covid-19-testing-in-rajasthan-11595733556362.html
Express news service, "Aadhaar mandatory for government jobs: Kerala Public Service Commission", *The New Indian Express,* June 15, 2020
https://www.newindianexpress.com/states/kerala/2020/jun/15/aadhaar-mandatory-for-government-jobs-kerala-public-service-commission-2156644.html
Ravi Prakash Kumar, "Aadhaar card made mandatory in Tamil Nadu for getting haircut, visiting spas", *Livemint,* June 3, 2020
https://www.livemint.com/news/india/aadhaar-card-made-mandatory-in-tamil-nadu-for-getting-haircut-visiting-spas-11591149863735.html
Express News Service, "Motorists fume as Aadhaar mandatory to recharge fastags", *The New Indian Express,* January 6, 2020
https://www.newindianexpress.com/nation/2020/jan/06/motorists-fume-as-aadhaar-mandatory-to-recharge-fastags-2085572.html

Operationalizing privacy in the Data Lifecycle

In order to design privacy preserving data exchange and welfare delivery platforms, a privacy by design approach is required, where privacy principles are in-built into the design and operation of the platform. This would include both technological and policy choices made about the operation and governance of the platform. In this section, we will look at the entire lifecycle of data from collection to deletion, and look at design features that make the platform privacy enhancing.

Privacy Impact Assessments

A privacy impact assessment (or a data protection impact assessment) helps in identifying and minimising the risks associated with a processing activity prior to initiation of such activity[39]. Across data protection regulations, the assessment is conducted when the processing indicates a significant risk to the rights of the data principal. Under India's proposed regulation, there is an additional requirement of being classified as a significant data fiduciary by the DPA[40]. Due to the possibility of processing of sensitive personal data such as biometric data for the process of service delivery, it would be reasonable to assume that any system that is part of welfare delivery would need to conduct the assessment prior to processing.

The assessment should contain a description of the processing activity including details related to the personal data collected, methods and points of data collection, the specific purpose of processing, security standards, data sharing protocols, effectiveness of the incident response systems in case of a data breach etc. Each step of the activity should be assessed for any potential harm to the data principal and the resultant risk should be rated. The risk rating should be juxtaposed to the necessity and proportionality of that particular activity to the overall purpose of processing. The risks identified should be removed in case of a suitable alternative. In the absence of an alternative, the steps taken to manage or minimise the risk must be documented.

[39] Data protection impact assessment, Information Commissioner's office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessment/

[40] Section 26 Personal Data Protection Bill, 2019

The option to consult with the DPA for advice on the mitigation strategy must be provided. The results of the assessment must be provided to the DPA to seek approval for initiating the processing. For better transparency and accountability, the report should be released to the general public.

Data Collection

Using the Market Incentive

While collection is not done directly by the data exchange and delivery platform, they have a unique opportunity to set some thresholds by specifying minimum privacy standards for all databases for them to qualify to join the platform.

Timing of the Privacy Notice

The privacy notice shall be provided at the time of collection from the data principal, or where the personal data is obtained from another source, at the time of receipt of data from such source.[41] Further, data protection authorities must explore, incentivise and mandate evolving standards and norms for provision of privacy notices in a staggered manner which ensure repetition of notice when the activity in question is relevant to the privacy interests of the individual.[42]

Content of the Privacy Notice

The privacy notices should include the following information:

a. What personal information is being collected;

b. Name and contact details of the entity collecting the data;

c. Purposes for which personal information is being collected;

d. Uses of collected personal information;

e. Whether or not personal information may be disclosed to third persons, and the third party recipients or categories of recipients of the personal data;

[41] Traditionally, the notice and consent regime only involves notification from the data collector directly collecting personal data from the data principal. Given the indiscriminate sharing of data in the age of big data, we suggest aligning the notice requirement with Section 7 (f) of the Personal Data Protection Bill, 2019 which introduces another layer of notice, wherein each data controller in receipt of personal data from other service providers must notify the data principal as well. This additional layer of notice is also reflected in Article 14 of the GDPR.

[42] While we do not suggest adoption of prescriptive formats for providing notice, however, it is expected that the regulator plays an active role in the evolution and adoption of privacy enhancing privacy notices as standards.

f. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

g. The manner in which it may be accessed, verified and modified;

h. The procedure for grievance redressal in relation to collection and processing of data

i. Security safeguards established by the data fiduciary in relation to the personal information;

j. Contact details of the privacy officers for filing complaints.

Form of the Privacy Notice

The privacy notice should be easily accessible, easy to understand, in clear, plain, intelligible, easily legible and concise language that a reasonable person without any legal or technical training can comprehend, and must follow any standards or formats that the DPA or the relevant sectoral regulatory bodies specify. The Bill requires data fiduciaries to provide the privacy notice in multiple languages where necessary and practical[43]. The privacy notice ought to be a meaningful overview of the intended processing of the data collected.

Standardized Privacy Notices

The form in which notices are presented is extremely important. Therefore, summaries, infographics, highlighting relevant and actionable information can go a long way in making notices much more intelligible to laypersons. Some existing models of standardized formats for simple and easy to use privacy notices include the following: i) National Telecommunications and Information Administration (NTIA) developed a code of conduct for standardized short-form privacy notices for smartphone apps.[44] ii) Private Parts is a web based service to simplify privacy notices, [45]

The development of Privacy Commons Notices on the lines of Creative Commons Licenses can be a useful soft standard for recognised, easily understood privacy notices which are human and machine readable. Not only will it increase awareness of key terms in privacy notices, this will also create an incentive for service providers to improve their privacy policies if they want to claim that they use Privacy Commons Notice. Also, in the chain of big data co-controllership and information sharing, privacy preferences of the data principals may often be neglected or not adequately considered. This creates the need for automated policy definition and enforcement so that one party cannot refuse to honour the policy of another

[43] Section 7(2) Personal Data Protection Bill, 2019
[44] "Short form Notice Code of Conduct to promote Transparency in Mobile App practices" available at https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.
[45] Lookout Privacy Policy https://www.lookout.com/legal/privacy-policy

party in the chain of big data analytics. For this, the research community and the big data analytics industry needs to explore the area of privacy policy definition and relevant mechanisms for automated enforcement of privacy requirements and preferences.[46]

[46] Giuseppe D' Acquisto et.al "State of the Art Analysis of Data Protection in Big Data Architectures" *European Union Agency For Network And Information Security*, (December 2015) https://iapp.org/resources/article/state-of-the-art-analysis-of-data-protection-in-big-data-architectures/.

