BANK FOR INTERNATIONAL SETTLEMENTS

BIS Papers
No 124

The design of a data governance system

by Siddharth Tiwari, Sharad Sharma, Siddharth Shetty and Frank Packer

Monetary and Economic Department

May 2022 (revised July 2022)

JEL classification: G28, H41, K00, L17, L51, O33.

Keywords: Data governance, big techs, data-sharing, data taxonomy, consent framework, account aggregators, General Data Protection Regulation (GDPR), Data Empowerment Protection Architecture (DEPA).

The views expressed are those of the authors and not necessarily the views of the BIS.

This publication is available on the BIS website (www.bis.org).

ISSN 1682-7651 (online)
ISBN 978-92-9259-558-6 (online)

The design of a data governance system

By Siddharth Tiwari,* Sharad Sharma,^ Siddharth Shetty^ and Frank Packer*

Abstract

Technological developments over the last two decades have led to an explosion in the availability of data and their processing. With the advent of smartphones, digital technologies, software applications and network connectivity, the consumer digital footprint has expanded at a dramatic pace. In such a setting, the key questions are who has control over these data, where they are stored, with whom and under what conditions they are shared, and who operates the data governance system.

Central to the privacy laws of most countries is a set of principles that define how personal data are collected, shared and processed. However, consumers often do not know the benefits and costs of the data that pertain to them. And even when they do, consumers find it difficult to assert their rights regarding the collection, processing and sharing of their data.

This paper proposes a data governance system that corrects for the market failures described above. In particular, we argue that these can only be corrected by restoring de facto control of data to the consumers and businesses generating the data, and requiring their consent prior to collection, sharing and processing of their data by service providers. In order that such a consent system is adopted widely within a jurisdiction, it should be user-friendly, with low transaction costs. Such an approach will empower data consumers and businesses to use their data for their own benefit.

An effective data governance system must embody data protection principles and the protocols to operationalise them in a consent-based architecture. Conditions for effective data-sharing will include notice and consent, purpose limitation, data minimisation, retention restriction and use limitation. The system also needs to be open, with consent that is revocable, granular, subject to audit, and with notice in a secure environment. Trust in the system and widespread adoption of the consent-based architecture can be significantly enhanced by mandating specialised data fiduciaries to ensure that data are shared in a fashion that respects the above-mentioned principles of effective data governance. The experience with India's Data Empowerment Protection Architecture (DEPA) suggests that such a consent-based system can operate at scale with low transaction costs.

JEL classification: G28, H41, K00, L17, L51, O33.

Keywords: Data governance, big techs, data-sharing, data taxonomy, consent framework, account aggregators, General Data Protection Regulation (GDPR), Data Empowerment Protection Architecture (DEPA).

We are indebted to Rahul Matthan for close collaboration on data governance issues that has imprinted this paper. We thank Agustín Carstens and Nandan Nilekani for discussions on these (and related) issues over the years. We are grateful to Sanjay Jain, Saurabh Panjwani, Vamsi Madhav, B G Mahesh, Pramod Varma, Raphael Auer, Stijn Claessens, Jon Frost and Hyun Song Shin as well as participants at a BIS seminar for their comments on earlier drafts of this paper. Several conversations with Derryl D'Silva are also acknowledged. Martin Hood contributed helpful editorial advice. Shreya Ramann and Jenny Hung provided excellent support. All errors are ours.

* Bank for International Settlements
^ iSPIRT Foundation

Contents

The design of a data governance system

1. Introduction and summary

What is the problem around data?

Throughout history, consumers and businesses have generated data through their everyday choices. These data could relate, inter alia, to doctor's visits, purchases and sales of goods, or financial transactions. Traditionally, this information was paper-based and resided with the entities that engaged in these transactions (doctors, merchants and financial service providers).

Technological developments over the last two decades have led to an explosion in the availability of data and their processing (Feyen et al (2021)). The combination of the expanding consumer footprint, increased availability of data and inexpensive storage has provided the foundations for high-performance computation. It has also enabled the harnessing of very large amounts of consumer data – often referred to as "big data" – into a valuable commodity (Barocas and Nissenbaum (2014)). In such a setting, the key questions are who has control over these data, where they are stored, with whom and under what conditions they are shared, and who operates the data governance system.

Globally, most countries have privacy laws. These privacy laws have enabled countries to create accompanying legislation that recognises the rights of individuals over their data. Central to these laws is a set of principles that define how personal data are collected, shared, and processed. However, in spite of these laws, generators of data such as consumers and small and medium-sized enterprises (SMEs) do not have control over the data they generate and are denied the opportunity to reap the full value from their use (Solove (2013)). Inaccessible data, including data walled off in silos owned and operated by big tech firms, represent a significant cost to consumers and to society (OECD Library (2019)). These costs range from, on the one hand, consumers feeling disempowered and losing trust in the security of the system they live in, to, on the other hand, not reaping the benefits that data ownership would bring to them. At the same time, big tech firms aggregate and exploit personal data, but fail to fully pass on the resulting benefits to consumers (Solove (2013)).

Finally, there is a lack of global consensus on an optimal data governance system – both within a country and across borders (Matthan (2022), Basu (2021), Carstens (2019)).

Why is there a problem?

In most jurisdictions, laws give data subjects – consumers and businesses in this case – the opportunity to exercise control over their data through the granting or withholding of consent to the use and transfer of these data.

However, consumers find it difficult to effectively exercise this consent for a few reasons. First, a service provider usually seeks consent to use and transfer data at the time when a consumer agrees to participate in an activity with the service provider. Since this consent is sought ex ante and for a wide range of possibilities, it tends to be broad and sweeping in nature. Consumers – impatient and possibly ignorant of the value of the data they generate – quickly grant consent to gain access to the service.

Second, newly created data are often gathered and retained in proprietary silos and stored in various institutions in incompatible formats. Even when aware of their value, consumers find it difficult to access their own data as they are in different formats and in different locations, and consumers have only limited options for combining data requests across institutions.

What is the solution?

This paper proposes a data governance system that corrects for the above-mentioned market failures by restoring control of data to the consumers and merchants generating the data – whom we refer to as data subjects. The system allows data subjects to effectively operationalise their rights with regard to the collection, processing and sharing of their data and requires service providers such as social media channels or lenders – whom we refer to as data users – to always provide notice and seek the consent of data subjects prior to sharing and processing their data. Such a consent system would replace "broad and sweeping" consent with "granular" consent. In order for it to be adopted widely within a jurisdiction, it should be data subject- and data user-friendly, with low transaction costs. Such a consent-based system will empower data subjects to use their data for their own benefit.

The proposed data governance system is grounded in current national privacy laws in various jurisdictions that set out core data protection principles. The governance system describes how these privacy principles are operationalised. Given the granularity of data-sharing requests, the enormous amounts of data involved, the possibility of data being spread over several data users and providers (also referred to as "data controllers" below), and the need to keep the data secure and cost-effective, consent-based systems with the above characteristics must be digital to meet these objectives. For a digital system to operate effectively, it should embody the protocols that translate the privacy framework to the digital space. This will include elements from the so-called ORGANS principles on notice and consent, purpose limitation, data minimisation, retention restriction and use limitation (NITI Aayog (2020)). It will also need to be open, with consent that is revocable, granular, subject to audit, and with notice in a secure environment.

We argue that any solution would need to be part of a public-private partnership system and market-friendly. In the present situation, where data subjects are at a significant handicap, trust in the system as well as widespread adoption of the consent-based architecture has the potential to be significantly enhanced by mandating specialised data fiduciaries whose primary task – as advocates of data subjects – is to ensure that data are shared in a fashion that respects the above-mentioned principles of effective data governance.

