Data Governance Network
Anchored by IDFC Institute

December 2021

Working Paper 21

Tech Tools to Facilitate and Manage Consent: Panacea or Predicament? A Feminist Perspective

Tripti Jain

internet democracy project

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organisation.

Design

Cactus Communications

Suggested Citation:

Jain, T. (2021).Tech Tools to Facilitate and Manage Consent: Panacea or Predicament? A Feminist Perspective. Data Governance Network Working Paper 21

Supported by a grant from Omidyar Network

Abstract

In this exploratory study, I assess account aggregators (AA) in India, and the emerging ecosystem in which they are embedded, against the feminist principles of consent in the age of embodied data. While consent continues to be a cornerstone of ensuring autonomy across data protection regimes, research has nevertheless been critical of it. In an earlier study, Anja Kovacs and I (Kovacs & Jain, 2020) identified the current perception of data, i.e. as a resource, as one of the crucial problems plaguing existing consent regimes; instead, we demonstrated, data is increasingly functioning as an extension of, or even integral to our bodies. We then built on this reconceptualisation to draw parallels between feminist learnings around sexual consent and data protection, to delineate six feminist principles that need to be observed in data protection regimes for consent to be meaningful there (Kovacs & Jain, 2020). Meanwhile, technology-enabled consent frameworks, such as the account aggregator framework conceptualised and launched in India, aim to similarly address key criticisms of consent regimes today, to thus strengthen user consent and the autonomy of individuals. I examine in this research study how well the developing AA ecosystem in India is delivering on these claims in practice. Assessing it against each of the feminist principles of consent, I ask to what extent AAs align with the feminist principes, whether AAs are effective, and what the way forward is. As we will see, while AAs do mark a notable improvement over existing consent regimes in a number of ways, many weaknesses remain. All too often, this is because AAs are positioned as a silver bullet: changes in the broader landscape in which they are embedded, while crucial to their mission, remain absent. As long as this does not change, it will not be possible for AAs to do all the work that is currently expected from them.

Table of Contents

List of Abbreviations

AA	Account aggregator
API	Application programming interface
CBDT	Central Board of Direct Taxes
CCI	Competition Commission of India
DEPA	Data Empowerment and Protection Architecture
FIP	Financial information provider
FIU	Financial information user
GDPR	General Data Protection Regulation
GST	Goods and Services Tax
IRDA	Insurance Regulatory and Development Authority
iSPIRT	Indian Software Products Industry Round Table
MeitY	Ministry of Electronics and Information Technology
NABARD	National Bank for Agriculture and Rural Development
NBFC	Non-banking finance company
NDSAP	National Data Sharing and Accessibility Policy
PFRDA	Pension Fund Regulatory & Development Authority
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
TRAI	Telecom Regulatory Authority of India
UI	User interface
UPI	Unified Payments Interface
UX	User experience

1. Introduction

In this exploratory study, I assess account aggregators (AA) in India, and the emerging ecosystem in which they are embedded, against the feminist principles of consent in the age of embodied data. Account aggregators have been developed with the stated aim of improving consent management by users and thus enabling greater user autonomy while expanding participation in the digital world. Through this assessment, I aim to understand to what extent this developing ecosystem currently delivers on these claims in practice, where there might be room for improvement, and what such improvements would look like.

1.1. Context

Most data protection frameworks across the globe consider consent mechanisms as tools for privacy self-management (Solove, 2013) and enablers of individual autonomy. The European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act, the United Kingdom's Data Protection Regulation and India's Personal Data Protection Bill 2019 all recognise “consent” as an expression of agreement, or denial of agreement, on the part of the user to share their data and to allow for its accumulation and processing. It is “consent” that effectuates the formal social contract (Kaye et al., 2015) between data subjects and data fiduciaries.

Despite the centrality of consent, research in the past has, however, been critical of consent mechanisms. (Kovacs & Jain, 2020) Some scholars, such as Matthan (2017), have therefore suggested moving away from consent and exploring other realms of ensuring privacy, such as accountability, instead. However, in earlier research Anja Kovacs and I (Kovacs & Jain, 2020) have argued that consent mechanisms can be rescued. While consent regimes may fail to enable the autonomy of individual users for a range of reasons, what unites them, we demonstrated, is that they are based on the conceptualisation of data as a resource. This perception of data sometimes invisiblises and at other times allows us to overlook the harms that are caused to human bodies by decisions that are made on the basis of individual's data. For example, individuals have been denied access to rations, which they have a right to under Indian law, because of fingerprint authentication failures (Khera, 2019). Rather than simply a resource, data is, in other words, increasingly an extension, or even integral to our bodies, and recognising this allows us to also recognise more easily the range of harms incurred on bodies as a result of different data driven exercises. Having established the close connections between bodies and data, Kovacs and I turned to existing areas of research in which questions of consent and the body have figured strongly for guidance on how to strengthen consent regimes, and found that feminist debates on sexual consent have particularly rich discussions on consent and body. Based on a detailed examination of these debates, we, finally, formulated a list of six core principles that take the integrity of the self as their starting point and that need to be observed in data protection regimes for consent to be meaningful there as well (Kovacs & Jain, 2020).

We are not the only ones who continue to recognise the value of consent, however. Among particularly interesting other efforts are several concrete technology-enabled tools and frameworks that have been proposed to enable consent and are being launched in India and across the globe. In India, these tools and frameworks include the Electronic Consent Framework by the Ministry of Electronics and Information Technology (MeitY), the Data Empowerment and Protection Architecture (DEPA) by iSPIRT and NITI Aayog (a think tank of the Government of India), and the Account Aggregator Framework by the Reserve Bank of India (RBI). Among examples elsewhere are the Open Banking System in the United

Kingdom and the X-Road framework in Sweden. All these tools or frameworks claim to enable individuals to exercise greater control over their data by allowing them to manage their consent more efficiently. They aim to do so by addressing some of the common criticisms that the consent regime faces, including consent fatigue, the complexity of notice, and that consent is often sought up-front for subsequent transactions (Basu & Sonkar, 2020). All these, and others, are concerns that Kovacs and I addressed by means of the feminist principles of consent as well (Kovacs & Jain, 2020).

In order to understand how well such technology tools deliver on their promises, I aim to assess, in this exploratory study, the efficacy of one such proposed technology solution, the account aggregator, against the feminist principles of consent delineated by Kovacs and Jain (2020). In doing so, I aim to understand to *what extent* AAs align with the feminist principles; whether they are effective in strengthening user consent; and *what* can be done additionally to further strengthen the consent mechanism in the AA framework. The paper focuses on the account aggregator framework in particular, as the other Indian frameworks that have been proposed are either a component of the AA framework or are yet to manifest into working tools and technologies. On the other hand, the account aggregator framework, which was proposed in late 2015, has seen significant progress. In fact, Onemoney, one of the AAs, has already launched its beta application, thereby making this ecosystem a suitable fit for this exercise.[1]

1.2. Research Methodology

To answer the research question, a mixed-methods approach was adopted. First, I mapped all provisions in Indian statutes and directions that specifically concern consent management tools. Then I searched through the websites of the account aggregators, their beta applications, their privacy policies and terms of use, and other documents. I did so to understand the vision behind the introduction of the account aggregator framework, how it is being adopted, and its impact on individuals' privacy and autonomy. Due to the nascent nature of the technology, the literature available in the public domain was, however, limited, which served as a hurdle for this research.

I tried to fill any gaps through interviews with early adopters of the ecosystem, to the extent possible. However, it deserves to be pointed out that some concerns can only be clarified as the ecosystem evolves. I conducted semi-structured interviews with eleven key informants who have been involved in envisioning, designing, adopting and critiquing this ecosystem. I interviewed them for their expertise on the subject matter or due to their extensive contribution to building digital public goods. These interviews were conducted on telephone or online (mobility constraints imposed by the nation-wide COVID-19 lockdown made in-person interviews not possible). The interviews took place between November 2020 and January 2021 in English and Hindi. The following are the persons that I interviewed for this research: A Krishna Prasad (Founder of Onemoney, the first account aggregator to get an operating license and the first AA to launch its beta application), B.G Mahesh (Co-founder of Sahamati Foundation, a self-regulatory organisation for the AA framework), Kamya Chandra (building public digital platforms to drive India's economic growth at iSPIRT Foundation and co-author of the DEPA Book), Malavika Raghavan (Senior Fellow for India, Future of Privacy Forum), Munish Bhatia (Co-founder of Finvu, an AA), Praneeth Bodduluri (Co-founder, Base Account), Rahul Matthan (Partner at Trilegal), Saurabh Punjwani (Volunteer Technologist at iSPIRT Foundation and one of the security engineers involved in conceptualisation of the AA ecosystem), Srikanth L (Public Interest Technologist, with expertise in digital payments), and Vinay Sathyanarayana (Chief Engineer at Perfios Software Solutions Pvt. Ltd, an AA). Names have been used after seeking explicit written or verbal consent from the research participants.

[1] The ecosystem was officially launched in September 2021, while this paper was being prepared.

Finally, along with the semi-structured interviews, I also conducted a review of the literature regarding the regulatory frameworks governing the AA ecosystem, covering both academic papers and newspaper articles.