Steps to Develop Privacy Notice

A guidance note released by the Centre for Information Policy Leadership assists organizations in developing a multi layered privacy notice. These steps can be adjusted to account for the Indian population in the context for a social protection scheme. Following are the steps:

1. Map the **data flows** for the schemes that are coordinated and managed using the registry. Identify the **agency collecting the personal data** and the **point of collection** of data.
2. Verify the nexus between the **categories of personal data collected** and the **purpose** of such data collection to state the lawful ground of processing in accordance with the draft PDP, 2019.
3. Develop an **internal privacy policy** to describe the processes from data collection to data destruction.
4. Based on the internal privacy policy, create an **external privacy policy/ notice** that meets the requirements of the draft PDP, 2019 and is in a "clear, concise and easily comprehensible manner and in multiple languages where necessary and practical"
5. **Test** the external privacy policy on the **target audience**.
6. Based on the external privacy policy, **condense** the main points, points that a reasonable person would want to be aware of prior to disclosure of personal data, using **icons** etc. for better readability.
7. Determine the format to **harmonise** the condensed and external privacy policy based on the **medium** that is used to display the notice.
8. **Test** if the format of condensed and external privacy policy is comprehended by the target audience.
9. **Publish**.

Centre for Information Policy Leadership, Ten steps to develop a multilayered privacy notice
https://www.huntonak.com/files/Publication/37a71d77-14c4-4361-a62b-89f67feb544f/Presentation/PublicationAttachment/e7ffca9d-da66-4ed6-a445-f8fdc0b97e22/Ten_Steps_whitepaper.pdf

Informed Consent

1. **Timing of Consent**
   A data fiduciary shall obtain the informed consent of the data principal to the processing of her personal data prior to the collection and processing of the data.

2. **Nature of Consent**
   Informed consent should be voluntarily given through an express and affirmative act on the part of the data principal which establishes a freely given, specific, informed and unambiguous indication of the data principal's agreement[47]. It shall be the responsibility of the data fiduciary to demonstrate consent. When the processing has multiple purposes, consent should be given for all of them.[48]

3. **No One time Consent**
   When the purposes for which personal data was collected are modified or expanded subsequent to its collection, consent will be deemed to be specific only if it is obtained afresh in respect of that modification or expansion, prior to any use of that data for the modified or expanded purposes.

4. **Consent should not be a Tool of Coercion**
   If the data being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent.[49]

5. **Exceptions**
   In the following circumstances and only to the extent necessary, personal data may be collected and processed in the absence of informed consent: (a) vital interest of data principal (question of life and death such as medical emergencies) (b) legitimate interest of the data fiduciary, except where such interests are overridden by the interests or fundamental rights and freedoms of the data principal.[50]

For data collection to be valid under the lawful ground of consent, the consent has to be free, informed, specific, clear and capable of being withdrawn[51]. For consent to be considered free according to the Indian Contract act, 1872[52], it has to be devoid of coercion, undue influence, fraud, misrepresentation or mistake. Undue influence is defined[53] to include situations

[47] Section 11 Personal Data Protection Bill, 2019
[48] This principle seeks to address the issue of implied consent where privacy policies available on web-pages are seen as valid contracts without any affirmative action on the part of the users.
[49] This principle responds to the concerns arising out of the negligence of the data minimisation principle, and data is collected often without having a reasonable nexus to the purpose of data collection.
[50] Vital interest and legitimate interest have been articulated as exceptions in the EU Directive and the GDPR.
[51] Section 11 Personal Data Protection Bill, 2019
[52] Section 14 Indian Contract Act,1872
[53] Section 16 Indian Contract Act, 1872

consisting of a power asymmetry between the person providing consent and the person/entity seeking consent. Provisions requiring transparency of processing apply throughout the lifecycle of the data collected regardless of the lawful ground of processing identified by the data fiduciary. Relying on a ground that is not consent also should not relax any of the obligations stemming from the data protection legislation on the data fiduciary.

The Bill introduces the concept of a consent manager for the purposes of assisting the data principal in reviewing and managing consent through an accessible, transparent and interoperable platform.[54] The data principal will need to prove their identity even while exercising their rights through such a manager. The Bill doesn't provide any additional procedural details on the relationship between the consent manager and the data fiduciary who is responding to the data principal request. Due to lack of clarity on the functioning of consent managers, it is advisable to refrain from including them in the design of the data exchange and delivery model till additional rules on their functioning are drafted by the data protection authority.

Personal Data Stores could be one alternative to the consent manager model.[55] A Personal Data Store or PDS helps you gather, store, manage, use and share the information. It gives the user a central point of control for their personal information (e.g. interests, contact information, affiliations, preferences, friends). For instance, openPDS can be installed on any server under the control of the individual (personal server, virtual machine, etc) or can be provided as a service (SaaS by independent software vendors or application service providers).

[54] Section 23(3) Personal Data Protection Bill 2019
[55] This solution can aid the Consent principle.

Purpose and Collection Limitation

Collection Limitation

Personal data collected and processed by data fiduciaries should be adequate and relevant to the purposes for which they are processed. The data collected should be necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection. The principles of collection limitation requires that only the data that is necessary and proportionate to the identified legitimate purposes are collected. Due to the high risk of harm as a result of unauthorised use of sensitive personal data, apart from strong data access protocols and security measures, it is essential that only such information that is required to achieve the objective of the particular social protection scheme is collected at the outset. Practice of collecting additional data points with the intention of using it for a scheme to be introduced later should be highly discouraged.

Purpose Limitation

The processing of personal data of the data principal will be valid only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed. A data fiduciary shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice prior to collection of personal data. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes. The purpose of processing stated in the privacy notice should not provide the data fiduciary with a blanket approval for data processing across multiple schemes.[56] After the personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures.