The rest of the paper is organised as follows. In Part 2, we define the terms used in the paper as they relate to the participants in the data-sharing system, and the various classes of data that could be shared. Part 3 describes the present landscape as well as the challenges that confront data subjects. It outlines the societal and individual costs of the present system as well as the possibilities that could be realised if data subjects were enabled to utilise their data for their own benefit. In Part 4, we propose a consent-based data governance system that corrects for the market failures described above and levels the playing field between data subjects and data controllers. We also develop a granular template that can be used for benchmarking data governance systems in various jurisdictions. The template provides a useful road map to enable existing systems to transition from one where data controllers employ data for their own benefit to one where data custodians pass on these data to others for the benefit of data subjects. This section concludes with initial thoughts on the specific design features that will enhance the market adoption of this governance system in competitive markets. In Part 5, we describe the Data Empowerment and Protection Architecture (DEPA) in India and the data flows underpinning the application of DEPA to the financial sector. We then benchmark DEPA against the template developed in Part 4. We also describe some early lessons learned after the implementation of DEPA in September 2021. In Part 6, we offer some concluding thoughts including the challenges that policymakers will face in the cross-border applications of this system.

2. Data-sharing systems: participants and data

a. Participants in the data-sharing system

There are four participants[1] in the proposed data governance system (Graph 1):[2]

Data subjects: individuals, consumers, and businesses whose activities (online or physical) generate data, and to whom the personal data pertain.

Data providers: entities where data are stored, often also referred to as data controllers. These entities are service providers – such as financial institutions, big techs or healthcare professionals – which have collected and stored data on individuals and/or businesses and have effective control over those data.

Data users: entities that receive and or process data shared by data providers on data subjects, as an input for providing a service to either the data subject or for the data user's own account.

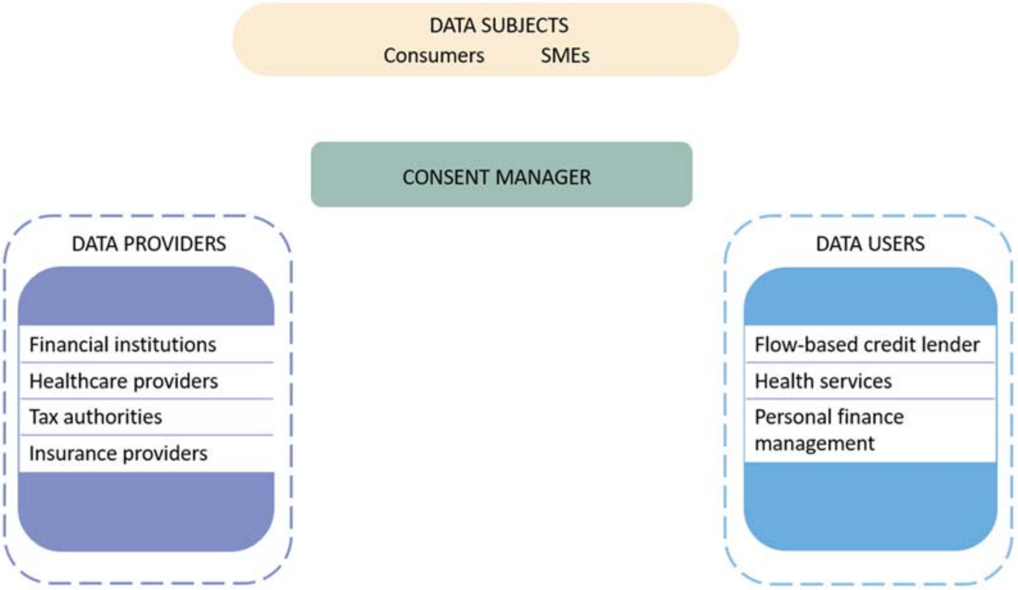
Specific entities are not restricted to being solely a data user or data provider, but can be either a data user or data provider depending on the data-sharing transaction they are involved in.

Consent managers: a licensed fiduciary who is the intermediary between data subjects, data providers and data users and – as an advocate for data subjects – ensures that the agreed rules for data-sharing and processing are being followed.

[1] Digital data are signed at source so that third-party verifiers – in the traditional sense – are not needed.

[2] The following discussion draws on NITI Aayog (2020).

Participants in the data-sharing system Graph 1



Source: Authors' elaboration.

b. Data taxonomy

In general, there are two classes of data: personal and non-personal data. Any data that are linked to a data subject's identity – ie they are personally identifiable – come under the category of personal data. From a data protection perspective, it is the data subject's personal data that are in the records (and under the control) of data controllers, and these data are subject to the rights of data portability. These two classes of data – personal and non-personal data – can be further disaggregated into constituent components. The data categories are:

1. Personal data

a. **Non-shareable data** – such as passwords and biometric data – are unique to the market participant. As the name suggests, this category of data is not subject to sharing, although it can be required to access a platform, subject to the relevant cyber security standards. In many countries, biometric identity, card personal identification numbers (PINs) etc form this class of data and subscribe to technology standards prevalent in the country.

b. **Profile data** – such as name, date of birth, gender and address, or health-related data such as vaccination status – comprise characteristics that change infrequently. While service providers quite often require the provision of such data to access their platform, user consent is required for sharing this category of data (often through electronic know-your-customer (eKYC) or digital lockers).

c. **Generated data**[3] – such as payments or borrowing transactions – are digital trails generated by the online activities of a consumer or SMEs. These data

[3] See discussion of generated and derived data in OECD (2014).

pertain to the activities of data subjects (consumers or SMEs) and consent is required for sharing this category of information. The service provider, in whose systems these data often reside, usually acts as the custodian for such data.

d. **Derived data** – such as credit scores – are developed by service providers through the mapping of generated data together with other attributes such as income, education status etc across users. In contrast to generated data, derived data consist of data drawn from the analysis of many data subjects (in the case of the big tech firms, millions of data subjects). That said, as such data could not be derived without the original generated data, the data subject has at least a partial claim to them, and some form of consent should be required for sharing data for which their generated data were an input.

2. **Non-personal data**[4]

a. **Anonymised data** – such as transaction data after removing personal identifiers – do not map to the identity of data subjects. These large data sets are crucial for scientific innovation (eg medical research or financial inclusion to name but a few). Typically, consent is not required for the sharing of these data, which need to meet anonymisation standards prevalent in the country to limit triangulation and ensure data anonymity. Some anonymised data are only available at group-level aggregates.

b. **Public data** – such as GDP, Covid infection and death rates, retail sales or jobs-related data – that are regularly released by the government and research institutes. These data provide crucial input for the conduct of public policy. Consent is not required for assembling these data sets (although, when based on surveys, the input is likely to be anonymous), which are regulated by law and subject to open standards.

The public policy issues concerning the storage, sharing and processing of data and the frameworks proposed in this paper pertain to all forms of personal data, whether they be non-shareable data that allow access to the platform, profile data related to the data subject (consumer or SME), generated data in which the data subject has a stake and for which the service provider acts as a custodian, or derived data that are co-owned by the data subject and the service provider. While there are also important policy issues relating to non-personal data, whether they be anonymised or public data, these are outside the purview of this paper.