As noted, the AA framework is still being developed and iterated. Therefore, some concerns and nuances may remain unarticulated for the moment. However, I hope this research and the questions that I aim to answer herein may provide some useful insights to further strengthen consent management frameworks, at this early stage.

In what follows, I will first outline the landscape of technological tools that claim to operationalise consent in India. In that same section, I will also take a deeper dive into the account aggregator ecosystem and delineate its objectives, major stakeholders and how the consent mechanism in the ecosystem works. The heart of the paper is section three, in which I will outline, for each of the feminist principles, a number of key conditions that need to be fulfilled to enable meaningful consent in the AA ecosystem, then examine and assess the tool against each of these conditions, drawing on the interviews conducted and literature available. In section four, I will then summarise, based on the earlier analysis, to what extent the AA framework complies with the feminist principles. Finally, in section five, I will make some concrete recommendations to address the concerns identified in the paper and thus fully meet the minimum requirements necessary to ensure meaningful consent.

2.Understanding the Landscape, and Account Aggregators and their Functioning

Since 2015, a number of technological tools and frameworks that claim to operationalise consent have been proposed in India. Understanding this landscape, and the place of account aggregators within it is, essential before assessing the account aggregator ecosystem against the feminist principles of consent.

2.1. A brief overview of consent enabled technology tools in India

A number of technological tools and frameworks that claim to operationalise consent have been proposed in India thus far. Some of these tools and frameworks are built on each other's specifications or have borrowed underlying architecture from one another. However, each of these tools has been introduced in different years, by different entities and with some additional features. Thus, it is imperative to understand these tools separately.

A chronological analysis of these consent management tools and the overarching framework suggests that the idea was first mooted within the financial sector through the RBI Master Directions, 2016. Upon operationalising the Master Directions, the regulators seem to have realised the necessity of allowing secure sharing of user data in various sectors, therefore encouraging technical infrastructure that enables more broadly secure collection of user information based on consent provided by said user. The Electronic Consent Framework (MeitY, 2018) intends to achieve this goal. Following this, the Personal Data Protection Bill, 2019, in section 23, identified and gave legal footing to a new category of entities called “consent managers”. Finally, the draft DEPA Book (NITI Aayog, 2020) was brought out as an umbrella framework to advance consent management systems through technical and regulatory mechanisms. While these frameworks and tools may have emerged in separate years, a deeper dive into each reveals that these different modules were, in fact, in the works parallelly.

Account Aggregators (2016)

In 2015, at the 52nd meeting of the Central Board of the Reserve Bank of India, the Governor announced that the RBI will put in place a regulatory framework to allow a new kind of non-banking finance company (NBFC): account aggregators (Reserve Bank of India, 2015). The conception of account aggregators resulted from the recommendations of the Financial Stability and Development Council. The Council recommended a new kind of NBFC which would help people see their accounts across financial institutions in a common format. Following that, in 2016, the draft Directions regarding Registration and Operations of NBFC – Account Aggregators were issued under section 45-IA of the Reserve Bank of India Act, 1934.[2] These were finalised by 2 September 2016, as the RBI's final Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions (henceforth, "the Master Directions").[3] Along with these regulatory requirements, the RBI also issued, in 2019, the Technical Specifications for Application Programming Interfaces (APIs) to be used by all participants of the account aggregator ecosystem.[4]

In 2018, after the release of the Master Directions, the RBI invited applications from non-banking financial companies to be licensed as account aggregators (NBFC-AAs). Currently, there are six entities that have been given in-principle and operating account aggregator licenses from the RBI. The first license for an NBFC-AA was issued in 2018 (Lakshmanan, 2018). In 2019, Sahamati, a non-profit collective of AAs was formulated. It is similar to the Wifi Alliance, the GSM Alliance, the Bluetooth Alliance, and other such entities, in that it acts as a self-regulating organisation. Sahamati specifically aims to work towards growing the adoption of the AA framework in the financial world, which it claims will achieve the goal of "data empowerment" for data principals.

Account aggregators consolidate the financial data of an individual, previously spread across various financial sector institutions, and facilitate access to such financial data by acting as "consent brokers'': entities mediating consensual data transfer across financial entities, such as banks and mutual fund companies, termed financial information users (FIUs). It is claimed that account aggregators will make credit accessible to the people who are currently not part of the credit ecosystem, thus ensuring the formal financial system becomes more inclusive (Belgavi & Narang, 2019).

As per the existing RBI Master Directions, 2016, AAs are currently only allowed to serve as a data pipe for financial data. However, Telecom Regulatory Authority of India (TRAI) Chairman RS Sharma, in August 2020, argued that telecom service providers should be allowed to be financial information providers as well. This example indicates that there exists scope to extend the use cases and information providers within the AA ecosystem.

Electronic Consent Framework (2018)

The Electronic Consent Framework (MeitY, 2018) was proposed by the Ministry of Electronics and Information Technology to enable the effective and secure implementation of two government policies: the Policy on Open Application Programming Interfaces (APIs) for the Government of India,[5] and the National Data Sharing and Accessibility Policy (NDSAP), 2012.[6] Both policies focus on laying down guiding principles for data sharing. The Open APIs Policy was formulated to promote software

[2] Available at https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142.

[3] The directions, updated on 22 November 2019, are available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

[4] Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11729&Mode=0.

[5] Available at https://meity.gov.in/writereaddata/files/Open_APIs_19May2015.pdf.

[6] Available at https://smartnet.niua.org/content/2bac29b3-ffbd-45df-a219-91c07b343dbd.

interoperability for all e-governance applications and systems. It aims to enable any public service provider to access data and services so as to promote participation of all stakeholders, including citizens. The NDSAP delineates an overarching framework for sharing of data that is collected by State entities using public funds with service providers that work for public interest. Embodying the guiding principles prescribed by the Open API policy and the NDSAP, the Electronic Consent Framework was drafted. It is a framework that runs on an Open API and allows data subjects to entrust a platform with sharing their personal data with other data fiduciaries on a need basis, while providing technical safeguards for the use and management of consent in a paperless ecosystem.

Consent Manager (2019)

The Personal Data Protection Bill, 2019 borrowed underlying principles from the discussions around DEPA (see below) and the Electronic Consent Framework, and proposed, in section 23, another tool: the consent manager, a data fiduciary that enables a data principal to gain, withdraw, review and manage their consent through an accessible, transparent and interoperable platform. However, the current version of the Personal Data Protection Bill, 2019 is silent on the technical, operational, financial and other working conditions of the consent manager. It states that these specifications will be delineated in regulations. Thus, it is unclear for the moment how these consent managers will function, and whose interests they will serve and to what extent.

Data Empowerment and Protection Architecture (DEPA) (2020)

The Data Empowerment and Protection Architecture (DEPA) (NITI Aayog, 2020) is the consent layer of Indiastack,[7] developed by iSPIRT and NITI Aayog (a think tank of the Indian government). It is one of the frameworks proposed in the Indian context to empower individuals to control how their data is being used. In fact, the work on DEPA seems to have predated the idea of consent managers in the Personal Data Protection Bill. The ball started rolling as early as August 2017 (ProductNation/iSPIRT, 2017a) and has since been championed by iSPIRT.[8] DEPA is not just a technology tool but a sector-agnostic overarching framework that governs the consensual transfer of user data currently resting in silos. The proposers of the DEPA framework are of the view that digital footprints can serve as a means to build trust between the users and institutions (NITI Aayog, 2020, p. 25), and that empowering individuals with control over their data will enable their well-being and allow them more autonomy over their personhood. To ensure this, DEPA proposes to enable consensual sharing between service providers of personal data that currently resides in silos, so as to allow users to access better financial, healthcare and other socio-economically important services in a secure and privacy-preserving manner. The architecture is built with the expectation that, for example, a bank could design and offer regular big and small loans based on demonstrated ability to repay (known as flow-based lending) rather than only offering bank loans backed by assets or collateral. The decision to offer the loan would hinge on the integration of financial data such as GST (Goods and Services Tax) payments, payment of invoices, etc., which can help demonstrate the ability to repay.

Concretely, the DEPA framework proposes the development of new market entities or institutions, known as consent managers, to manage consent. Consent managers in the financial ecosystem are known as account aggregators, which we have already discussed above. Policymakers argue that this new class of institutions, i.e. consent managers, will be able to ensure individuals' data rights around

[7] "India Stack is a privately-owned bouquet of proprietary software or APIs powering Aadhaar-based applications, and UPI based digital transactions. It allows the government and businesses to use India's digital infrastructure to deliver private services." (Sircar, 2020).

[8] iSPIRT has also organised multiple industry engagement initiatives including policy hackathons since 2017 to present what has eventually become the Draft DEPA book.

privacy and portability because, unlike current data fiduciaries, who are interested in collecting behavioural surplus of users, these will be incentivised to protect user interest without engaging in exploitative practices. (NITI Aayog, 2020). They argue this on the basis that these new market entities have their economic incentives aligned with those of the users regarding the sharing of personal data, as they can charge a nominal fee to facilitate data exchange (NITI Aayog, 2020). Currently, the financial model proposed for account aggregators, for example, is based on charging the FIU or the end consumer, but not the FIP (financial information provider), for the data requested (Sahamati, 2019a).