There is no definitive approach to implement this principle. For example, countries have adopted varied approaches to detect welfare fraud. An analysis[57] of the purpose specification provisions in certain EU countries has revealed differences in their approach despite the overall application of the General Data Protection Framework. Germany proceeded to limit the processing of personal data for detecting welfare fraud by codifying the requirements in the overarching sector specific social security legislations. The overarching legislation for detection of welfare fraud in the United Kingdom has a very broad scope for data collection. The competent authority responsible for implementation has narrowed down the scope by

[56] Kumar Sambhav Shrivastava "Exclusive: Documents show Modi Govt Building 360 Degree database to track every Indian " Huffpost, March 17, 2020 https://www.huffingtonpost.in/entry/aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462

[57] Valery Gantchev "Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?" 21 European Journal of Social Security, 3-22 (2019)

adopting the Code of Data Matching. The code consists of details of the personal data that can be collected in the event of a suspicion of fraud and is updated on a regular basis. In India, Section 36 of the Bill exempts personal data that is processed in the interest of prevention, investigation, detection and prosecution of an offence from application of certain provisions. Despite the wide exemption, provisions related to fair and reasonable processing continue to apply to such processing. Hence, even in cases where the purpose of processing is welfare fraud, it is essential that the processing has to still be "specific and clear.[58]"

Processing for Reasonable Purposes

Under the Bill, the data fiduciary may process personal data for purposes other than those expressly consented to by the data principal, if such processing is necessary for specified reasonable purpose[59]. The following factors should be considered while determining what constitutes reasonable purposes

a. the reasonable expectations of the data principal,
a. whether processing leads to an adverse impact on the data principal,
b. overriding public interest,
c. nature of the data that are processed (sensitive or not),
d. the relationship between the data principal and the fiduciary and their respective positions of power, and
e. the measures that the fiduciary has taken to reduce the impact on the privacy of the individuals.[60]

Currently, Bill classifies processing personal data for the purpose of prevention and detection of unlawful activity such as fraud as one of the potential reasonable purposes for processing without consent of the data principal. However, the impact of classification of processing of fraud as a reasonable purpose in the context of welfare fraud needs to be examined in the off-chance that the overlap with section 36 of the Bill is not addressed in the final version of the legislation. The absence of the phrase "necessity and proportionality" before relying on the lawful ground can result in an adverse impact[61] on the data principals considering the existing power asymmetry between beneficiaries of social protection schemes and the government and their agencies. In the event that the data fiduciary relies on this lawful ground for processing data for welfare fraud, the privacy impact assessment should take into

[58] Section 4 Personal Data Protection Bill, 2019
[59] Section 14(1) Personal Data Protection Bill, 2019
[60] Lokke Morael and Corien Prins, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016), available at http://dx.doi.org/10.2139/ssrn.2784123
[61] Valery Gantchev "Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?" 21 European Journal of Social Security, 3-22 (2019)

consideration the harms arising out of the potential unnecessary surveillance and resultant exclusion from the benefits of the scheme[62].

Data Processing

Operationalising Purpose Limitation

The principle of purpose limitation requires that the data collected only be processed for the purposes identified. There is a need for clear analysis of the purposes that must be identified with the objectives of the welfare scheme. The purposes identified should have a legal setting.

Machine-readable policies can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information. Sticky privacy policies involve cryptographic solutions in which policies can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information. They allow the data principal to decide on a set of conditions and constraints which unambiguously lay down how their personal data is to be used by the party receiving the data. As the data moves across multiple parties, these policies define an allowed usage and obligations, thus enhancing the control of the data owners over their personal information. They impose prohibitions and obligations such as access of third parties and the purpose for which the data is being used. These policies also allow the data owners to blacklist certain parties from gaining access to their personal information along with laying down rules such as a notice of disclosure and the deletion or minimization of data after a specified period of time.

Each data point should be classified into Non-PD, Non SPDI-PD and SPDI. What is further needed is a mapping of each data point against the purpose of collection, and the intended usage to achieve that purpose. Drawing on the research on sticky privacy policies, these would serve as attributes of data as they travel across data fiduciaries.

The rules governing data processing in the platform must clearly specify that data minimisation can be implemented in the following manner:

a. Where the processing relates to the direct purpose for which the data was collected, the data in its original form may be used.

b. Where the processing relates to incidental purposes, there must be an analysis on whether this can be done simply by using anonymised data.

[62] The District court of the Hague , ECLI:NL:RBDHA:2020:1878

c. Where the processing relates to a new purpose, then either it must be done using aggregate/anonymised data or by seeking permission from the data principal afresh

d. Where the processing relates to planning related decisions, there must only be reliance on aggregate data, so as to avoid the risks of social profiling

In the case of implementing the principle of Opt Out, data principals should be provided with the option of no collection of further data. This could be facilitated by a system such as a centralised website/service/phone number/email number - where an individual can withdraw consent easily, for instance through a single SMS for which the syntax is easy to use. Service providers could be automatically informed of such choices, or they could access the details of the users who have opted out periodically (daily or bi-weekly basis) and effect changes. In order to prevent mistaken removal of users, an additional layer of confirmation through email/SMS can also be built in.

Anonymisation and Encryption

Data that can be anonymised without hampering the functionality of the platform should be anonymised using recognised techniques (removal of all identifier fields or use of statistically significant techniques). The Bill defines anonymisation in relation to personal data as "an irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority."[63] Aggregation of personal data is an example of anonymisation used for data analysis where data is displayed as totals rather than individual value.

There must be appropriate guidance for anonymisation standards. The process of de-identification removes identifying information from a dataset such that remaining individual data cannot be used to personally identify specific individuals, thus reducing the privacy risk of further sharing and processing of data. The different approaches to de-identification include removal of direct identifiers, pseudonymization, De-identification of Quasi-Identifiers, field based de-identification, privacy preserving data mining and publishing.

The basic idea of anonymisation seems straightforward. However, anonymisation can be reversed as long as there is some informational content remaining in the data. There have been examples[64] of anonymised data being reversed and the personal information and identity of the individuals being revealed. Effective employment of these techniques would

[63] Section 3(2) Personal Data Protection Bill, 2019

[64] Ran Singel, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims", Wired, December 17, 2019 https://www.wired.com/2009/12/netflix-privacy-lawsuit/

Alex Hern, "New York taxi details can be extracted from anonymised data, researchers say", The Guardian, June 27, 2014 https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn

involve regulatory bodies to frequently examine the efficacy of these techniques in light of emerging re-identification approaches, incentivising and/or mandating the use of de-identification techniques based on the sensitivity of personal data in question through sectoral regulations.

It has been widely argued that the utility derived out of a data set is inversely proportional to the privacy of data.[65] Understandably, stripping the personal data identifiers from a welfare service delivery database can drop the functionality of such a dataset which renders any potential usage of differential privacy mechanisms non-feasible.[66] An accurate determination of the context and purpose of processing of the anonymised data is essential to determine the exact techniques that need to be used to anonymise a particular data set.[67]

Data that is used for welfare service delivery is to be encrypted. At the platform level, there should only be access to anonymised data. If specific access to personal identifier information is needed by another department, then there must be a clear system of raising query to the relevant department (which is governed by a set of data access protocols). The welfare benefit schemes are operated at the Central Government level as well as by different State Governments and therefore, multiple state actors have access to personal data of the beneficiaries. Access to the data should be available in an aggregate manner and only non-identifying data should be made publicly available.