3. The current landscape: opportunities and challenges

a. The explosion of data

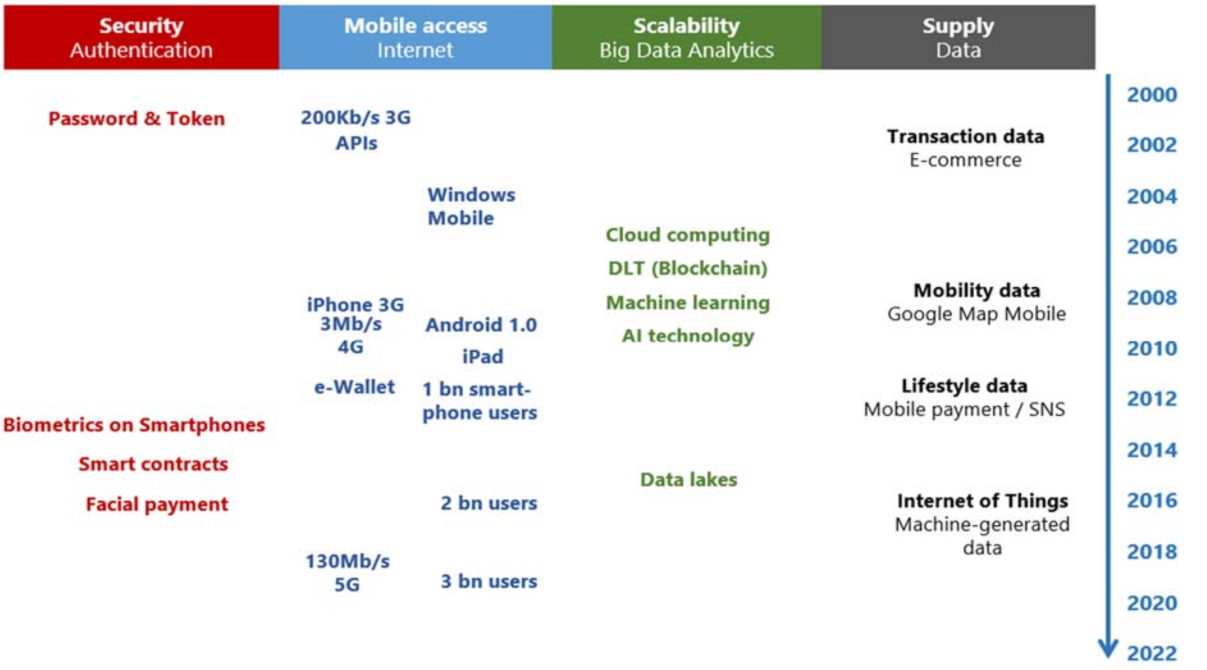
Recent technological developments have led to an explosion in the availability of data and their processing. With the advent of smartphones, digital technologies, software applications and network connectivity, the consumer digital footprint has expanded dramatically (McKinsey Digital (2021)). Users have also benefited from innovations such as cloud computing, which radically cut the cost of permanent storage while

[4] See discussion of non-personal data in Government of India, Ministry of Electronics and Information Technology (2020).

improving real-time global accessibility (Waibel et al (2017)). The combination of the expanding consumer footprint, increased availability of data and inexpensive storage has provided the foundations for high-performance computation. Real-time computation and communication between humans and machines, and between machines combined with intelligent human interfaces, have provided the groundwork for artificial intelligence, machine learning and deep learning.

Timeline of technology and digital financial infrastructure development

Graph 2



Source: Authors' elaboration.

It has also enabled the transformation of consumer data into a valuable commodity. In such a setting the key questions are who has control over these data, where they are stored, with whom and under what conditions they are shared, and who operates the data governance system.

b. Approaches to data governance

There have been two important milestones in the development of approaches to data governance. First, in the United States, as early as the 1970s, the obligations of data controllers were set down in a US Department of Health, Education and Welfare report – later known as the Fair Information Practices Principles (FIPPs) – which included transparency of the record system, ensuring data quality, provisions to data subjects of notice of collection, right of access, right to prevent collection being used for alternative purposes and the right to correct errors, as well as data security protections (United States Department of Health, Education and Welfare (1973)). A streamlined version of the FIPPs was recommended by a US Federal Trade Commission report in 2000, by which time online business was expanding and companies were developing policies that effectively incorporated the FIPPs on a voluntary basis into their terms of services on the internet. Customers received notice and gave consent prior to gaining use of service. At the time, this was viewed as sufficient and appropriate as a means of giving subjects authority over the data being collected from them (Schwartz and Solove (2009)). As the volume and value of data increased – with accompanying increases in data collection practices – data subjects pressed for more changes. In 2018, the State of California enacted a Privacy Act guaranteeing six privacy rights to individuals, including the right to see their personal information, the right to know what information is being collected about them and how it is used and shared, the right to delete information collected about them (ie, the right to be forgotten), the right to opt out of the sale of their data, and the right to non-discrimination for exercising their data rights.

Second, in Europe, the 1995 European Union (EU) Data Protection Directive, largely inspired by the FIPPs, also focused on the collection and processing of data. Subsequently, the General Data Protection Regulation (GDPR), which was adopted in 2016 and came into force in 2018, set out seven principles – fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability (European Union (2018)). The EU is now widely recognised as the global leader in data regulation and the GDPR is the principal data protection regulation in Europe.

That said, the GDPR still stipulates consent as the primary ground for the processing of personal data. Further, the requirement of notice and consent prior to collection, processing and sharing of data is hard to enforce under the present framework. The same is true for the requirement to use open interoperable standards for data-sharing, and for granular consent requests that specify the data and the length of retention. While data collectors are subject to strict compliance obligations, technology companies are still free to operate in much the same way as before simply by obtaining prior consent to do so. There remains an imbalance between the scope of the law and the ability of the system to fully implement it.[5]

c. Challenges posed by the current system

Globally, most countries have laws that recognise the rights of individuals over the data that pertain to them.[6] These laws give data subjects – consumers and businesses in this case – the opportunity to exercise control over their data by granting or withholding consent to the use and transfer of these data. However, consumers find it difficult to exercise this consent effectively for three reasons. First, a service provider usually seeks consent to use and transfer data at the time when a consumer agrees to participate in an activity with the service provider. Since this consent is sought ex ante and for a wide range of possibilities, it tends to be broad and sweeping in nature (Solove (2013)). Second, consumers in many cases may not be fully cognisant of the value of the data that pertain to them (Barocas and Nissenbaum (2014)). Third, newly created data are often gathered and retained in proprietary digital platforms – "data silos" – and stored on these corporate platforms in incompatible formats (van der Vlist and Helmond (2021)). Even when the value of data is recognised by consumers,

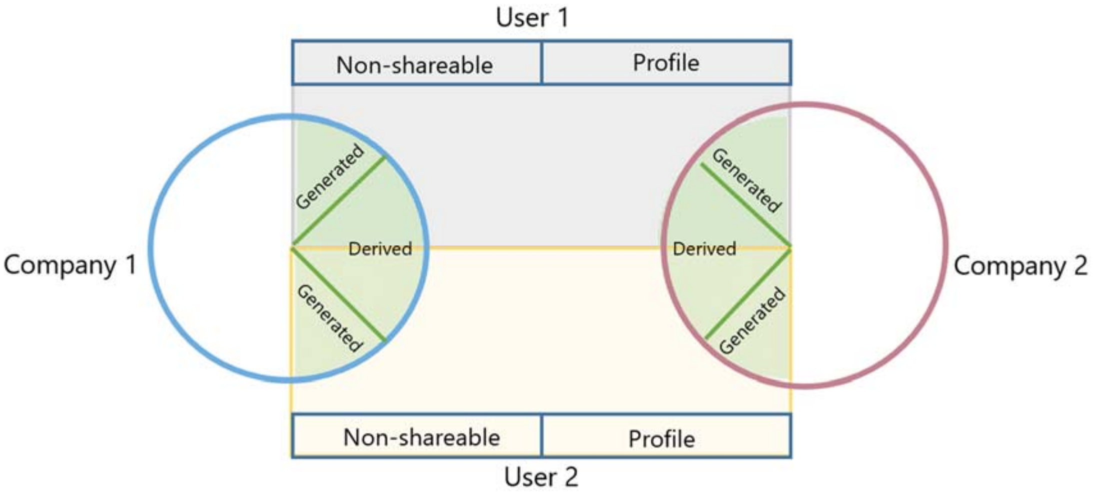
[5] Another issue is that existing rules such as the GDPR and the California Consumer Privacy Act may have benefitted large players at the expense of small entrants, for whom compliance is more expensive. See Canayaz et al (2021).