The DEPA Book recognises the following three "digital public goods" as basic building blocks that will govern DEPA's technology architecture: 1. MeitY's Electronic Consent Framework - to build consent artefacts;[9] 2. Data sharing API standards - to enable an encrypted flow of data between data providers and information users; and 3. sector specific data information standards[10] (NITI Aayog, 2020 pp.38).

Implementation of the DEPA framework has already started in the financial sector, with the launch of the account aggregators (AAs), under the joint leadership of the Ministry of Finance, the Reserve Bank of India, the Pension Fund Regulatory & Development Authority (PFRDA), the Insurance Regulatory and Development Authority (IRDA), and the Securities and Exchange Board of India (SEBI). AAs are discussed at length in the next section of this paper.

The architecture was also expected to be piloted in the health sector in 2020; however it has not yet been launched at the time of writing. On 15 August 2020, Prime Minister Narendra Modi announced the National Digital Health Mission, which includes a Health ID and a data-sharing framework for personal health records. This is based on the National Digital Health Blueprint (Ministry of Health, 2019), published by the Ministry of Health, which in turn builds on the National Health Stack Strategy Paper, published by NITI Aayog in July 2018 (NITI Aayog, 2018).

Following the TRAI consultation report on privacy (TRAI, 2018), released in July 2018, and a workshop held by TRAI Chairperson RS Sharma in August 2020, it is expected that DEPA will also be launched in the Telecom sector (NITI Aayog, 2020 p. 48). RS Sharma highlighted that in India, telecom data often constitute the first digital footprint of a low-income household. Therefore, a steady history of on-time recharges could formulate a basis for credit history. Telecom service providers could, thus, serve as information providers as well.

2.2. Account Aggregators and Their Functioning

Before I begin to assess the consent mechanism in the AA framework from a feminist perspective, it is further imperative to learn what the AA ecosystem aims to achieve, who the key stakeholders are in the ecosystem and how they are expected to interact within it, as well as to better understand how consent functions in the ecosystem. In this subsection, I outline each of these aspects.

2.2.1. Objectives of Account Aggregator Framework

As noted earlier, policymakers and early adopters of the AA ecosystem observed that currently, financial data of individuals rests in silos, and even if an individual wishes to access their own financial data in consolidated form, there exists no platform that allows individuals to do so (Sahamati, 2019b). Similarly, if someone is required to transfer their data to other entities, there are no digital means available to do

[9] The consent artefact is a technology standard for programmable consent to replace the all-permissive terms and conditions forms (NITI Aayog, August 2020).

[10] Data Information Standards are the technology module that will be enforced sectorally to ensure uniformity in shared elements of data across the sector.

so. In times of increasing datafication of people's bodies and lives, spearheaded by private entities, this has resulted in reduced autonomy of an individual in decision-making. Thus, to enable easy viewing and sharing of financial data with consent, AAs were conceptualised.

Moreover, good connectivity to the formal financial system ensures access to a wide range of financial products. The AA framework assists in decision making required by financial institutions for the provision of financial services such as (lending, wealth management and personal finance management, by eliminating paper trails.[11] Thus, AAs can facilitate access to financial services and credit for earlier underserved and unserved segments, i.e. enable financial inclusion, by reducing information asymmetry.

In the first press release by the RBI that touched upon AAs (Reserve Bank of India, 2015), the policymakers envisioned AAs as NBFCs that would merely enable users to see their financial data spread across different financial institutions. However, in the final Master Directions from the RBI, a transformation was observed in the role of account aggregators. According to the 2016 Directions, AAs were conceptualised to help end-users keep oversight of their personal data by managing consent and subsequently the flow of information between the various financial institutions with which they engage in data-generating exchanges.

2.2.2. Key Stakeholders in the AA Ecosystem

There are 4 major actors in this ecosystem: FIPs, FIUs, end-users, and the AAs themselves.

FIPs (Financial Information Providers): As the name suggests, financial information providers are the data fiduciaries that will be providing information to other financial entities, enabling them, in turn, to provide financial instruments to the customer. FIPs could be entities like banks, banking companies, non-banking financial companies, asset management companies, depositories, depository participants, insurance companies, insurance repositories, pension funds and such other entities as may be identified from time to time by the RBI for the purposes mentioned in the RBI directions 2016. So far a total of eleven institutions have publicly expressed their participation in the ecosystem as FIPs. They are Axis Bank, Bajaj Finserv, DMI Finance, Federal Bank, HDFC Bank, Hero FinCorp, ICICI Bank, IDFC FIRST Bank, Indusind Bank, LendingKart, and State Bank of India (SBI).

FIUs (Financial Information Users): Financial information users are data fiduciaries that seek information from FIPs to provide financial services. FIUs are entities registered with and regulated by any financial sector. They could very well be FIPs themselves, such as banks, asset management companies, and insurance companies. For example, a bank might require certain financial data prior to issuing a credit card to an individual; as it accesses data through the pipeline mediated by AAs, it will then be acting as an FIU .

Account Aggregators (AAs): AAs are non-banking financial companies, defined and regulated by the central bank, i.e. the RBI. No other entity apart from an NBFC can seek a license to be an AA. AAs are consent managers in the financial sector. The RBI has confirmed in-principle approval of six account aggregators for building a data-sharing solution: CAMS FinServ, Cookiejar Technologies (product named Finvu), FinSec AA Solutions Private (product named OneMoney), National E-Governance Services Limited (NESL Asset Data Limited), Yodlee Finsoft, and Perfios Account Aggregation Services (Sahamati, 2020a).

[11] Available at, https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1124

End-users or Customers: The end-users enter into a contractual arrangement with the account aggregator to avail of their services.

2.2.3. Obtaining Consent in AA Framework

On the basis of the information available about AAs (Reserve Bank of India, 2016b; Sahamati 2019a), I have been able to piece together how AAs function, and how they enable FIPs and FIUs to join hands. AAs are data blind pipelines at the best of the end user. This means that data will be encrypted and access will be only available to those who have private keys to the encrypted data. Let us trace the user journey here to understand in more detail how the consent mechanism works.

A user may access the AA's services through an app made available by the AA on smartphone app stores or through the AA's website. Users may sign up on the AA app with the usual credentials. Currently, only full names and mobile phone numbers are being used as identifiers. We are yet to see whether and which other identifiers will be required as the system evolves, such as PAN or Aadhaar Number. This is critical as this might contribute to function creep and other harms to user privacy.

Once signed up, the user should link all their financial accounts and instruments which they wish to manage through the AA, such as bank accounts, demat accounts, fixed deposits, etc. In order to link their financial accounts and instruments with the AA, users are required to furnish the mobile number through which they have already registered with the FIPs. The AA then looks up the registered mobile number across various FIPs and provides the user with a list of accounts and instruments that are linked to their registered number, and allows the user to choose the account(s) or instrument(s) they wish to link. Once the bank accounts and instruments are linked, users can start managing their consent concerning their data for the linked accounts and instruments.

At the moment, the AA ecosystem envisions four types of consent:

a. View: allows FIU to only view the data;
b. Store: allows FIU to store the static data unless the consent expires;
c. Query: allows FIU merely to authenticate the veracity of the data that user has provided;
d. Stream: gives FIU access to the flow of data, such as ongoing transactions, etc., unless the consent expires.

Along with different types of consent, the ecosystem also envisages two types of fetch:

a. One time: wherein FIUs seek all the desired information in one go;
b. Periodic: which enables FIUs to seek information in a periodic manner, such as on a daily, weekly or monthly basis.

From their side, FIUs can raise a consent request through the AA to seek information from the user. As per the RBI Master Directions 2016, this consent request is required to have the following details:

- the identity of the customer and optional contact information;
- the nature of the financial information requested;
- the purpose of collecting such information;
- the identity of the recipients of the information, if any;
- the URL (in case of website access) or other address to which notification needs to be sent every time the consent artefact is used to access information;
- the consent creation date, expiry date, identity and signature/ digital signature of the account aggregator; and
- any other attribute as may be prescribed by the RBI.

[12] Fetch is the pre-programmed command whereby data is brought from the database for the purpose of fulfilling the request of the FIU.

Users can give or deny consent to the FIU for the request raised. Once the request is accepted by the user, the AA conveys such consent to the concerned FIP(s). The FIP(s) would then create a private key to encrypt the data requested and send it across to the FIU through the AA. In order to decrypt this information, the FIU creates a public key which goes all the way to the FIP, which then, after receiving consent, encrypts the desired information and sends it across to the FIU.