[65] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 57 UCLA Law Review, 1701 (2010)

[66] Prashant Agrawal, Anubhutie Singh, Malavika Raghavan, Subodh Sharma, Subhashis Banerjee, "An operational architecture for privacy by design in public service applications", arXiv preprint, June 8, 2020 https://arxiv.org/abs/2006.04654

[67] Article 29 working party opinion on anonymisation techniques https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Data Sharing

Sharing of data from different nodes of the platform must involve the following:

- Only anonymised/aggregate data is shared by default
- There should be a clear timestamp accompanied by a system of digital signature that is followed for all data sharing from one node in the platform to the other[68]
- In case of any query for specific information including personal identifiers, an encrypted data query must be sent from Department A via the platform to Department B. Ideally all departments are connected to the platform through Security Server and all communication between the nodes pass through this
- There must be clear 'Rules for Information Sharing' for any data sharing or exchange through the platform
- Data sharing protocols for state agents and non state agents (Kenya data sharing protocols permits data sharing based on a data request form[69])

A data fiduciary shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force.

[68] Personal data usage monitor in Estonia stores transaction logs using block chain technology. World Bank, Privacy by Design: Current Practices in Estonia, India, and Austria, 2016, Washington, DC: World Bank https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf

[69] Hunger Safety Net Programme Data Request and Confidentiality Form, https://www.hsnp.or.ke/images/mis/hsnp_data_request_form.pdf

Data Security and Breach

Security obligations

A data fiduciary shall take measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality, secrecy, integrity and safety of all information collected including but not limited to personal data, including from theft, negligence, loss or unauthorised disclosure. The security measures, as appropriate may include, without limitation: a) de-identification of personal data, b) ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and c) ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.

Notification obligations

If the confidentiality, secrecy, integrity or safety of the data is violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to these principles, or for any other reason whatsoever, as soon as the data fiduciary becomes aware of such violation, they must notify the data principal to whom it pertains, and the regulatory bodies responsible for data protection.

Key Considerations to Operationalise Data Breach Notifications

The PDP Bill 2019 requires data fiduciaries to report a data breach to the data protection authority if such a breach is likely to cause harm to the data principal. The harm threshold does avoid the dangers of over notification however, clear guidance on determination of such harm is awaited. In the absence of such a guidance and in the unlikely event that a registry is set up before the privacy bill is notified, best practices from countries with similar breach notification requirements will need to analysed. Determination of harm should take into consideration the categories of personal data and the volume of personal data compromised.

According to the 2019 version of the bill, data fiduciaries are not required to notify the data principal unless and until the data protection authority requires them to do so. The notification that is sent to the data principal is required to have the same content that is provided to the data protection authority. It is advisable that the content of the notification that is being sent to the data principal be modified according to a reasonable man standard i.e. language devoid of complicated legalese and technical specifications.

The Bill also requires data fiduciaries to upload the details of the breach notification on their websites in certain cases. Due to the diversity in the socio-economic conditions of data principals that the social registry aims to cater to, it would be advisable to find adequate alternatives such as publishing the notification in regional newspapers.

Data Portability and Machine Readable Policies

Under Section 19(1) of the Bill, the data principal has the right to receive the personal data in a structured, commonly used and machine readable format. However, as per Section 19 (2), this provision is not applicable where the processing is necessary for any function of the state or in compliance of a court order.

Article 20 of the GDPR, states that the data subject has the right to receive personal data concerning her from the data controller in a "structured, commonly used and machine readable format". The meaning of machine readable in the European context can be inferred from the field of public sector information - Rectial 21 of the Directive 2013/37/EU - and is defined as " a file format that is structured in such a way that software applications can easily identify recognise and extract specific data from it." UK's data protection authority ,ICO, In addition to the field of public sector information refers to the open data handbook wherein data is said to be machine readable if it is "in a format that can be automatically read and processed by a computer."

GDPR doesn't impose a strict legal requirement on the format through which personal data has to be provided to the data subject or transmitted to another data controller. However, Article 29 working party guidelines[70] warns against using formats that are subject to expensive licensing requirements. In the absence of industry standards, data controllers are advised to provide personal data using open formats. In cases where internal systems use proprietary software which individuals may not be able to access, additional/ancillary processing may be needed to provide the personal data to the data subject in the format that is required by GDPR. Additional processing may also be required in cases where extraction of personal data from internal databases renders it non-comprehensible.

There is a shift in the terminology of data portability in the United States. The Health Insurance Portability and Accountability Act and the California Consumer Protection Act (CCPA) have clauses related to data portability, but both of them use the phrase "readily usable format" in place of "machine readable". Hence, even though it is the same requirement, lack of technical specifications makes the CCPA requirement easy to comply with. For the Indian context, surveys around GDPR implementation and implementation of data portability need to be referred to determine whether it is appropriate to use "machine readable" or "readily usable" for the right to data portability.

In the welfare delivery context, right to data portability is vital in cases where the schemes can require data transfer to multiple municipalities enabling the data principal to avail the benefits of the scheme regardless of the geographical location. However, incorrect porting

[70] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party (4 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

can result in exclusions. Ensuring that the technical specifications of portability are easy to comply could be one way to mitigate potential exclusions.

Key Considerations for Machine Readable Formats

To determine the implementation of the right to data portability, a study was conducted wherein 230 data portability requests were sent out to a broad range of data controllers. Responses were provided in numerous formats, however tabular CSV or XLS files were the most widespread. An analysis of the formats revealed gray areas in terms of strict compliance with the machine readable requirement of GDPR, despite consensus over the overall file formats. For example, XLS files may not be machine readable if multiple sheets are included in a single workbook. A HTML file may not be compatible till the time it is marked up and includes a data structure that allows structural relationships between elements within tabular data.

Janis Wong and Tristan Henderson "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", 9, International Data Privacy Law, 173-191, (2019)

Data Principal Rights

Ease of Exercise of Data Principal Rights

Exercising the data principal rights is one way for the data principal to exercise control over their personal data. Under the current data protection framework, body corporates are required to allow the providers of information to review the information that has been provided and correct any inaccurate data provided. In the past, government agencies processing personal data of the individuals needn't follow these requirements since they didn't fall under the definition of body corporates. However, since the data protection principles (including the data principal rights) enshrined in the Bill, apply to the state actors once notified, government databases that are currently in the process of design need to develop mechanisms that operationalise these rights. The rights that the data principal can exercise are as follows:

1. **Right to Withdraw**

   The data principal shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

   The data principal shall have a right to seek all information reasonably necessary to decide whether to withdraw their consent, including not limited to purposes for which their data is being processed, the manner in which such processing is being conducted, the duration which the data collector intends to process and retain the data. While this may provide limited recourse in cases of welfare delivery or essential services, it is important that this right is provided where an individual may be able to exercise this choice.