[6] See European Union (2018), and also The Treasury, Australia (2019).

they can find it difficult to access and share their data as they have only limited options for combining data requests across institutions (van Ooijen and Vrabec (2019)).

Data silos: Firms hoard the data of users

Graph 3



Source: Authors' elaboration.

Based on the data taxonomy presented earlier, the loss of value suffered by data subjects because their data are locked up in data silos is depicted in Graph 3. In this stylised example, User 1 and User 2 sign up for services from Company 1 and Company 2. Under the current system, prior to making the service available, Company 1 and Company 2 make the provision of service conditional on ex ante broad and sweeping consent. As User 1 and User 2 (*data subjects*) use the service, they leave behind digital trails (*generated data*) from their online activities, and their generated data are now under the control of Company 1 and Company 2. In turn, the companies combine their generated data with other attributes (such as income and education) to derive insights and predictions, thus creating *derived data* across users. Derived data could not have been created without the original generated data of many users and thus the data subjects conceivably have at least a partial claim to the value of derived data. In reality, users have access to neither their generated data nor the data derived from it across users. As they sign on to more services, this cycle repeats itself. In the extreme – with the exception of non-shareable and profile data – the entire set of data pertaining to a user could be under the control of their service providers.

At an aggregate level, inaccessible data, because they are isolated in silos, represent a significant cost to society and to data subjects. Examples of societal costs include compromising trust in a competitive commercial and financial system as "value" is traded without the participation of those who created it (see Morey et al (2015))[7], and loss of the ability to generate the large anonymised data sets that are

[7] The willingness to share personal data and trust in different counterparties can differ across demographic groups. See Armantier et al (2021).

crucial for research and development, thus driving innovation (see World Economic Forum (2021)).

At an individual level, the benefits derived by the sharing of own data are also not fully appreciated and utilised. This is particularly noteworthy in consumer lending. For example, the World Bank's Findex data show that only a small fraction of bank account holders in the formal system borrow from the system (Demirgüç-Kunt et al (2018)). This is not solely a developing country or emerging market economy phenomenon. It is true even in jurisdictions with high income, good education (including financial literacy), near universal accounts in financial institutions, and deep mobile penetration (Demirgüç-Kunt et al (2018), Croxson et al (2022)). There are two reasons for this. First, tangible collateral has traditionally been key to consumer lending. The young take time to accumulate tangible collateral and the poor may never acquire sufficient collateral. Second, these low-margin, high-risk consumers are uneconomical to reach in the traditional system without access to digital data-sharing. To be sure, financial companies are increasingly using technology to exploit the data footprints of individuals and firms, thus generating information capital and allowing for a reduced reliance on tangible collateral when offering loans and other financial services. In such a setting, increasing the ability of individuals to access and share their information capital is crucial to enhancing financial access for the young and the poor.[8]

It is noteworthy that the European Commission has judged it necessary to have measures in addition to the GDPR to foster government-business data-sharing as well as to require data-sharing among businesses. The challenges associated with big data – both the substantially larger volumes and more complex processes of data collection – require a more comprehensive framework for data collection. The EU is currently considering additional legislation – the Data Act to increase access and use of data, the Data Governance Act to create platforms for the exchange of data and the Digital Markets Act to ensure that data guardians do not hamper innovation – to help unlock data currently in silos and more effectively enforce the broad data protection framework contained in the GDPR.

Advances in technology also have the potential to help unwind some of these intertwined challenges. A robust data governance system could help consumers/SMEs to derive value from their data while maintaining control of them. Such a system should be able to accommodate a large volume of data, multiple data users, and observe the basic principles of data privacy. It should be data user- and data provider-friendly and operate securely at low transaction costs.

4. Proposed consent-based data governance system

a. General considerations

In this section, we propose a consent-based data governance system that corrects the market failures described above and empowers consumers and businesses to use the data they create for their own benefit. Such a system starts with the proposition that data control rests with those who create the data. Giving consumers control over

[8] See Chen et al (2022) and references therein.

their data can improve overall efficiency and increase welfare (Jones and Tonetti (2020), Carrière-Swallow and Haksar (2019)).

There are two building blocks for an effective consent-based data-sharing system.

- **A data protection policy framework.** It is common practice that privacy (and data rights) is defined through domestic laws that recognise privacy (and data rights). In this manner, an overall consistency of approach is ensured across sectors, as cross-sectoral portability of data is crucial to an effective data governance framework (OECD (2021)). These rights then cascade down to a particular sector consistent with the overall national objective.[9]

  In the proposed framework, data subjects are empowered to use the data they create for their own benefit through two avenues. First, when the data protection policy framework recognises the rights of data subjects over the data they create – whether these data reside with them or not. Second, when the data governance system asks for the consent of the data subjects prior to the processing and sharing of data, which is consistent with the provision of notice prior to the collection, sharing and processing of data.

- **A technological infrastructure that enables a user-friendly implementation of the data protection policy framework**. The technological infrastructure should be sector-agnostic to allow for cross-sectoral **applications**. To accommodate the many players involved such as financial and data services providers as well as both public and private sector institutions, the platforms upon which the infrastructure operates should be open, interoperable and non-discriminatory. At the same time, their design should ensure data security.

  Given the need for granularity of consent, and given that data are to be spread among many users and providers, the quantity of data that need to be managed within the system is enormous. To achieve cost savings, data management must be digitally based and scalable across large numbers of users.

  Ensuring that data are controlled by those that generate them is in some respects more difficult than before given the speed and ease with which digital data can be copied. That said, technological progress offers the prospects of a variety of solutions for consent-based data sharing, such as a confidential clean room, where data can be processed and results obtained, without extracting the personally identifiable data themselves.

b. The conditions for data-sharing

When data are shared between data providers and data users, the data governance system should specify which data are requested for sharing, how long they will be retained by data users, and who will process them. In these areas, the system should meet the following five standards.[10]

[9] An important exception is India, where, in the absence of a national framework currently being debated in the Parliament, sectoral data-sharing policy frameworks and laws are leading the way. The sectoral approaches are built around the ORGANS principles (see below).

[10] See Article 5 in European Union (2018), and also OECD (2013).

(i) **purpose limitation,** ie ensure that the purpose for which data are being shared is described in clear and specific terms;
(ii) **data minimisation,** ie share only as much data as are strictly necessary to achieve the stated purpose;
(iii) **retention restriction,** ie ensure that data are not shared for longer than required to achieve the stated purpose;
(iv) **use limitation,** ie ensure that data are used only for the purpose for which they were shared; and,
(v) **operational resilience,** ie ensure that data are secure and the overall system is resilient to unauthorised access.

c. ORGANS principles

State-of-the-art digital consent systems are built around the so-called ORGANS principles[11] (referring to Open, Revocable, Granular, Auditable, Notice and Secure), which form the foundation for unbundling the single act of giving consent to collect, process and share data. To obviate the need for provision of broad and sweeping ex ante consent, as is now the case, the granting of consent should be made more granular, specifying to whom data are provided, for how long and for what purpose. Since multiple players are involved in data-sharing – such as financial service providers, data services providers and data held by the government – the system must be open and interoperable. Data subjects should provide consent just before data are shared, it should be revocable once provided, and data subjects should have the right to audit data-sharing transactions ex post.