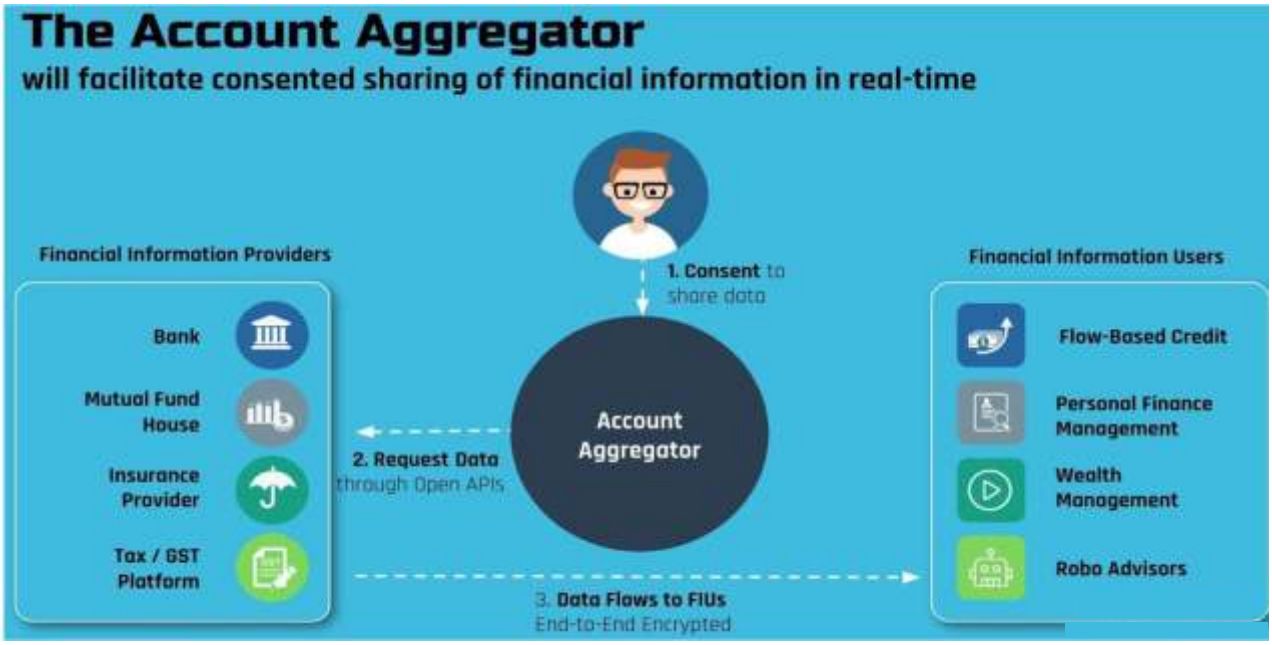

Figure 1. Consent Flow in the AA Framework (Sahamati, 2019a).

3. Examining the AA Ecosystem against the Feminist Principles of Consent in the Age of Embodied Data

In the previous sections of this paper, we learnt about the reasons for the introduction of the AA ecosystem and the need to assess the AA ecosystem. In this section, the efficacy of this framework will be examined against the feminist principles of consent in the age of embodied data proposed by Kovacs and myself (Kovacs & Jain, 2020). To do so, first, let's recall the feminist principles:

- Consent must be embedded in a notion of relational, rather than individual, autonomy.
- Consent must be given proactively, communicated in the affirmative.
- Consent must be specific, continuous and ongoing, to be sought for different acts and at different stages. Consent is required to be built.
- Consent is a process, and thus opens up a conversation, rather than entailing merely a yes/no decision.
- Consent allows for negotiation by all parties involved.
- Conditions must be created so that consent can be given freely. This implies that the person should be free from any fear of oppression or violence of any kind.

To examine the ecosystem against the deduced consent principles, it is imperative to understand the conditions necessary to enable a consent principle. It is impossible to present in detail all the conditions to enable a principle, their nuances and what all could they entail - nor do I want to claim that I possess

full knowledge of all changes that are needed at this time. The framework is still being developed, implemented and iterated, and in the middle of this process, I can only propose qualifiers and conditions based on what is known about the ecosystem now. Nevertheless, on the basis of existing literature, I have identified a number of such key conditions for each principle, and will assess the AAs and their functioning against this.

To conduct this exercise, I follow the same procedure for each principle. I first lay down the principle and illustrate its importance. Then I highlight its relevance in the AA ecosystem. After doing so, I identify the conditions to enable a principle, based on what is known about the ecosystem so far, and examine the ecosystem against these. A summary of all principles and their conditions can be found in Annexe I.

3.1. Consent must be embedded in a notion of relational, rather than individual, autonomy

THE PRINCIPLE: Feminists such as Lacey (1998), and Nedelskey (1989) have noted that the assumption that every individual is free and autonomous in every context is false. Individual autonomy cannot be presupposed. Instead, autonomy is always relational: it is conditional on multiple factors concerning the individual (Nedelsky 1989, p. 12). Thus, a person can express autonomous consent only if the conditions allow them to do so, because irrespective of how robust their personal intentions are, external conditions can nevertheless prevent them from expressing autonomy.

RELEVANCE: For the data governance regime, too, this means that when consent is sought, the nature and quality of this consent is determined by the conditions under which this consent is obtained. This understanding is a departure from the existing paradigm, in which consent is so individualised that it ignores the conditions and mechanisms that have been deployed to seek consent online (Cohen, 2019).

In fact, scholars such as Austin (2014) and Cohen (2019) have highlighted that the reason for the current failure of notice and consent mechanisms in data governance is precisely that they overlook the full complexity of social conditions. For example, current notice and consent mechanisms are based on the assumption that an individual has an ability to exercise autonomy by expressing consent on the basis of the notice furnished. However, the following conditions are often not accounted for: the ability of an individual to assess a notice, the contradictory interests of the parties involved (i.e. data fiduciaries and data subjects) while collecting data, legalese used in notices, etc. As a result, the individual from whom consent is sought is often unaware of many of the risks and harms, thereby making consent meaningless. Thus, there's a need to move away from a "subject-centered to a condition centric approach" (Cohen, 2019 p. 17).

As discussed above, account aggregators are tools that aim to empower the people in India with the ability to manage their financial data in a convenient, secure and transparent manner. In order to do so, it provides for a consent artefact that empowers individuals to regulate access to and manage their financial data according to their will. As observed above, to ensure autonomy and enable individuals to exercise their will in practice, it is pertinent to ensure that a condition centric approach is deployed. Thus, AAs must approach consent in a relational manner and not just in an individual manner.

ASSESSMENT: What does this mean in practice? Let us consider four key conditions that need to be in place to strengthen user's relational autonomy, and examine whether they are being observed by the current framework.

The ecosystem should provide means that prevent data fiduciaries from misappropriating and misusing user data.

Currently, the ecosystem only prevents AAs from misappropriating and misusing user data. The Master Directions, 2016 state that the AAs are data blind. This means that the data that flows through AAs is encrypted and AAs cannot access or use it. In addition, the Master Directions lay down restrictions to prevent misuse of data by AAs. Among other duties, this includes a prohibition on retention and disclosure of user information by the AAs in the absence of explicit user consent.

However, the threat of misuse of personal data continues to persist in the ecosystem because FIPs and FIUs are only lightly regulated as far as privacy of user data is concerned. Direction 7.6.2 of the Master Directions provides that the information received by an FIU through an AA cannot be used for any other purpose except as is specified in the consent artefact. However, there is no technology layer or regulatory method to assess how FIUs are using the personal and financial information that they receive. Apart from this one measure, the Master Directions, 2016 put the onus on sectoral regulators - such as those from IRDA and SEBI - to regulate either end of the data blind pipes (i.e. FIPs and FIUs) with respect to data, audits and accountability, among other things. Laws that currently govern data practices in the banking sector include section 43A of the Information Technology Act, 2000; the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; section 3 of Public Financial Institution Act, 1983; and section 29 of the Credit Information Companies Act, 2005. However, these laws are dated and cannot address the problems posed by existing data practices and technology, such as overcollection of personal data, creation of profiles and serving of targeted advertisements. A public interest litigation was filed at the Delhi High Court seeking a ban on the sharing of PAN and financial transaction data of clients with credit rating agencies without clients' formal consent (PTI, 2019). This further highlights that FIPs such as CIBIL, Equifax and other credit rating agencies, in particular, are under-regulated as far as privacy and data regulation is concerned.

Thus, the humbleness of the purpose limitation provision in Master Directions, 2016 and non-availability of a robust Personal Data Protection Act or other purpose limitation or collection limitation directions prevent desired checks on the FIUs. As a result, in practice, FIUs can access, process and share unlimited personal and financial data of consumers, to profile individuals, target advertisements and sell individuals' data, among other things. Moreover, the individuals concerned would not know whom to hold accountable, as once consent has been obtained by the FIU, there is no means to find out what data profiling techniques are being used by this FIU and what they are being used for.

In summary, at present, there is no technology layer and the available regulatory layer is insufficient to prevent individuals from being profiled, targeted or surveilled by FIUs or FIPs on the basis of data shared through AAs. Having robust AAs alone, while a step forward, is not sufficient to enable users' autonomy. Autonomy is relational and therefore, policymakers will need to go a notch further and build tools and/or regulations which protect users from the actions of FIUs may take with user data.

The ecosystem should enable users to choose and switch AA at any time, without being bound by a penalty or lock-in periods. This implies that there should be a sufficient number of AAs competing with each other in the market. In addition, there should be many FIUs, so that users have the ability to choose from a variety.

In my interviews with Saurabh Punjwani, Rahul Mathhan and Kamya Chandra, among others, they indicated that the framework aims to equip users with the ability to choose and switch AAs so that there is no oligarchy.

In the actual market, there are four AAs, at the moment: although six account aggregators have received a license of approval from the RBIa, only four have received an operating license so far (Sahamati, 2020a). Because the FIPs and FIUs are common across the entire ecosystem, these first few operational AAs may have first movers' advantage.