2. **Right Against Unfair Denial of Service**

   All persons shall have the right against unfair denial of services on the grounds that such persons do not agree to share data, which is not essential but merely incidental to the provision of service, being made a precondition to the provision of services.

3. Right to Access

The data principal shall have the right to obtain from the fiduciary access to the personal data collected and/or being processed. Additionally, the data principal can seek the purposes of the processing, the recipients or categories of third party recipients to whom the personal data has been or will be disclosed, the intended time period of which the data would be stored, details of sources where data was not obtained directly from the data principal. The data will be made available by the fiduciary in a structured, machine-readable as well as human-readable format. This shall include both data directly collected from the data principal as well as data observed about the data principal.

4. Right to Portability

The data principal shall have the right to transmit the data obtained from the fiduciary under the right to access to another fiduciary without hindrance from the fiduciary to which the data was originally provided.

5. Right to Correction

The data fiduciary shall have the right to ensure from the data fiduciary, the rectification of inaccurate or incomplete personal data, without any undue delay, especially in cases where the incompleteness or inaccuracy of the data has adverse impacts on the data principals.

6. Right to Restrict Processing

In cases where the accuracy or completeness of the data is contested by the data principal, the data principal has the right to restrict the processing of the data in question.[71]

[71] This right adds to the principle of Opt-Out and seeks to strengthen it by formulating it as a separate right available at all times to data principals.

7. Right to Access when Data Indirectly Obtained

All data principals shall have a right to seek details as laid down in the notice principle from any data fiduciary about personal data about them obtained, not directly from the data principal, from a third party source.

The methods of exercising these data principals rights should be economically feasible and should be executed in a time sensitive manner. Since the quality and accuracy of the personal data collected is essential for efficient service delivery, any arduous data correction and updating practices may result in exclusion errors. Apart from the digital options to exercise these rights, multiple helplines and facilitation centres[72] for the sole purpose of correction of personal data is advised. Measures such as multiple language operators and on ground assistance is encouraged. In the case of biometric collection of personal data, any blanket prohibition on correcting the core biometric information is counterintuitive to enabling efficient welfare delivery and is strictly forbidden.

Following are some of the additional rights (that are not provided for under the Bill) that need to be provided to the data principals:

1. Rights to Access Data about Previous Breaches

All data principals should have the right to seek information about the any previous instances of security breaches resulting in the theft, loss, negligence, damage or destruction of data held by the data fiduciary or its agents, and the steps taken by the data fiduciary to address the immediate breach as well as steps to minimise the occurrence of such breaches in the future.[73]

2. Rights Against Automated Decision Making

Additional safeguards need to be provided in cases where the delivery of services or exclusion from services is solely dependent on automated decision making. In the absence of a provision related to such decision making the proposed data protection framework, measures to promote transparency in the context of service delivery

[72] Section 112 of the Code on social security,2020 advocates for such a model to facilitate enrolment, registration and dissemination of information regarding the social protection schemes to the workers. Similar model can be used for the sole purpose of exercising the different data principal rights. This model should be separate from the grievance redressal models to prevent bottlenecks.

[73] Along with transparency and openness obligations, this right may also foster market competition for services providers to address security issues.

should be implemented. The EU best practice i.e. details regarding the logic used for decision making can be provided to the citizens. The other option is to require agencies relying on automated decision making to incorporate processes (eg. independent audits) that minimize the risk of discrimination, bias or incorrenct decision[74]. Public disclosure of details regarding the measures taken is essential for transparency.

[74] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (July 2018) https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Key Considerations for Implementing Data Principal Rights

Authentication of the data principal request

Prior to responding to the request of the data principal, the identity of the data principal raising the request needs to be verified. The data principal can be required to either submit documents or passcodes authenticating their identity depending on the procedure to raise a rights request in the first place. Relying on biometric details for authentication in this case might not be feasible since expecting the data principal to physically approach an office is cumbersome.

Understanding the flow of the personal data amongst the different schemes

For adequately responding to a request to access or portability of the data principal, a very clear view of the flow of data within the entire service delivery system is necessary. For example, if the team tasked with the responsibility of responding to the request is aware of only one of the data collection points out of three, the data that will be provided to the data principal will be incomplete. If there is a centralised database for the all personal that has been collected from the data principal for all the social protection schemes part of the system, the team handling the data principal requests should have access to that database. In the absence of a centralized database, the structure of responding to a request might be relatively complicated. Policies enabling coordination between the different teams managing the database will need to be drafted and implemented.

Records containing details of the time taken to respond to a request, documents used to authenticate the identity of the data principal, the specific right that has been exercised, explanation for not fulfilling the request of the data principal needs to be maintained.

Awareness of the data principal rights

For these rights to be effective, it is essential that the data principal is made aware of the existence of these rights along with the process to be followed for exercising them. The draft regulation requires data fiduciaries to provide details of the existence and procedure of exercising these rights in the privacy notice.

Incremental Approaches to Data Privacy

The fundamental problem for IT systems in governance in India is that they have so far existed in a regulatory vacuum with barely any legal safeguards for privacy. As a result, the state of data practices pay little heed to privacy preserving principles. The key challenge is ensuring better governance for India is to move rapidly to a more robust form of privacy governance. Following are the stages through which compliance with the data protection legislation can be operationalised:

Incremental Approaches to Data Privacy

	Stage 1	Stage 2	Stage 3
1	Ensuring all personal data is further delineated into PII and SPDI.	Use of APIs and guidance make available by the platform to ensure encryption and anonymisation (removal of identifiers/k-anonymity)	The platform to create some standardized formats for simple and easy to use privacy notices on the lines of NTIA and Privacy Parts
2	Compulsory privacy policies for all policies on the platform. The privacy policies to be easily accessible, in a clear, plain and concise language that a reasonable person without any legal or technical training can comprehend.	The platform to create some standardized formats for simple and easy to use privacy notices on the lines of NTIA and Privacy Parts	Mechanism to ensure consent is not a tool for coercion. If data being collected is merely incidental and not essential to the service being provided, then agreeing to a privacy policy that mandates collection of such data should not be a condition precedent
3	Map the data lifecycle to ensure that the privacy notice is provided at the time of collection from the data principal and where the personal data are obtained from another source, at the time of receipt of data from such source.	More robust opt-out mechanism	Proactive disclosures with respect to usage of personal data collected
4	Enforcing purpose limitation in use and sharing of data. Specifying a vague and broad purpose in an attempt to enable usage and sharing of data for unforeseen situations should be discouraged. For guidance on the extent of specificity of the purpose, the legislation or executive order that is providing legitimacy to the scheme can be referred to.		Mechanisms for easy implementation of access and portability rights such as a direct download option and direct transmission of the data to another fiduciary upon the request of the data principal
5	Right to access, correction and deletion must be provided.		Platform to set a clear mechanism for transfer of data such as Sticky Privacy Policies [94].
6	A digital, easy to access, grievance redressal mechanism must be set up and details to be provided in the privacy notice.		Post classification of data, what is further needed is a mapping of each data point against the purpose of collection, and the intended usage to achieve that purpose. Drawing on the research on sticky privacy policies, these would serve as attributes of data as they travel across data fiduciaries.