The ORGANS principles are:

- **Open**: require the use of open, interoperable standards for the sharing of data.
- **Revocable**: enable the revocation of consent once provided by the data subject; this includes the right to be forgotten, ie data subjects' data need to be deleted.
- **Granular**: allow for consent to be provided in granular fashion just before data are shared. Granular consent requests – specifying which data are requested, how long they will be retained, and who will process them – satisfies purpose limitation,[12] data minimisation,[13] retention restriction[14] and use limitation.[15] Such granular consent can be granted on a recurring basis under similar conditions.
- **Auditable**: give data subjects the right to audit data-sharing transactions. Ease of audit requires machine-readable records of all consent provided by data subjects.
- **Notice**: recognise consent as a requirement for processing and sharing of data and require a notice of consent prior to collection, processing and sharing of data. The notice of consent sets forth the obligation to obtain the informed consent of the data subjects with the granular details described above prior to the collection, processing and sharing of data.

[11] This section draws on NITI Aayog (2020).

[12] The obligation to ensure that the purpose for which data are being collected is described in clear and specific terms.

[13] The obligation to collect only as much data as are strictly necessary to achieve the stated purpose.

[14] The obligation to ensure that data are not retained for longer than required to achieve the stated purpose.

[15] The obligation to ensure that data are only used for the purpose for which they were collected.

- **Secure**: impose data security obligations on data controllers. The consent artifact must subscribe to the highest standards of data providers and data users.

There is little to prevent data users from using data for their own purposes because digital data can be copied. Even in the best designed systems, ensuring use limitation is a challenge because – with the currently available technology – it is difficult to enforce. However, advances in technology provide for the possibility of technological solutions to ensure use limitation. One possibility is a confidential clean room environment in which the data user can process the data and extract the results of the analysis but not the personally identifiable data themselves (Mehta (2021)). Because data never leave the execution environment, this architecture when available will provide a high degree of assurance regarding use limitation.

d. Granular template underpinning the proposed data governance system

In this subsection, we develop a granular template which describes the proposed data governance framework that combines the data protection principles and the protocols for electronic consent with conditions supportive of consumer adoption. Table 1 takes as given that privacy regulations are enshrined in core legislative principles and that personal data are increasingly portable. As mentioned earlier, the governance architecture includes both a data protection policy framework, whereby data rights and privacy are defined through laws that recognise rights and privacy on a national basis, and a technological infrastructure that enables a user-friendly sectoral implementation of the framework though software code.

The data protection policy framework (Table 1, left-hand side) governing the processing and sharing of data is the starting point in any jurisdiction. The framework focuses on empowering data subjects (individuals and businesses) by granting them the right to the benefits that are derived from the store of value embodied in the data they created. It covers all the specific dimensions outlined above, including both the five data-sharing principles, as well as the ORGANS principles.[16] Technology offers protocols and tools to implement the data protection principles outlined above. This will ensure that the rights available to users under various regulations can be enforced through code.

[16] The ORGANS principles are intended to apply to technological protocols, and are thus not inclusive of all data protection principles.

Granular template underpinning the proposed data governance system

Table 1

	Data protection policy framework	Technology infrastructure
	The jurisdiction or one or more sectors within the jurisdiction has laws/policies that:	*In one or more sectors or cross-sectoral, standard interoperable technology structure is in place that:*
Data rights:	Recognises the rights of the data subjects over their data even if such data are under the control of data providers (controllers).	Enables the sharing of data between data providers (controllers) and data users with the electronic consent of data subjects.
Framework:	Governs the sharing of data.	Enables the sharing of data.
Open:	Requires the use of open interoperable standards for the sharing of data.	Enables the sharing of data that has been built using open, interoperable standards.
Interoperability of framework:	The same framework applies across sectors	The same framework applies across sectors
Notice and consent:	Recognises consent as a legitimate ground for processing and sharing of personal data and require notice prior to collection, processing or sharing of data.	Implements the principles of notice and consent in an electronic format.
Consent manager:	Allows for the establishment of consent intermediaries.	Implements a digital framework for consent intermediaries.
Granular:	Allows for consent to be provided in a granular fashion just before the data are shared.	Implements granular consent for data-sharing electronically.
Revocable:	Enables the revocation of consent once provided.	Implements the electronic revocation of consent for data-sharing.
Auditable:	Gives users the right to audit data-sharing transactions.	Enables the electronic audit of data-sharing transactions.
Data security:	Imposes data security obligations on data providers (controllers) and data users.	Builds data security into the design of the infrastructure.
Consumer adoption:	Implements measures to encourage consumer adoption such as simplification obligations, standardisation norms etc.	Encourages consumer adoption through, inter alia, inclusive user interfaces, transaction simplification for first-time digital users etc.

e. Oversight of regulatory and technological standards

The principles, and the granular template for conditions that best combines these principles with technological protocols for electronic consent, have been covered in the previous sections. In this section, we describe a typical oversight framework that has been used for other digital public infrastructures and has the potential to play the same role here.

The governance of digital public infrastructure (DPI) involves two distinct building blocks. First, the policy framework that defines the architecture and the accompanying operational framework which implements the policy guidelines; and second, a technological component for the efficient functioning (including the upkeep) of the architecture, including periodic auditing and updating of the technological protocols and standards.

The structure described above lends itself to three institutions with defined roles and responsibilities:

1. **The regulatory authority**. The policymaking body, which may be a statutory, executive body of the government, should be responsible for creating a legal ringfence around the DPI, ensuring, through guidelines and executive policies, that the state provides the normative and institutional basis for the adoption and implementation of the technical architecture. It articulates the principles by which the infrastructure should operate, most importantly that it should be open and non-exclusionary, and that it should not discriminate among market participants.
2. **The self-regulating organisation (SRO)**. An SRO is responsible for the actual implementation of the framework defined by the regulator.[17] As the name suggests, the SRO – an alliance of entities that have a stake in the system – is self-governed with its own institutional framework and rules of business. The key responsibilities of an SRO are threefold: (i) to be the conduit through which sectoral policymakers and regulators interact with market participants on the DPI; (ii) to run the dispute resolution system between market participants; and (iii) to certify the proper adoption of the DPI by market participants as they develop their own user-facing apps and services. The SRO has a critical role to play in enforcing the twin principles of interoperability and non-discrimination that are critical to the smooth and effective adoption of the DPI, as articulated by the regulator.
3. **The technology standards organisation (TSO).** A TSO maintains the technical standards that underpin the digital public infrastructure. More than either the regulatory authority or the SRO, it is responsible for the maintenance of the standards.[18]

[17] While some may see the government as taking this role, there are risks to the government being a player, regulator and standard setter in the same market. These include the state picking national champions, which can negatively impact the quality of technical standards through a risk-averse decision-making process. Accountability to market players and the technical community is compromised.

[18] TSOs can be organised in different ways, but one well known model is that of the World Wide Web Consortium (W3C). This is an international community that develops open standards to ensure the long-term growth of the web, most prominently in the development of HTML standards a few decades ago. Software standards developed by the W3C are open and available to all.

It is worth noting that multi-tiered models of oversight do not necessarily envisage a dominant role for the state in the standards development process.[19] Rather, what is formalised are consultations with the government.

f. Creating conditions for market adoption

The success of large-scale public policy initiatives lies in the public sector setting the institutional and regulatory framework and the private sector then designing consumer interfaces to drive market adoption. In the case of data, three building blocks are crucial for market adoption.[20] They are:

- Data portability. This involves some of the principles outlined above, including clarity that data subjects have rights to the data they created, including the right to move the data from one provider to another, as well as open and interoperable consent mechanisms that are user-friendly, low cost, real time, efficient and secure.
- Getting prices right. As market participants need to recover costs in any market system, the prices charged need to be market-determined.
- Keeping the data marketplace competitive. While market participants must be able to recover costs, oversight of the system should ensure that the prices set do not bar access to data by data subjects.