The developers of the ecosystem are optimistic. Vinay (Chief Technologist at Perfios) stated that the first mover may have an advantage, but user experience, transparency, lower failure rates and customer support are differentiating factors between competing AAs, which should enable competition. Vinay drew parallels between the AA ecosystem and the unified payments interface (UPI) ecosystem and was of the view that, just like the UPI ecosystem enables a future of multiple specialised payments apps (for women-first payments, children-first payments, a hyper-secure variant for the armed forces, etc.), so does the AA ecosystem. However, I see a different trend. Despite raising millions, most small wallets and companies were squeezed out by big tech companies due to a range of reasons, including that big companies have an existing user base, large amounts of funds available, etc. (Christopher, 2020). Today, 45 and 34.3 percent of the market are held by Google Pay and Phone Pe respectively (Upadhyay, 2021).[13]

This illustrates that the developers of the AA ecosystem should be very cautious so as to prevent it meeting the same fate as the UPI ecosystem. If the AA ecosystem fails to enable competition, there would only be one or two dominant players, which means no real choice for the customers, leading to a power imbalance.

Thus, having an ecosystem that enables competition is not sufficient, enforcing competitive practices is equally important. Therefore, the regulators – both the RBI and the Competition Commission of India (CCI) – have an important responsibility. They must identify and eliminate anti-competitive behaviour, such as monopoly pricing, cartelisation by players, customer-locking, and any other market abuse (Uppal, 2020).

Another challenge that will need to be addressed is that many entrepreneurs and institutions are skeptical towards the AA ecosystem and so far hesitate to participate. This is for two main reasons in particular.

1. *Lack of clarity with respect to the revenue models of the AAs*

Neither the Master Directions, 2016, nor the AA's self regulatory organisation, Sahamati Foundation, have delineated any clear revenue scheme for account aggregators. In the definition clause of the Master Directions, it is briefly mentioned that account aggregators undertake the business of AA for a fee or otherwise. The fee will be decided by an Account Aggregators' Board approved policy. Pricing of services will be in strict conformity with the internal guidelines adopted by the Account Aggregator which need to be transparent and available in public domain. However, the Directions do not provide any clarity regarding the assessment and calculation of this fee. This is worrisome, particularly from the consent perspective, because a clear revenue model is necessary to attract new investors in this ecosystem . Malavika Raghavan, researcher and a keen observer of the sector, highlighted:

> There exist fundamental economic and operational problems in this ecosystem. The RBI Master Directions clearly state that AAs cannot use data flowing through their systems, but they fail to clarify how an AA can make customer propositions. Policymakers have left a lot of basic questions unanswered.

Until these ambiguities are addressed, the proposed framework, allowing for participation of many AAs, might not become operational in practice. As a result, users' choices regarding AAs would also be limited.

[13] https://entrackr.com/2021/05/phonepes-upi-market-share-rises-to-45-in-april-google-pay-slips-a-tad/

2. Low level of participation of FIPs and FIUs

Without a sufficient number of FIPs and FIUs in the ecosystem, it will not be possible for AAs to acquire customers. Therefore, it has been a constant endeavour of the developers of the ecosystem to get as many financial service providers as possible onboarded in the ecosystem.[14] After two years, eight banks have been onboarded both as FIPs and FIUs (Sahamati, 2020b).

Along with the developers, Sahamati has been at the forefront of these efforts. In an interview, Kamya Chandra pointed out that the RBI is mostly concerned with preventing and addressing financial crises; their focus is not on financial inclusion. Therefore, there is a need for someone else to take up the responsibility of implementing the AA framework, and according to Chandra, "Sahamati's focus for the last six months, and for the next six months, will just be to make sure that the FIP and FIU modules are live across major banks, allowing for the sharing of a core set of data that's required for cash flow lending."

Directions 3(1)(xi) and 3(1)(xiii) from the Master Directions, 2016, seem to further support this quest, as they allow for a wide range of institutions to be FIPs and FIUs. But despite these favourable regulatory conditions, banks have not been very enthusiastic.[15] Munish, Co-Founder of Finvu, stated that "to have institutions onboard has been a slow process and has not been the easiest thing. It required a lot of convincing; institutions have been hesitant".

Vinay, at Perfios, specified three reasons in particular why banks have been slow in adopting the AA framework. First, the impact of Covid-19 prevented the banking industry from being enthused about lending until August/September 2020. In addition, setting up their IT systems in a state of lockdown was not feasible. Second, banks are strictly regulated by the RBI, so in case of any change, they need to notify the RBI and seek permissions. Considering that this ecosystem has the RBI's blessing, doing so has been easier, but the process still remains slow and time-consuming. And third, it takes a lot of time for a traditional bank to finetune their IT ecosystems to participate in the AA framework, as the current IT systems would require a complete overhaul.

Apart from banks, there are other FIPs and FIUs, such as the Central Board of Direct Taxes (CBDT), under the Ministry of Finance, and telecom companies. It will be an even more complex task to integrate these into the ecosystem, as each of these information providers have unique data structures and the regulations that govern these entities are also varied. For example, the CBDT can share information about individual assessees with Scheduled Banks (Income tax Department, 2020). However, other FIPs and FIUs, such as telecom companies and the Department of Revenue, are not allowed to do so. In addition, rules and notifications under the Income Tax Act, 1961 are at odds with the expansive range of information made available to FIPs and FIUs by the RBI. Similarly, the law does not allow for the sharing of telecom data yet (TRAI, 2017). Thus, due to the legal vacuum with respect to data sharing policies, it will be a long term process to onboard all FIPs and FIUs to fulfil all desired use-cases. This will have a direct impact on entities that wish to seek an AA license: seeing the circumstances, a potential new entrant might be rather hesitant to enter the space.

The ecosystem may have been envisioned with the intention that there would be multiple service providers, i.e. AAs, and that users would have the ability to choose and switch their accounts. But if

[14] Munish, Co-founder at Finvu noted that so far, getting the banks onboard has been their primary focus.

[15] Despite reaching out to a few banks and their staff, no positive response for the interviews was received.

choice does not exist in practice, users' bargaining power could be diminished. To encourage more participation there is a need for a strong business model for the AAs and a regulatory policy that would enable competition as well as incentives for FIUs and FIPs to integrate themselves in the ecosystem. Otherwise, the vision of enabling users with ample choice might not come true.

Privacy respecting ecosystems are easier to promote and operationalise as users are less hesitant to give consent when they believe their data will be kept private. Thus, the ecosystem should provide regulatory and technical tools or frameworks to ensure privacy.

Let us first examine *whether the AA framework's technical specifications are resilient.*

While the RBI's Master Directions, 2016 provide a framework for the registration and operation of account aggregators in India, its Technical Specifications for Application Programming Interfaces (APIs) provide technical guidance for the development of the AA ecosystem. The Directions and Specifications both require AAs to be data blind. This implies that AAs do not have access to the information that is being transmitted through them. In addition, AAs cannot perform any other business apart from serving as data intermediaries.

AAs being data blind is a positive element. However, this requirement alone is not sufficient to address all privacy concerns arising within the ecosystem. In particular, the current system provides no technology tools or framework for four key privacy issues.

First, while facilitating data transfer by users and FIUs and FIPs, AAs will be collecting metadata such as users' basic profile information, including name and registered mobile number; which FIPs they are interacting with; and how often they interact with them. There is no technical or regulatory specification to regulate storage or use of this data as per the current Master Directions. This is problematic for two reasons: Firstly, this data would enable AAs to learn which user interacts with which FIUs and FIPs and which FIUs have higher traffic. As the business model of AAs is to charge consumers and FIUs for the exchange of data, they can potentially identify the nature of transactions done by users and FIUs and on the basis of this accumulated metadata, increase the cost for certain transactions for certain users or for FIUs. Secondly, since there is no mandate to encrypt or delete the metadata, the metadata continues to be vulnerable from the moment it is recorded, and if leaked, FIUs can take unfair advantage of this data to manipulate users by increasing costs, targeting ads, etc.

Second, as per the RBI's Master Directions, 2016, AAs are required to store data for a maximum of 72 hours. However, there is no technological means to enforce the transience of the storage. If stored for longer, the risk of leakage increases (NeSL, 2018; Jagirdar & Bodduluri, 2020).

Third, there are no technological means to assess whether purpose limitation and collection limitation are being observed by FIPs and FIUs, or to enforce these limitations. In the absence of a Personal Data Protection Act and a technology layer that enforces collection and purpose limitation, despite Direction 7.6.2, FIUs could request for unnecessary information and could use this data for purposes for which consent was not obtained, rendering the consent mechanism meaningless.

Fourth, there is no specification that allows for the identification of frauds in this ecosystem. A motivated user can easily create a trail of data to prove the existence of fifty transactions to different accounts in order to get a loan, while in reality, all those fifty transactions would have been made to fifty different UPI IDs created by the user herself. Considering the entire ecosystem has minimal human involvement, it would be very difficult to identify the frauds.

The current technology specifications are, thus, not sufficient to address various existing privacy concerns. However, sometimes what the technology layer fails to address can be resolved by the regulatory layer. For example, GDPR provides for a Data Protection Officer to ensure that privacy by design is being observed by data controllers while creating technologies to collect and process data. Thus, it is also imperative *to assess whether the AA ecosystem is governed by a robust regulatory framework.*

Currently, there is ambiguity regarding the recognition of AAs as NBFCs. Thus, the RBI's claim to regulate AAs is also questionable. As per section 45 IA of the RBI Act, the RBI is empowered to register, lay down policy, issue directions, inspect, regulate, supervise and exercise surveillance over NBFCs that meet the 50-50 criteria of principal business.[16] However, since more than fifty percent of the income of the AAs does not come from financial assets, because they do not technically provide financial activities (Raghavan & Singh, 2020), it has been argued that AAs cannot be termed NBFCs. Moreover, the RBI has failed to clarify the motive and the reasoning behind the categorisation of AAs as NBFCs in formal public documentation (Raghavan & Singh, 2020).