Openness

The Openness movement in India has seen important landmarks in the last two decades. When we talk about an 'Open' digital platform of this nature with DXL features, we refer to several different aspects of openness which must be conformed to. The National Data Sharing and Accessibility Policy ("NDSAP") received Cabinet Approval in 2012.[75] The primary purpose of this policy was to facilitate access to Government of India owned shareable data and information in both human readable and machine readable forms.

OSS Policy: The Policy on Adoption of Open Source Software for Government of India was promulgated in 2014[76] and relates to the open availability of source code of the software being deployed by the government for the technology community and citizens so they may use, modify and reshare the code, but also so that faster and more agile testing and audit of the code can be conducted openly. Therefore, not only the software used by deployment of existing and available open source software, but the versions deployed by the government must also have its source code available.

Open API Policy: Another aspect of openness which has become very prevalent in conversations on the use of digital platforms for e-governance is that of Open Application Programming Interfaces (APIs) for the Government of India ("Open API Policy").[77] The primary focus of this policy is interoperability, wherein "Open APIs" can facilitate integration between different e-Governance applications.

Below we look at some lessons that can be drawn from the set of Open APIs, India Stack[78] built by iSPIRT, and the mistakes which we should avoid for future platforms. While the Unique Identity Project uses open source software as building blocks and as part of its infrastructure and the code developed by Ispirt to work with Aadhaar may be licensed to or used by the government, however none of this code is available under an open source license. This prevents any public testing or audit of the code. There are also parts of the digital infrastructure which have been allowed to remain proprietary code owned by vendors, for which adequate licensing steps have not been taken so as to make it open. While data exchanges are enabled through Open Standards and while using Open APIs, they are also operational within a very controlled environment of licenses parties.

IndEA Framework: The India Enterprise Architecture Framework ("IndEA Framework") by MEITY sought to establish an e-governance model which would clearly adopt the policies on open

[75] National Data Sharing and Accessibility Policy, 2012
http://surveyofindia.gov.in/files/gazette%20(1).pdf
[76] Policy on Adoption of Open Source Software for Government of India,
https://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf
[77] Policy on Open Application Programming Interfaces (APIs) for Government of India,
https://meity.gov.in/writereaddata/files/Open_APIs_19May2015.pdf
[78] "What is Indiastack?", Indiastack https://www.indiastack.org/about/

source (OSS Policy) and open APIs (open API Policy) as the basis for the application architecture of its model. This would be a good model to look at and learn from.

Open source software has been used by Kenya and Uganda for their databases on Hunger Safety Net Programme and Social assistance grants for empowerment respectively.[79] The Kenyan government in an effort to achieve the objectives set by their National Social protection policy, created a framework to coordinate the activities of their five cash transfer programs to establish the National Safety Net Program. The MISs of these five cash transfer programs are one of the key elements for the monitoring and evaluation system of the program. While determining the factors of the database that would form the basis of the electronic MISs, emphasis[80] was laid on the open source nature of the HSNP database. It was decided that the proprietary nature of the CT-OVC[81] database would render any changes to the database a cumbersome task, making the HSNP database the preferred alternative. The data exchange platform of Estonia, X-Road, is based on open standards[82] and the source code is available on github[83]. The interoperability framework requires the public sector to adhere to the principle of openness and any departure from this principle has to be justified.

In the context of data exchange and service delivery platforms, the rich history of openness movement would be most useful to adhere to. For instance, following the INDEA framework model would also ensure that the some of the issues that exist with the NODE Consultation Whitepaper[84] can be avoided. For instance, the NODE paper states that each part will 'have its own configuration of degree of "openness"'. Clear adherence to the existing openness policy documents in India, as well as respecting the legacy of work done towards openness can easily prevent such issues from arising. The clear adherence of the OP policy would ensure clear auditability and robustness of the software and algorithmic decisions.

[79] Good practice in the development of management information systems for social protection, Development Pathways, (2018) https://www.developmentpathways.co.uk/wp-content/uploads/2018/06/Good-Practice-in-theDevelopment-of-Management-Information-Systems-for-Social-Protection-Help-Age-International.pdf

[80] Program appraisal document on a proposed credit to the Republic of Kenya for a national safety net program for results, World Bank, June 26, 2013, documents.worldbank.org/curated/en/500691468273333320/pdf/782940KE0PAD0I00Box0377356B00OUO090.pdf

[81] Cash Transfer for Orphans and Vulnerable Children

[82] Interoperability of the State Information System. Framework Version 3.0. The Ministry of Economic Affairs and Communications (2011) https://www.mkm.ee/sites/default/files/interoperability-framework_2011.doc

[83] Github (2016). X-Road https://github.com/vrk-kpa/xroad-public

[84] Strategy for National Open Digital Ecosystem, Ministry of electronics and Information Technology, Government of India https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

Governance

A mammoth task such as integrating databases with details of personal and sensitive personal data should not be undertaken in the absence of a data protection regulation and an independent authority to oversee the enforcement of the regulation. In the absence of the notification of the law prior to initiation of the design of the system, a privacy protocol, that emulates the standards set in the Bill, should be drafted along with clear and enforceable guidelines on oversight of the personal data processing. The principle of consent and purpose limitation needs to be strictly adhered to i.e. any change in purpose needs to be notified and fresh consent must be sought from the data principal. In case of proposals expanding the role of information management systems from service delivery to an emergency response system or law enforcement purposes, such proposals shouldn't be acted upon until a clear, specific and unambiguous regulation authorising such use along with safeguards to protect the citizens from the harms arising out of has been enacted.

In addition to the data protection legislation, the functioning of the data exchange and delivery platform (platform) should have legislative backing. The legislation that legitimises the platform should have provisions related to its governance and accountability , the Authority providing oversight and its powers, adequate grievance redressal mechanisms and its interaction with other subject matter specific statutes.