Once the right framework is in place, developing a consent-based system to scale is key to its success. There are several examples of building technological solutions to scale; India alone offers recent illustrations in the areas of both identity and payments.[21] Here, India has utilised a financial technology stack in which a unified, multi-layered set of public sector digital platforms combine to provide substantial benefits to the population, from promoting financial inclusion and increasing efficiency to enhancing financial stability. In this framework, the official sector defines the regulatory framework and the private sector is encouraged to engage in innovation and manage the consumer interface. In other words, it seeks to build a balanced framework between protecting consumers on the one hand and supporting market innovation on the other. A data governance system is the next critical layer in a country’s financial technology stack.[22]

[19] In the case of DEPA, the above-described role of the SRO is filled by a not-for-profit private limited company, the DigiSahamati Foundation (Sahamati), a self-organised Industry Alliance for the Account Aggregator ecosystem. While the regulatory authority is the Reserve Bank of India (RBI), the TSO is the Reserve Bank Information Technology Private Limited (ReBIT), a fully owned subsidiary of the RBI. See Rao (2021).

[20] See discussion in OECD (2021).

[21] These examples allowed the widespread opening of bank accounts and advances in the payments system. A digital ID system, steered by the state, has helped more than a billion people to gain access to the banking system. Layered upon this is a fast payments system – the unified payments interface (UPI) – that is interoperable, allows open/contestable entry and operates within the regulatory framework. It has made payments services universally available in the country with over 4 billion transactions every month. See discussion in D D'Silva et al (2019).

[22] For further information on the India Stack, see https://indiastack.org/data.html.

5. Data Empowerment Protection Architecture (DEPA) in India[23]

This section describes the evolving application of the consent-based data governance system in India. At the national level, the data governance system, DEPA, reflects the proposition that data subjects (consumers, SMEs and in some instances service providers) should have a stake in what is created. In DEPA, data subjects – through a granular data consent system – are expected to control what data they wish to share, with whom and for how long.

An effective data governance system as described in Part 4 above – encompassing notice and consent, purpose limitation, data minimisation, retention restriction and use limitation – can only be implemented digitally. In India, the data protection policy framework that defines how personal data can be collected and processed has a technological framework as its counterpart: the principles of DEPA are implemented in software codes.

a. Application of DEPA to the financial sector

While the overall data protection policy framework has yet to be enacted in law, it has been adapted to – and is operational in – the financial sector through the Account Aggregator system, which went live in September 2021 (Graph 4).[24]

In the financial sector, the data governance system works as follows. Before a data subject initiates a data transfer, the subject needs to enrol with a consent manager (CM), and in so doing provides a list of approved data providers/controllers to the consent manager (1). When a data subject seeks service from a data user (2) – which, for instance, can comprise parties such as lenders, insurance companies and personal finance managers – the data user initiates a data transfer request (3), which is submitted to the CM. The data user chooses a template from a suite of templates designed for this – specifying the purpose of the data transfer, the specific data that are needed to satisfy that purpose and the duration for which they will be retained – and picks the data request format that meets the requirements of the request. While, on the one hand, these templates cover a broad range of uses for which data may be requested, on the other hand, they ensure that only the minimum amount of data needed for the purpose at hand is requested, thus meeting the principles of notice, consent, purpose limitation and data minimisation. In addition, this framework precludes a data dump (which is prevalent today) as a data dump makes processing costs to extract useful information prohibitively high, thereby rendering the data not useful.

Only after the data subject has provided the consent for sharing data (4) does the CM submit this request to the data providers (5). The data providers, in turn, can include financial information providers, tax platforms and insurance providers, among others. After verifying the request, the data provider transfers the data through an

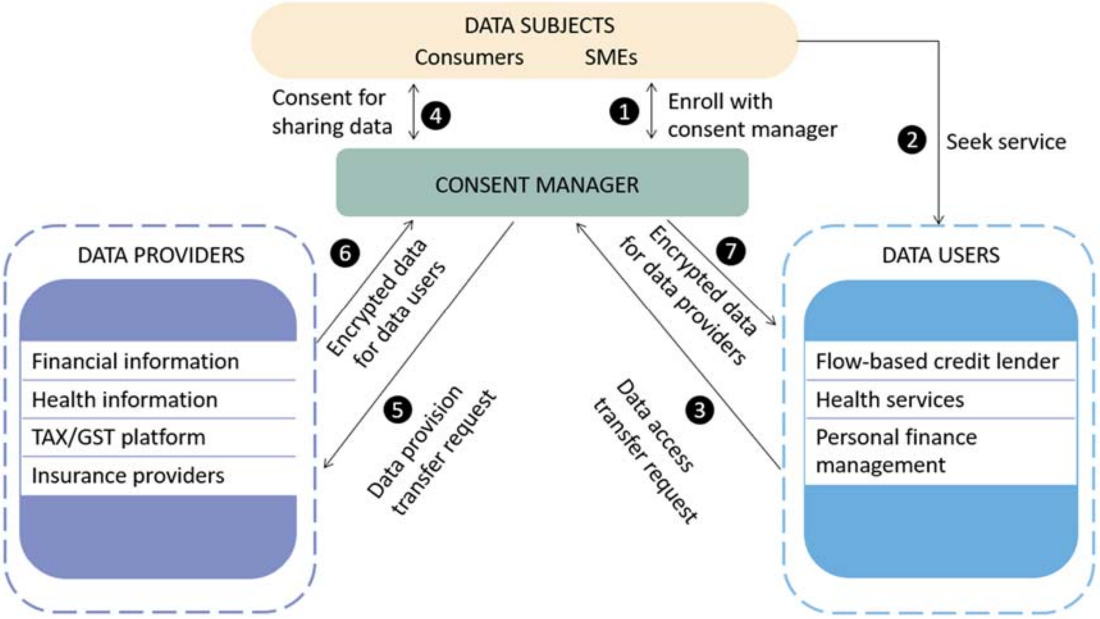
[23] The discussion in this section draws considerably on NITI Aayog (2020) and iSPIRT Foundation (2021).

[24] See Reserve Bank of India (2021). The Data Protection Bill, which covers a much broader mandate of privacy protections, is expected to be enacted into law in 2022.

end-to-end encrypted flow to the consent manager (6), who shares the data with the data user.[25]

India: financial sector data-sharing system

Graph 4



Source: Authors' elaboration.

In this series of transactions, the CM is aware of the identity of both the data users and data providers, but blind to the content of the data that the CM is transferring. Data users, on the other hand, are aware of the content of the data but blind to the identity of the data provider. Similarly, data providers are aware of the content of the data but blind to the identity of the data user. Through the consent manager, data flows are separated from consent flows, thereby ensuring the efficient transfer of data while respecting privacy concerns.

This structure, while vastly improved over most earlier consent systems, does not ensure that the data user is using the information only for the purpose for which data were shared or keeping them only for the period initially agreed. In other words, once the data are shared with the data user, there is no feature in this architecture that can assure the data subject that the principle of use limitation will be satisfied. Thus, the next advance in this architecture will be the addition of a confidential clean room environment in which the data user can process the data and extract the results of the analysis but not the personally identifiable information data themselves (iSPIRT Foundation (2021)). Because data never leave the execution environment, this architecture, when it becomes available, will provide a high degree of assurance regarding use limitation and increase incentives to share data.

[25] Public key-based cryptography can ensure that data are shared securely. For a discussion of the use of payment APIs to ensure that the technical standards ensure interoperability as well as the security of the data exchange, see BIS (2021).

b. Costs incurred in DEPA operations

Unlike other large digital public infrastructures in India, such as the digital identity system (Aadhaar) or the fast payments system (UPI), the architecture of the financial sector data-sharing system (Account Aggregator) entails no large upfront costs. In an open and competitive market, the data rails (flows 1, 2, 3, 4, 5, 6 and 7 in Graph 4 above) on which data move are provided and managed by technology service providers (TSPs). In particular, all market participants – consent managers, data users and data providers – use the services of TSPs to onboard themselves into the financial sector data-sharing system.