Even if we were to consider AAs as NBFCs, the question of whether the RBI is empowered and has the technical capability to regulate the information flows that are going through the data pipes of the AAs' networks remains. Raghavan and Singh (2020) highlight that the RBI's assertion of its intention to regulate all information flows in the financial sector, irrespective of their connection to financial activity, is complex and problematic, as it is beyond the competence and mandate of the RBI to regulate an activity which may not be purely financial, such as the consolidated viewing of data and consents.

However, neither regulators nor individuals have challenged the RBI's ability to regulate AAs. As a result, the account aggregators are subject to the RBI's Master Directions and the RBI's Technical Specifications for API's, in addition to the Information Technology Act, 2000. However, the Master Directions are not comprehensive and fail to rectify the privacy concerns that have been left unaddressed by the technical infrastructure of the AA ecosystem that I outlined above. The Master Directions do not apprehend apparent privacy risks, such as profiling and surveillance, within the AA ecosystem. The Directions only provide that AAs should be data blind; data collection by FIUs and usage and misuse of data by both FIPs and FIUs are not addressed. Moreover, the Master Directions are silent on excessive data collection through a consent artefact.

As the Master Directions, 2016, are insufficient to regulate data flows, there is a need for a robust and omnibus Personal Data Protection Act that delineates the overarching rights of users and obligations of data fiduciaries and contains provisions for transparency and accountability. However, the AA ecosystem has gone live prior to the promulgation of such a comprehensive data protection regime, which is worrisome. In the absence of a strong data protection law, there is no regulatory framework for the data collection and processing carried out by FIPs and FIUs; there are no means to assess the implementation of the rights and obligations of data subjects and data fiduciaries respectively; and in case of a breach, there is no recourse available for the customers of AA services, among other issues.

Even if the Personal Data Protection Bill had already been promulgated and notified in the Gazette of India, in its current form it would not have been effective, however, in addressing the privacy and consent concerns raised above. The current Bill fails to provide sufficient recourse to the data subject from misuse of data by data fiduciaries. Except when processing personal and sensitive data of children, the Bill does not obligate data fiduciaries to always act in the best interest of data principals.[17] Instead,

[16] Financial activity as principal business is when a company's financial assets constitute more than 50 per cent of the total assets and income from financial assets constitute more than 50 per cent of the gross income.

the Bill places high expectations upon data principals by requiring them to look out for their own interests. At the same time, some provisions enable excessive power concentration in the hands of data fiduciaries. This will benefit AAs, FIPs and FIUs, and not the users whose autonomy the Bill and this ecosystem supposedly aim to enable.

Praneeth, a technologist and fintech enthusiast, when discussing the regulatory framework governing the AA ecosystem, highlighted section 14 of the Personal Data Protection Bill, 2019 as one such example that furthers the concentration of power of data fiduciaries and prevents users from exercising autonomy. Section 14 lays down that certain additional grounds can be specified by regulations for processing of personal data without consent for "other reasonable purposes".

Section 14(1) empowers the Data Protection Authority to specify such other reasonable purposes after considering factors such as the interest of the data fiduciary, the effect of such processing on the data fiduciary, the public interest, and a reasonable expectation of consent. It is disconcerting that the interests of the data fiduciary are emphasised in this section.

In addition, section 14 grants the Authority the power to determine whether the provision of notice under section 7 will be applicable or not, depending on the nature of the reasonable purpose. Given that the grounds for defining reasonable purposes prioritise the interests of the data fiduciary, and not the interests of the data principal, it is particularly problematic to further redact the obligations under section 7.

Section 14(2) of the draft Bill provides a list of exemptions or instances in which personal data can be processed without seeking consent for reasonable purposes, which may include mergers and acquisitions, credit rating, recovery of loans and the detection of fraud. Praneeth considered many of these exemptions problematic because they empower data fiduciaries excessively. For example, if "credit scoring" is accepted as a reasonable purpose, this activity will be plagued by opacity. While traditional credit scoring comes with its own biases, the age of datafication, big data analytics and AI tends to magnify these biases, further impacting the communities concerned (Waddle, 2016; Eveleth, 2019). Moreover, it must be noted that companies have started to garner data across platforms, including from social media, to decide an individual's credit worthiness, going far beyond traditional metrics (Yanhao *et al., 2015*). While credit scoring may help to ensure access to credit for some, seeing the intrusive data gathering it often entails, such scoring should at a minimum be done with the consent of the individual concerned. However, the Bill would allow FIUs to ask for any kind of data under the garb of assessing creditworthiness, and users would not even have an option to deny consent because consent is not a pre-condition as per this section.

Thus, if the Personal Data Protection Bill, 2019 version is promulgated and would be applied to the AA ecosystem, it would not prove to be an effective regulatory framework for the users of AA services to exercise their autonomy and consent. This implies that to make the AA ecosystem resilient with respect to the privacy of its users' data, the ecosystem should be strengthened with tools and regulations that are robust enough to protect users' data and choice. Instead of instilling trust and confidence in the users, the current state of regulations overseeing the framework are worrisome and thus, should be reconsidered to enable the intent of the AA framework, i.e. autonomy of the users, while ensuring privacy.

Transparency measures need to be proposed by the regulators, so that users can become aware of the conditions and mechanisms deployed by data fiduciaries and thus, express their consent freely

[17] Chapter IV Section 16 (1), Personal Data Protection Bill, 2019.

The RBI's Master Directions, 2016, do prescribe some transparency measures that will allow users to trust the tools and express their consent more freely. In particular, they mandate that the names of the agencies that have been given licenses to be AAs, FIPs, and FIUs be made public and that, incase of revocation of the license of any agency, the announcement, too, will be made public.

However, these measures address only a very limited set of concerns. For example, they do not obligate data fiduciaries to inform users about data breaches or leaks. In contrast, the EU GDPR and even the Personal Data Protection Bill, 2019, provide for a number of transparency measures. For example, sections 23, 25, 26, and 28 of the Personal Data Protection Bill provide for transparency measures which include transparency in the processing of personal data; reporting of personal data breaches; classification of data fiduciaries as significant data fiduciaries, obligated to provide a higher level of care; data protection impact assessments; and maintenance of records by data fiduciaries. Unless all these measures are rolled out and the regulators are enforcing these mechanisms, it will be difficult for users to consent meaningfully because they will continue to be unaware of breaches, of the impact of technology used to process their data, etc. Thus, to enable autonomy, it is imperative to ensure all the conditions including transparency should be met.

3.2. Consent should be sought proactively

THE PRINCIPLE: The communicative approach to consent was developed in the early 90s by scholars like Pineau (1989), who argued that the person who is seeking consent for a sexual act, whatever their gender may be, must obtain consent in the affirmative from their sexual partner. Thus, this approach seeks to shift the burden of proving assent upon the person who is initiating the act. It simultaneously ensures that the partner - often a vulnerable person, such as a woman, trans person, or queer person - will no longer be required to prove that they expressed dissent.

This approach came into existence because earlier, the law generally required women to prove non-consent beyond a doubt. As this often is challenging, it was therefore presumed that the majority of sexual interactions are consensual. The communicative approach to consent was an attempt to address this shortcoming.

RELEVANCE: In the current data governance regime, consent is considered a means to enable privacy self-management. Thus, the burden to assess notices and express consent lies upon users or data subjects. However, once consent is obtained by the data fiduciaries, there is no means to audit that consent or find out how meaningfully it was obtained (Solove, 2013). In other words, in the current data protection regime, data fiduciaries seek consent at the very initial stage for all future acts through vague and ambiguous policies (Strahilevitz, 2013), and through opt-out methods (wherein parameters of consent are pre-chosen) that prevent individuals from expressing meaningful choice. Thus, consent obtained as per the current regime cannot be considered proactive, as the burden to prove dissent continues to lie on users.

If the AA ecosystem is to address these deficiencies of current consent regimes, AAs, FIUs and FIPs should bear the burden of proving beyond a doubt that they have pro-actively sought explicit consent for a specific purpose at every instance. In no circumstance should consent be presumed or assumed.

ASSESSMENT: In what follows, we will explore *three conditions* that need to be fulfilled by the data fiduciaries in the AA ecosystem if consent is to be obtained proactively and will investigate whether the data fiduciaries have already complied with these practices.

Consent mechanisms should be opt-in instead of opt-out

In interviews with Munish (Co-founder of Finvu) and Vinay (Chief Technologist at Perfios), it became evident that different types of consent artefacts will be used for different use cases within the ecosystem. For example, if consent is being sought for a lending use-case, the parameters of consent will probably be predefined and sometimes pre-chosen as well (meaning that will not be possible not to agree to providing the data), because in such a use-case, the FIUs bear a high risk; by seeking a certain amount of data, they hope to be able to assess their risk properly and thus mitigate it. However, in use-cases such as asset management, where the user is at higher risk, the user will have the ability to opt-in and customise the consent artefact. In other words, the system does not consistently follow an either-or approach. Instead, the mechanism on the basis of which consent will be sought, i.e. opt-in or opt-out, depends on the service that a consumer or user aims to seek.