Oversight and Accountability

Governance Structure

There should be a clear indication of the agency (data fiduciary) that is responsible for the management of such a platform and its compliance with the privacy principles. Clear systems of accountability should be set for the entities using the Platform i.e. they should be required to comply with the applicable legislations and should have adequate oversight. In case of involvement of private actors, additional safeguards related to the privacy and confidentiality of the data in the platform will need to be implemented. The roles and responsibilities of all the stakeholders will need to be formalised through legal agreements with specific provisions [85] requiring regular audits and clarity around enforcement and penalties in case of breach of responsibility.

[85] Article 28 General Data Protection Regulation

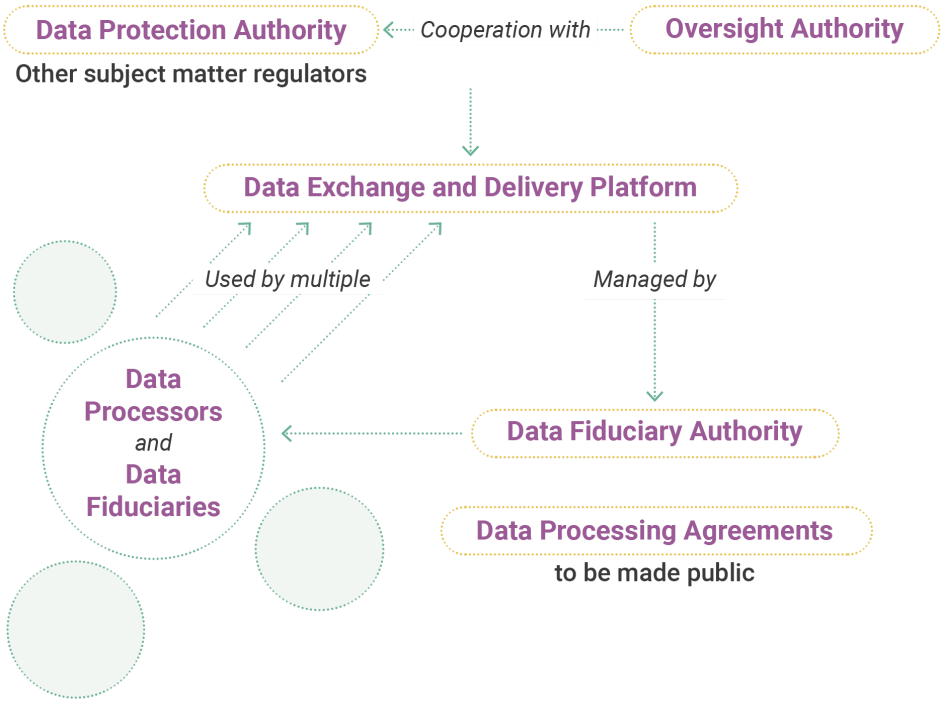
Accountability and Audit

The Authority that is providing oversight to the functioning of the platform should not be the same as the data fiduciary that is responsible for the management of the platform. Effective oversight will not be possible in the event of conflict of issues.

Guidance may be taken from the Telecom Regulatory Authority of India (TRAI) which was initially set up to undertake both regulatory as well as adjudicator functions. However, in 2000, the TRAI Act was amended and Telecom Disputes Settlement and Appellate Tribunal (TDSAT) was established, with a view to bring in "*functional clarity and strengthen the regulatory framework and the disputes settlement mechanism in the telecommunication sector.*" Guidance can also be taken from several existing independent authorities such as the Airports Economic Regulatory Authority of India (AERA) and the Securities and Exchange Board of India (SEBI). The AERA was established under the Airports Economic Regulatory Authority of India Act, 2008 which also established the Airports Economic Authority Appellate Tribunal. AERA is responsible for determining the tariff to be levied for provision of aeronautical services. The adjudicatory function has been vested with the Appellate Tribunal.

The data fiduciary should be in regular communication with the DPA and seek guidance wherever necessary and cooperate with the Authority for any investigations or audit of the Platform. In this respect, guidance may be taken from the U.K.'s Information Commissioner's Office (ICO), which has the power to undertake audits of the public and private organisation. Any organisation can request the ICO to carry out an audit of its activities to ensure that it is in compliance with the data protection obligations. The data fiduciary should seek periodic audit of the data protection obligations of the Platform by the DPA.

Governance Structure



Investigative and Corrective Powers

The Authority should have the power to implement a range of measures in response to an allegation of a violation by the platform. It should possess the power to summon key internal documents to validate the effective and lawful functioning of the platform while ensuring that they are strictly bound by the rules of confidentiality. Apart from mandatory periodic audits, the Authority should have the power to command the data fiduciary and data processors of the platform to conduct audits subsequent to a complaint regarding their functioning.

It is advisable that the regulatory actions, as a response to the investigations, be proportional to the violations and the scope of such measures should be clearly documented to ensure consistency in the enforcement actions. In case of minor infractions (such as not responding to a data principal request within the prescribed time frame), the Authority should have the option to contractually bind the data fiduciary for corrective action prior to resorting to civil

or criminal penalties(akin to ICO's powers to issue enforcement notices[86]). In the absence of adherence to the contractual undertaking, further action can be initiated.

Advisory Powers

Considering that effective operation of this platform is complex, the Authority should provide guidance wherever necessary and try to emulate the best practices that are implemented across similar platforms in other countries. Prior to adopting such guidance, the enforcement authority for the platform should cooperate with other domestic agencies and authorities that might have subject matter expertise on the topic of the guidance.

It would be useful for the Authority to set up a mechanism on the lines of the Security and Exchange Board of India (SEBI)'s Informal Guidance Scheme, which enables regulated entities to approach the Authority for non-binding advice on the position of law. Given that there is very little jurisprudence on the subject, it would be extremely useful for regulated entities to get guidance from the Authority.

Harms

If the intended use of the platform could lead to denial or restriction of services or benefits to individuals, or categories of individuals, then there must be a mechanism to ensure that such individuals are not disadvantaged. In these cases, individuals must be able to use other forms of identification to seek access to services or benefits.

Whether enrolling into and specific uses of such a platform should be mandatory or not remains one of the most important questions. As mandating such use limits the agency of individuals, it should be subject to strict legal tests, such as the need to obtain information that is strictly necessary to provide a service to an individual, prevention of harm to others, and eligibility to undertake specialised tasks. It is advised that enrolling into such a platform is not mandatory.

Security Obligations

The platform shall take measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality, secrecy, integrity and safety of all information collected including but not limited to personal data, including from theft, negligence, loss or unauthorised disclosure. The security measures, as appropriate may include, without limitation: a) de-identification of personal data, b) ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and c) ability to ensure the ongoing confidentiality, integrity, availability

[86] Regulatory Action Policy, Information Commissioner's Office, https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

and resilience of processing systems. Periodic audits of the security measures by external entities and disclosure of the result of the audits to the general public should be required.