In terms of costs, TSPs charge an upfront fee to implement the Consent Manager/Data User/Data Provider module and a fee per data pull – charged to the data user – for using the TSP's services. In a competitive marketplace, prices differ according to the suite of services offered. In a recent survey, the three packages offered by TSPs included:

- An INR 100,000 (USD 1,333)[26] fee charged to data users for accessing the services of the TSP plus a fee of INR 5 (equivalent to USD 0.07) per data pull.
- A one-time fee of INR 1,400,000 (equivalent to USD 18,667) charged for the use of services offered by the TSP company plus the normal annual maintenance charges. In this bundle, no usage-related fee is charged to data users by the TSP.
- An annual fee of INR 1,300,000 (USD 17,333) charged which includes unlimited access to TSP services as well as round-the-clock support by two technical staff.

Irrespective of the suite of services offered, it is clear that under the current circumstances with many TSPs operating in the marketplace, the marginal cost of a data pull to consumers is modest.

c. Benchmarking DEPA against the proposed data governance system

In this section, we benchmark the data governance architecture in India (NITI Aayog (2020)) against the proposals outlined in Part 4. While Table 2 takes as given that privacy regulations are enshrined in core legislative principles, these are still being debated in the Indian Parliament.

With regard to the data protection policy framework (Table 2, left-hand side), a framework that governs the sharing of data has been developed only for the financial sector (Reserve Bank of India (2016)). For this reason, the data protection policy framework can be viewed as only partially in place to ensure data governance in line with the attribute of interoperability. With this caveat in mind, the Indian framework focuses on empowering data subjects (individuals and businesses), by granting them the right of ownership to the data they own and the benefits that are derived from them. It covers all the other specific dimensions defined in Table 1, including the ORGANS principles outlined earlier.

[26] The exchange rate used for this and the subsequent estimations of US dollar costs is 75 INR per USD.

Benchmarking the data empowerment and protection architecture in India

Table 2

INDIA	**Data protection policy framework**		**Technology infrastructure**	
	The jurisdiction or one or more sectors within the jurisdiction has laws/policies that:	*Nationally or within a sector*	*In one or more sectors or cross-sectoral, a standard interoperable technology structure is in place that:*	*In one/ more sectors*
Data rights:	Recognises the rights of the data subjects over their data even if such data are under the control of data providers (controllers).	🟩	Enables the sharing of data between data providers (controllers) and data users with the electronic consent of data subjects.	🟩
Framework:	Governs the sharing of data.	🟩	Enables the sharing of data.	🟩
Open:	Requires the use of open interoperable standards for the sharing of data.	🟩	Enables the sharing of data that have been built using open, interoperable standards.	🟩
Interoperability of framework:	The same framework applies across sectors	🟧🟥	The same framework applies across sectors	🟧🟥
Notice and consent:	Recognises consent as a legitimate ground for processing and sharing of personal data and require notice prior to collection, processing or sharing of data.	🟩	Implements the principles of notice and consent in an electronic format.	🟩
Consent manager:	Allows for the establishment of consent intermediaries.	🟩	Implements a digital framework for consent intermediaries.	🟩
Granular:	Allows for consent to be provided in a granular fashion just before the data are shared.	🟩	Implements granular consent for data-sharing electronically.	🟩
Revocable:	Enables the revocation of consent once provided.	🟩	Implements the electronic revocation of consent for data-sharing.	🟩
Auditable:	Gives users the right to audit data-sharing transactions.	🟩	Enables the electronic audit of data-sharing transactions.	🟩
Data security:	Imposes data security obligations on data providers (controllers) and data users.	🟩	Builds data security into the design of the infrastructure.	🟩
Consumer adoption:	Implements measures to encourage consumer adoption such as simplification obligations, standardisation norms etc.	🟩	Encourages consumer adoption through, inter alia, inclusive user interfaces, transaction simplification for first-time digital users etc.	🟩

Note on colour scheme: Green indicates that the requisite data protection policy framework (left-hand side), or technology infrastructure (right-hand side) is in place to ensure data governance in line with the specific described attribute (row). Interoperability of framework is the only attribute which has been marked half-red in terms of both the data protection policy framework and the technology infrastructure. This is because the data protection policy framework has been developed only for the financial sector, and the Account Aggregator framework is currently interoperable only across four sectors in the financial system: banking, insurance, pensions and securities. The aim is to broaden the application of the Account Aggregator framework to non-financial sectors.

On the technology infrastructure side, India has the necessary standard of interoperable technology infrastructure in place for data governance (Table 2, right-hand columns). However, the framework in India applies to four sectors in the financial services industry – banking, insurance, pensions, and securities. For this reason, as with the data protection policy framework, the technology infrastructure can be said to be only partially in place to ensure data governance in line with the attribute of framework interoperability.

d. Early results[27]

DEPA went live in the financial sector in September 2021. As of 14 April 2022, nine banks were fully operational as financial information providers (FIPs). These nine banks have a combined total of 215 million individual savings, term deposits plus sole proprietor current accounts. On the other side, there are 35 financial information users (FIUs), predominantly non-banks, banks and a handful of registered investment advisors that are fully operational, or live.

There are 10 licensed consent managers known as Account Aggregators, of which 50% are fully operational.

India: Entities operational in the financial sector data consent management system

Table 3

	Financial information providers	Financial Information users
Banks	9	9
Non-banks	0	20
Wealth advisors	0	4
PFRDA registered entities	0	2
Total	9	35

Source: Statistics received from DigiSahamati Foundation (Sahamati), current as of 14 April 2022.
Note: PRFDA stands for the Pension Fund Regulatory and Development Authority.

In terms of the system's actual usage, 230,000 consent requests from the FIUs were processed over the initial 30 weeks, thus averaging around 1,000 consent requests daily. In about 90–95% of cases, the FIPs have successfully addressed consent requests with an average response time in seconds. For the remaining 5–10%, consent requests have not been addressed due to a combination of issues, including operational restrictions of FIPs to include only single-owner accounts at this stage, one-time password delays causing failures in the linking of accounts to Account Aggregators' systems, and, in some instances, user hesitation in proceeding with a consent request.

A larger number of entities across various financial sectors are currently engaged at some level in the Account Aggregator ecosystem (either live, testing, in the tech development stage or evaluating). When participation is defined this broadly, 41 banks are engaged as FIPs and FIUs, while 56 non-banks are engaged are FIUs. In total, 56 institutions are engaged as FIPs and 133 are engaged as FIUs.

The system is market-driven, with participants renumerated for the costs they incur. It allows data subjects to benefit from the data they create, while providing for

[27] All data are sourced from Sahamati, https://sahamati.org.in/.

both financial information providers and users to benefit from activities that make full use of their information capital.

6. Concluding thoughts

Technological developments over the last two decades have led to an explosion in the availability of data and their processing. This has also transformed big data into a valuable commodity. Globally, most countries have privacy laws and accompanying legislation that recognise the rights of individuals over their data. Central to these laws is a set of principles that define how personal data are collected, shared and processed. However, in spite of these laws, data subjects do not have control over the data they generate and are denied the opportunity to reap the full value from their use. This is because consent mechanisms are too broad and sweeping, and newly created data are often kept in data silos under the control of a single company. Inaccessible data represent a significant cost to consumers and to society.

In this paper, we have proposed a data governance system that restores control of data to data subjects with regard to the collection, processing and sharing of their data. This framework – which replaces broad and sweeping consent with granular consent provided on digital basis – is influenced by the privacy laws prevalent in many jurisdictions. Given the granularity and amount of data spread over numerous data subjects and data controllers, only a digital system can be secure and operate at low transaction costs. Thus, technological protocols for notice and consent, purpose limitation, data minimisation, retention restriction and use limitation play a key role in operationalising the data governance framework.