While the flexibility of the AA ecosystem is acknowledged, research on status quo bias (Kahneman, Knetsch & Thaler, 1991) has highlighted that opt-out mechanisms do not allow users to express consent meaningfully, as users tend to choose the option that is presented as a default, despite having an alternative option. Moreover, Jolls and Sunstein (2005) have noted that people suffer from consent fatigue online and frequently do not wish to engage with privacy notices. In fact, people develop badger blindness: they get so accustomed to certain notifications that they do not opt-out or customise consent and just accept whatever option has been set as the default for them.

In order to prevent badger blindness and to obtain consent from people proactively, opt-in mechanisms have proven to be great nudges. Unlike a default opt-out option which automatically assumes consent, an opt-in mechanism creates an opportunity for a user to realise that they will be parting with their data and to assess and express, or deny, consent in a proactive manner.

Since AAs aim to seek meaningful consent, it is imperative they adopt opt-in mechanisms for all use-cases. It may be true that for certain use-cases, such as lending, wherein FIUs bear high risk and the financial instrument is strictly regulated, a certain amount of data is necessary. However, even in such cases the user should be able to effectively exercise their autonomy; pre-chosen or already opted-in options will affect the effectiveness of the system to seek meaningful consent.

Wherever consent is obtained, it should be clear that the response is "yes/affirmative"

The RBI's Master Directions provide that consent artefacts should be auditable and verifiable. However, the Directions, or any other document, do not delineate the definition of audit; thus it cannot be stated concretely what auditable exactly means according to the existing regulatory framework.

In conversations, early adopters and advocates of the AA ecosystem such as Rahul Matthan (Partner at Trilegal), Vinay (Chief Technologist at Perfios) and Munish (Co-founder of Finvu), explained that at the technical level, an auditable consent artefact in the AA ecosystem has been interpreted to mean that all consents that are created and revoked are logged and stored in a server maintained by the AA. This enables all users, AAs, FIUs and FIPs to be informed about whether consent was obtained, when it was obtained, for what purpose, and if it has been revoked. Thus, if this feature is deployed as envisaged, it will enable all stakeholders in the ecosystem to learn about the response of the user when consent is requested, creating a means to ascertain whether the user has expressed their consent in the affirmative.

As the tools mentioned in this discussion are still being developed and introduced, I could not independently assess this functionality, using the application.

No convoluted terms or phrases, which may make it difficult for a person to understand what the exact purpose of data collection is, should be used while seeking consent

In conversations, the developers and promoters of the AA apps highlighted that the AA ecosystem will seek consent granularly, i.e. step by step, from users, so as to enable users to transfer and manage their financial data. They also noted that the privacy policies will be easy to read and comprehend. And, on the basis of information available on Sahamati's website (Mahesh, 2020) and in the video about the application prototype available on Finvu's website (Finvu, n.d.), it does seem that the consent artefacts generated to seek information on behalf of FIUs are simple, and are being further simplified (Mahesh, 2020).

However, AAs as service providers use old mechanisms to seek consent from users. They have bundled up and hyperlinked the terms of service and privacy policies, which are lengthy, full of legalese, and not very easy to understand. For example, in the terms of use of the OneMoney app,[18] under the clause titled "Third Party Accounts", it is stated that "you hereby appoint Company as your agent". One cannot expect every individual wishing to use AA services to be aware of the meanings and implications of terms such as "agent" and "lawful attorneys", which is used elsewhere in the terms of use, among others. Thus, for many readers it may simply not be possible to understand the entire policy. And unless a user expresses their consent after reading and understanding the policy, the consent obtained cannot be termed meaningful (Solove, 2013 ; Cohen, 2017). Such an approach is, therefore, counterproductive to enabling user autonomy and seeking informed and granular consent, as this ecosystem aims to do. Moreover, this approach is not limited to OneMoney: the same mechanism has been adopted by Finvu (Finvu, n.d.) in its prototype as well.

Even though the FIUs in the AA ecosystem imbibe the principle of granularity while seeking consent from users, the way AAs seek consent themselves, thus, remains a weakness: the consent artefact remains a bundled-up notice, that is hyperlinked and full of legalese. This weakness can be resolved only if AAs revisit their means of seeking consent.

3.3. Consent is specific, continuous and ongoing

PRINCIPLE: When consent is approached as a contract, it fails to account for the changing conditions and realities of an individual's life. In a contract-approach to consent, once a person has expressed their consent for a sexual act and a certain level of intimacy is established between the two individuals, there is no means to withdraw consent, and consent for one act is often assumed to be consent for the following acts too (Cahill, 2001). This, however, is not necessarily correct: a person may not be interested or keen at a later stage, and may wish to pause or rescind from the act while in it or even before getting into it.

In this way, the contract-approach to consent therefore not only fails to acknowledge the spontaneity of sexual consent, but also enables blaming and shaming. People who wish to or actually withdraw consent during an act may start to doubt themselves, often resulting in incomplete and coerced consent forming the basis of the sexual act. Moreover, as the presumption is that consent once given cannot be altered later, the contract approach frequently results in people being blamed for exercising their autonomy (Alcoff, 2009). In contrast, to ensure that individuals can seek pleasure on their own terms, consent must be specific, continuous and ongoing Gruber (2016).

RELEVANCE: In earlier research, Kovacs and I (2020) noted that in the data protection regime, consent, once obtained by data fiduciaries, is often taken for granted (GPEN, 2017).

[18] Available at, https://www.onemoney.in/tandc.html

Thus, to prevent users from being trapped in a data ecosystem, the AAs, along with other technology frameworks, should ensure that consent is obtained for a specific purpose, and is continuous and ongoing, for a number of reasons. First, the ecosystem is being built to offer various products and services within a sector. For example, AAs in the finance sector aim to enable customers to seek loans, wealth management advice and insurance, among other services. But consent obtained for one particular purpose cannot be blindly assumed for another. Second, the time period for which an individual may invest in such an ecosystem could be very lengthy and their decisions with respect to consent might change during that time. And, third, the risk and the stakes with respect to financial and health decisions in particular are very high and subject to change over the course of the lifetime of a person. Thus, consent should not be taken for granted, to ensure control and autonomy to an individual over the long term.

ASSESSMENT: Thus, we look at four conditions that can help us evaluate to what extent the above mentioned principle has been adopted by the current AA framework.

Consent should be sought every time the purpose of usage of the data changes or when the user of the data changes

In the current consent regime, whether in the existing online banking system or on various social media websites, the norm is to seek consent at one place, in a single instance, and through a single form. This mechanism of seeking consent upfront for all subsequent transactions has proven to be ineffective in seeking informed consent. When data is collected to provide a particular service or a product, that data is often kept for a long time and reused for multiple purposes in the age of data aggregation and networked environments. Moreover, when the data is processed over and again, this is often for purposes which were not thought of or explicitly mentioned at the time of data collection. For consent to be meaningful, it is therefore imperative to seek the consent of a user every time the purpose for which the data is being used or shared is changing or the user of data is changing. For example, in banking, consent for data collection should be sought at the time of opening a bank account, again if later that data is shared with a third party, etc.

The account aggregator ecosystem aims to address the problems that arise from obtaining consent through one form at a single instance by instead seeking granular consent, obtaining separate consent for different purposes and on different occasions. As Rahul Matthan (Partner at Trilegal) noted in our conversation, DEPA and AA are frameworks that enable FIUs to seek consent on different occasions and not upfront, and that is a positive step.

However, one challenge that continues to exist is that this step-by-step approach to consent has not been coded into the regulatory framework for any of the products or services. Moreover, as noted earlier, in the absence of robust data protection regime FIUs can continue to ask for excessive data from individuals, the mere capability of the AA ecosystem to obtain consent continuously will not be sufficient to encourage FIUs to imbibe this principle. The latter in particular remains an important limitation.

Even after users express consent, they should be empowered with the ability to view, edit and delete their data

From the very inception of the AA ecosystem, we saw that this technology was conceptualised to empower individuals to view their accounts and data across financial institutions in a common format. It was only later, in 2016, that the RBI modified the functionality of the AAs from being mere viewing dashboards to data intermediaries and consent managers (Raghavan & Singh, 2020). Thus, one of the primary functions of the AAs continues to be the ability of a user to view their financial data, normally resting in silos, consolidated and in a common format.

The RBI's Master Directions, 2016 provide that an individual can access a record of the consents provided by them, along with the FIUs with whom the information has been shared. Moreover, while discussing the privacy of the records that are to be maintained by AAs to enable users to view these consents, Vinay (Chief Technologist at Perfios) highlighted that the AA client would store these consent logs in an encrypted format, which can only be decrypted on the customer's handheld device or computer. This means that individuals will have complete control over their consent data as the key to encryption will be generated by the user within their handheld device only. If any entity wishes to access this data they will have to seek an individual's permission and key to decrypt the data.