Compliance with the ISO 270001, the standard for information security management system, has been recognised as satisfactory for the purposes of the Information technology Act 2000. However, it doesn't have comprehensive requirements pertaining to maintenance of the overall privacy framework of the system. The British standard BS10012:2017 is a specification designed based on the privacy principles outlined in the GDPR. The ISO 27701:2019 is a standard for privacy information management and defines processes to comply with the privacy specific requirements of data protection regulations. Current standards of information security under the Information Technology Act, 2000 and the proposed data protection framework need to be upgraded to include standards regarding maintenance of the personal information management systems.

Redress

Adequate redressal mechanisms would necessarily include the following three requirements:

a. User Notification: If the confidentiality, secrecy, integrity or safety of the data is violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to these principles, or for any other reason whatsoever, as soon as the data fiduciary becomes aware of such violation, they must notify the data principal to whom it pertains, and the regulatory bodies responsible for data protection.

b. Access, Correction and Deletion: Individuals must have access to personal data collected through, and the ability to seek corrections, amendments, or deletion of such information where it is inaccurate.

c. Due Process: individuals must be entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial adjudicating authority.

The World Bank has highlighted[87] the importance of citizen feedback on state service providers in increasing the capacity of the policy makers and managers. A free, fair and effective grievance mechanism has been considered a very important feature of a social protection program. Studies have found that due to reasons such as lack of awareness about the mechanism or the objectives of the scheme, lack of adequate method to lodge complaints either due to physical distance or inability to operate tech based platform, these

[87] World Development Report: Digital Dividends, The World Bank Group (May 17, 2016), https://www.worldbank.org/en/publication/wdr2016

grievance mechanisms have been inefficient in most countries[88]. Integration of grievance mechanisms across programs has been considered a best practice, however such an integration is difficult to achieve in cases where structures and capacities of programs are different[89].

It is accepted that addressing complaints at the point of service delivery is the most efficient due to low transaction costs[90]. However, not all complaints in the context of delivery of benefits under a social protection scheme can be addressed at the point of service delivery, e.g. targeting issues. A study[91] to analyse the existing grievance mechanisms in the four main social protection programs in Indonesia revealed that usually, the first point of contact (the district government) couldn't address issues related to targeting since it wasn't their mandate. However, the individual raising the grievance wasn't aware of the same.[92] Hence, for developing the system for India's schemes an understanding of the type of complaints that will probably be raised is required. Internationally, a three tier approach[93] has been suggested.

[88] Valentine Barca and Richard Chichir, "Single registries and integrated MISs: De-mystifying data and information management concepts", *Oxford Policy Management*, (May 2014) https://www.opml.co.uk/files/2018-05/barca-chirchir-2014-data-information-management-social-protection.pdf?noredirect=1

[89] Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary registries Australian Government, Department of Foreign affairs and trade (October 2017) https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf

[90] Review of, and recommendations, for grievance mechanisms for social protection programmes, Oxford Policy Management (September 2012) https://www.opml.co.uk/files/Publications/7748-indonesia-grievances/grievances-exec-summary-final.pdf?noredirect=1

[91] Review of, and recommendations, for grievance mechanisms for social protection programmes, Oxford Policy Management (September 2012) https://www.opml.co.uk/files/Publications/7748-indonesia-grievances/grievances-exec-summary-final.pdf?noredirect=1

[92] Review of, and recommendations, for grievance mechanisms for social protection programmes, Oxford Policy Management (September 2012) https://www.opml.co.uk/files/Publications/7748-indonesia-grievances/grievances-exec-summary-final.pdf?noredirect=1

[93] Stephen Kidd et.al "How to implement inclusive social protection schemes", *United Nations ESCAP,* (2018) https://www.unescap.org/sites/default/files/Social_Protection_module_3_English.pdf

- The first tier is supposed to deal with issues related to registration papers, identity documents, payment related issues etc.
- The second tier should be operated by the administrators of the specific social protection program. Any issues related to incorrect targeting criteria etc. should be dealt with here.
- The third tier is the authority of last resort for appeals. Those handling appeals shouldnt be directly responsible for the program.

Therefore, multiple channels for receiving complaints must be set up to pander to the citizen's convenience. A purely digital mechanism might be difficult in India due to the lack of widespread access. A centralized repository of the complaints registered can be created to enable coordination across relevant agencies depending on the scheme (data sharing protocols to apply).

Annexure

Definitions

Management Information Systems (MIS)
These are systems/databases of individual social protection programmes that can be used for coordination of service delivery, identification of beneficiaries etc.[94]

Integrated Beneficiaries Registries
These are databases that contain data only about the existing beneficiaries. These databases can assist in coordination of service delivery and oversight of the same once the beneficiaries of the social protection schemes have been identified. [95] For the registry to be effective in monitoring and evaluation of the beneficiaries, the existing MISs of the individual programmes need to be of high quality.

Social Registries
These are databases that contain data of the existing beneficiaries of a program along with potential beneficiaries. These databases have more coverage in terms of population covered relative to the integrated beneficiaries registries. Since these databases cover potential beneficiaries, the data can also be used to determine potential eligibility for programs in addition to coordination of service delivery and oversight. [96] For the registry to be effective, the dynamic nature of the registration process i.e. the frequency of data updation/collection is highly essential.

Data Exchange Layer
This layer provides for a secure method of data exchange between information systems which are connected through standardized access points.[97] This specific definition has been drawn from Estonia's data exchange layer, X-Road

Data Fiduciary means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data[98]. This is with reference to India's proposed data protection framework.

---

[94] Evie Browne, "Social protection Management Information Systems(MIS)" , *GSDRC*, 19 December 2014, https://gsdrc.org/docs/open/hdq1180.pdf
[95] Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary registries Australian Government, Department of Foreign affairs and trade (October 2017) https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf
[96] Id
[97] "X-Road® Data Exchange Layer", X - Road, last accessed September 2, 2020 https://x-road.global/
[98] Section 3(13) Personal data protection Bill, 2019

Data Processor means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary.[99] This is with reference to India's proposed data protection framework.

Data Principal means the natural person to whom the personal data relates.[100] This is with reference to India's proposed data protection framework.

Data Subject means the identified or identifiable natural person to whom the personal data relates.[101] This is with reference to European Union's data protection framework.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law[102]**.** This is with reference to European Union's data protection framework.

[99] Section 3(15) Personal data protection bill, 2019
[100] Section 3(14) Personal data protection bill, 2019
[101] Article 4(1), General data protection regulation
[102] Article 4(7), General data protection regulation