Large public digital infrastructures for commercial use are successful when designed as part of a public-private partnership, where the public sector creates the foundations (legal and policy underpinnings) for the private sector to develop and maintain the (technological) underpinnings of the consumer interface. The data governance system we propose is no exception. With this in mind, we also develop a template that can be used for benchmarking data governance systems across various jurisdictions. The template can serve as a useful guide for any particular jurisdiction that wishes to modify its data governance framework so as to empower data subjects to use their own data for their own benefit. It also offers pointers on how to encourage greater market adoption by lowering transaction costs. We also present a representative oversight framework for digital public infrastructure comprising a regulatory authority, a self-regulating organisation, and a technology standards organisation.

A good example of such a framework can be found in India's Data Empowerment and Protection Architecture (DEPA) and the way in which data flows are managed in the application of DEPA to the financial sector. This consent system embodies the protocols that translate privacy principles to the digital space, not least by mandating specialised data fiduciaries whose primary task – as the advocates of data subjects – is to ensure that data are shared in a fashion that respects widely agreed principles of effective data governance. The early results from the account aggregator framework are encouraging.

Although the proposed framework for consent-based data governance has the flexibility to be applied across multiple jurisdictions to enhance domestic efficiencies, this paper has not addressed the conditions for the development of common, interoperable protocols for data-sharing across countries. There is a lack of global consensus on an optimal data governance system – both within countries and across borders. How consent frameworks can be made interoperable across jurisdictions to streamline and secure data flows is a topic that is attracting an increasing amount of interest. One likely condition is that jurisdictions arrive at a common understanding of the value of protecting internet users, and the promotion of fair competition in the digital economy.

References

Armantier, O, S Doerr, J Frost, A Fuster and K Shue (2021): "Whom do consumers trust with their data? US survey evidence", *BIS Bulletin*, no 42, May.

Bank for International Settlements (2021): *Annual Economic Report 2021*, Chapter 3, "CBDCs: an opportunity for the monetary system", June.

Barocas, S and H Nissenbaum (2014): *Big data's end run around anonymity and consent*, Cambridge University Press.

Basu, A (2021): "Sovereignty in a 'datafied' world: A framework for Indian diplomacy: A 2030 Vision for India's Economic Diplomacy", Observer Research Foundation, May.

Canayaz, M, I Kantorovitch, R Mihet, S Abis and H Tang (2021): "Privacy Laws and Value of Personal Data", *Swiss Finance Institute Research Paper*, no 21-92, December.

Carrière-Swallow, Y and V Haksar (2019): "The Economics and Implications of Data: An Integrated Perspective", *IMF Departmental Papers*, no 2019/013, September.

Carstens, A (2019): "Data, technology and policy coordination", keynote speech at the 55th SEACEN Governors' Conference and High-level Seminar, Singapore, 14 November.

Chen, S, D D'Silva, F Packer and S Tiwari (2022): "Virtual banking and beyond", *BIS Papers*, no 120, January.

Croxson, K, J Frost, L Gambacorta and T Valletti (2022): "Platform-based business models and financial inclusion", *BIS Working Papers*, no 986, January.

Demirgüç-Kunt, A, S Ansar, J Hess, L Klapper and D Singer (2018): *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, World Bank.

D'Silva, D, Z Filkova, F Packer and S Tiwari (2019): "The design of digital financial infrastructure: lessons from India", *BIS Papers*, no 106.

European Union (2018): General Data Protection Legislation.

Feyen, E, J Frost, L Gambacorta, H Natarajan, and M Saal (2021): "Fintech and the digital transformation of financial services: implications for market structure and public policy", *BIS Papers*, no 117, July.

Government of India, Ministry of Electronics and Information Technology (2020): *Report by the Committee of Experts on Non-Personal Data Governance Framework*.

iSPIRT Foundation (2021): *Data Empowerment: A Techno-Legal Approach*.

Jones C and C Tonetti (2020): "Nonrivalry and the economics of data", *American Economic Review*, vol 110, no 9, September.

Matthan, R (2022): "A world fragmented by divergences in data regulation", Mint, March.

McKinsey Digital (2021): "What's next for digital consumers", May.

Mehta, H (2021): "Confidential clean rooms in DEPA", iSPIRT Foundation, 14 October.

Morey, T, T Forbath and A Schoop (2015): "Customer data: designing for transparency and trust", *Harvard Business Review*, May.

NITI Aayog (2020): "Data empowerment and protection architecture", August.

OECD (2021): "Data portability, interoperability and digital platform competition", *OECD Competition Committee Discussion Paper*.

——— (2013): "Guidelines governing the protection of privacy and transborder flows of personal data".

——— (2014): "Protecting privacy in a data-driven economy: taking stock of current thinking", Privacy Expert Roundtable, March.

OECD Library (2019): "Economic and social benefits of data access and sharing", Chapter 3 of *Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies*.

Rao, R (2021): "Regulatory framework for account aggregators", remarks during a virtual event organised by iSpirt Foundation, September.

Reserve Bank of India (2016): "Master direction – non-banking financial company – Account Aggregator directions", (as on 5 October 2021).

Schwartz, P and D Solove (2009): "Notice and choice: implications for digital marketing to youth", memo for The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children, Berkeley, 29–30 June.

Solove, D (2013): "Privacy self-management and the consent dilemma", *Harvard Law Review*, no 1880.

The Treasury, Australia (2019): *Consumer Data Right Overview*.

United States Department of Health, Education and Welfare (1973): "Records, computers and the rights of citizens", May.

van der Vlist, F and A Helmond (2021): "How partners mediate platform power: mapping business and data partnerships in the social media ecosystem", *Big Data & Society*, vol 8, no 1, pp 1–16.

van Ooijen, I and H Vrabec (2019): "Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective", *Journal of Consumer Policy*, vol 42, pp 91–107.

Waibel, P, J Matt, C Hochreiner, O Skarlat, R Hans and S Schulte (2017): "Cost-optimized redundant data storage in the cloud", *Service Oriented Computing and Applications*, vol 11, pp 411–26.

World Economic Forum (2021): "From competition to collaboration: How secure data sharing can enable innovation", June.

Previous volumes in this series

No	Title	Issue date
BIS Papers No 123	CBDCs in emerging market economies	April 2022
BIS Papers No 122	The monetary-fiscal policy nexus in the wake of the pandemic	March 2022
BIS Papers No 121	Covid-19 and the monetary-fiscal policy nexus in Africa	February 2022
BIS Papers No 120	Virtual banking and beyond	January 2022
BIS Papers No 119	Non-bank financial institutions and the functioning of government bond markets	November 2021
BIS Papers No 118	A taxonomy of sustainable finance taxonomies	October 2021
BIS Papers No 117	Fintech and the digital transformation of financial services: implications for market structure and public policy	July 2021
BIS Papers No 116	CBDCs beyond borders: results from a survey of central banks	June 2021
BIS Papers No 115	Multi-CBDC arrangements and the future of cross-border payments	March 2021
BIS Papers No 114	Ready, steady, go? – Results of the third BIS survey on central bank digital currency	January 2021
BIS Papers No 113	Financial market development, monetary policy and financial stability in emerging market economies	December 2020
BIS Papers No 112	The dawn of fintech in Latin America: landscape, prospects and challenges	November 2020
BIS Papers No 111	Inflation dynamics in Asia and the Pacific	March 2020
BIS Papers No 110	Measuring the effectiveness of macroprudential policies using supervisory bank-level data	February 2020
BIS Papers No 109	The digital economy and financial innovation	February 2020
BIS Papers No 108	Stress testing in Latin America: A comparison of approaches and methodologies	February 2020
BIS Papers No 107	Impending arrival – a sequel to the survey on central bank digital currency	January 2020
BIS Papers No 106	The design of digital financial infrastructure: lessons from India	December 2019

All volumes are available on the BIS website (www.bis.org).