Along with the consolidated view of data, the RBI's Master Directions also equip the users to pause (temporarily) or revoke (permanently) consent. However, as of now, no regulatory direction or technology tool enables individuals to edit the data, once fed into the AA ecosystem, at any stage. This is problematic because there may be mistakes in an individual's data, or the data may undergo a change. In such cases, even if an individual wishes to correct their data so as to express their consent meaningfully, the ecosystem as it is does not allow them to do so. For consent to be meaningful, an individual should be able to at least raise a request to edit the incorrect or changed data.

Moreover, when an FIU raises a request to seek data, it is called a consent artefact. This consent artefact has information about the type of data that is being requested, the time period for which it is sought, the type of fetch it is, etc. But there is no provision for the user to view the actual data that an FIP transfers to an FIU before the transfer. Thus, the system expects an individual to remember what data resides with each FIP. It only allows an individual to view the consent requests and the data that is transferred after it is shared through the AA ecosystem. However, because many users will have set up their financial accounts a long time ago, they may not be aware what information of theirs is residing with FIPs. In addition, most banks that are FIPs in this ecosystem have such lengthy terms of conditions and data policies that users are not even fully aware of the data that resides with them. Thus, when an unaware user gives consent, their decision might have serious consequences, including unnecessary delays that may affect their livelihood.

To seek meaningful consent, users should be allowed to view the data that is being transferred to the FIU prior to the transfer, and in case the user is of the view that the data provided is incorrect, users should be allowed to raise a request to address and edit the discrepancies prior to transfer, to enable autonomy and prevent adverse consequences.

Users should be allowed to revoke consent at any time, and the mechanism to exercise that right should be seamless

To enable users to consent meaningfully, the system must offer an ability to revoke consent whenever desired by the user. The RBI's Master Directions provide that the AAs must design consent artefacts in such a manner that users can do precisely that. It is further prescribed that the mechanism to exercise revocation should be easy to adopt. This is a welcome step.

However, there is a regulatory vacuum regarding what happens when a person wishes to delete their AA user ID, and the data associated with it, after having been enrolled in the AA ecosystem. Currently, the RBI's Master Directions do not lay down any provision to delete that data, and the specifications are silent on what AAs can do with a person's data after that person decides to quit using AA services. To enable easy exit from the AA ecosystem, the RBI should also specify when and how the data of individuals will be removed after they revoke their consent to participate in the AA ecosystem.

Data fiduciaries should only gather the data that is necessary to provide the service or product

The AA architecture aims to enable users with control and autonomy over their data. To achieve this goal, it has been observed in previous research (Kovacs & Jain, 2020) that it is imperative to build a technology layer of specifications that provide for purpose limitation and a regulatory regime that prescribes punishments for excessive data collection or collection of behavioural surplus.

Behavioural surplus is data that is generated not to improve user experience, but to predict and orchestrate the future behaviour of users. Zuboff (2019) notes that behavioural surplus is a means to manipulate users in the name of convenience and comfort. Companies collect surplus data of individuals and then use that information to influence online and real time behavior of individuals. These practices are not mere nudges but are exploitative by nature. Therefore, to enable autonomy of the users over their bodies and data, such data accumulation practices should be prohibited.

Currently, the technical specifications for AAs provide that data should be collected on the basis of user consent and of a consent artefact which states the purpose of collection (Jagirdar & Bodduluri, 2020). However, no regulation or Direction imposes a hard mandate of purpose limitation. As a result, the ecosystem arguably can enable FIUs to collect excessive data about users. As Malavika Raghavan (Senior Fellow for India, Future of Privacy Forum) pointed out, "the text of the RBI's Master Directions, 2016 does not provide any restrictions or mandatory requirements vis-a-vis the manner in which customer financial data procured through the system may be used. The regulatory vision for the account aggregator system therefore remains to be clearly articulated in formal regulatory documents." One of the chief architects of the ecosystem, Saurabh Punjwani, also acknowledged that the system does not provide a good solution for preventing FIUs to collude with consent managers to over-collect data. And the AA ecosystem lacks the legal framework and market forces (where such practices are criticised) to prevent over-collection of data by FIUs, thereby limiting the ability of individuals to meaningfully express their consent in a specific, continuous and ongoing manner.

We have learnt in section 3.1 that due to the absence of regulatory standards on data collection by FIUs, FIUs can collect behavioural surplus of customers. This regulatory vacuum is disconcerting because misuse of data collected by FIUs can have far-reaching implications. For example, when credit or financial instruments are offered on the basis of data trails, in the absence of regulation FIUs can ask for access to the details of all expenditures made by an individual over a year. This data will provide FIUs with excessive insights into the behaviour and habits of a user, such as the number of times they buy alcohol or cigarettes. Such insights can then result in higher insurance premiums and mediclaims for such an individual. Thus, in the absence of purpose limitation, not only the autonomy of the user, but the right to liberty of individuals would be impacted.

Therefore, to enable user autonomy and ensure the right to liberty of consumers in the ecosystem, there should be more transparency in data collection and means to ensure that no excessive data collection and processing is taking place. Further, a user should be able to see what data will be transferred before the transfer.

3.4. Consent is a process

PRINCIPLE: In the previous principle, we have already learnt that one size does not fit all and that consent is a process. But as feminist scholars working on sexual consent have made clear, it is not merely about at which step, or at what time, one should seek consent: there should also be space to say "maybe" as part of the process (Bussel, 2008). This is because consent is not just about answering one question, i.e. whether to go ahead with an act or not, but also to understand why a partner is interested or not and to explore the desires of that partner. Thus, when consent is approached as a process, it allows a person to learn about and accept their partner with all the worries and fears that they may have regarding the act under consideration.

RELEVANCE: The account aggregator framework is a consent management framework that aims to allow users to manage and express consent with respect to their data with more autonomy than what the current consent regimes offer. In order to facilitate this, it must identify what the current regimes lack and address this. One of the pain points of current regimes is that personal data is perceived as a valid consideration for an exchange of services, and consent forms are treated as mere contracts governing that exchange. As a result, individuals have only two options: yes or no. There is no space to say "maybe". Thus, to enable users with the highest degree of autonomy, to genuinely understand and cater to the needs of the user, the tools must concentrate on user experience, and ensure that the user senses that seeking consent through the AA ecosystem is a process. The AA should be a toolbox that allows them to also manage their consent and not merely a technology to seek their consent.

ASSESSMENT: Thus, we look at two conditions that can help us understand to what extent the above mentioned principle has been adopted by the current AA framework.

Users should have the ability to say "maybe"

When I asked the early adopters of the AA ecosystem whether the consent artefacts enable users to say "maybe", apart from "yes" or "no", Vinay (Chief Technologist, Perfios), Krishna Prasad (Founder, Onemoney), and Munish (Co-founder, Finvu) all explained that FIUs request users for their data through a consent artefact and that users have the last say: they can always refuse to furnish the information sought. It appears that the current user interface design of the consent artefact does not allow users to say "maybe", or to question or suggest changes in the consent artefact. However, technologists are hopeful for the development of the artefact in the future to be more accommodative: with the evolution of the ecosystem, there may be the option of designing your own consent artefact, with certain mandatory information. At present, however, the ecosystem provides no hard mandate for FIUs to enable users to say "maybe", or to question or suggest changes in the consent artefact.

There should be an option for a user to speak with a person who works with the AA or FIU and is well versed with the nuances of data collection and processing

The AA ecosystem is geared to considerably simplify privacy policies and notices, as expressed in the DEPA book (NITI Aayog, 2020). However, when we look at the users of this ecosystem, they are very diverse, even with the limited application of AAs so far: AA services are being built for everyone above the age of 18 seeking financial products. Thus, users may include everyone from a tech-savvy school graduate, to a sixty five year old single woman who is hesitant to use technology to manage her financial affairs. In such conditions, a single format for the privacy policy to seek consent might not work, as the needs and qualms of users will likely vary significantly. A school graduate who is born in the digital age and is familiar with using online banking systems and other online services may be very comfortable sharing information while using AA services. On the other hand, a sixty five year old woman might have a number of concerns; for example, they may not be aware of terminologies and may not be familiar with certain icons and even the financial products.

Developers are aware of these challenges. Praneeth, technologist and fintech enthusiast, narrated the fears of his parents while using online banking. They are hesitant to use UPI or other online banking mechanisms, as they are unaware of the infrastructures that have been instituted to enable secure online transactions or of where and how to seek redressal in case of a mishap. These fears are not limited to Praneeth's parents: Mehra (2018) highlighted that there are countless senior citizens who are apprehensive about digitisation and about the use of technology to facilitate their financial transactions. They find new technologies time consuming and arduous because they are not familiar with the technology, and their deteriorating eyesight makes matters worse. As a result, the elderly often prefer

one-on-one assistance that allows them to seek out trained professionals to assist them in answering their queries and in their decision making.

In fact, from 6 July to 1 August 2020, Sahamati organised a four-week-long virtual hackathon on the following themes: consent management user interface (UI)/user experience (UX), security and middleware, FIU use cases, and artificial intelligence/machine learning. There were forty six submissions and some interesting innovations at the event. These included Aagya, which explored the usage of a guided chat as well as a vernacular voice assistant for a user, to enable the user to apply for a loan via a banking app and to provide consent for financial document sharing via the AA app. These also included Iconsent, a UX toolkit specifically designed for consent journeys for the very diverse user space. Notable use-cases of Iconsent include the usage of the audio background of video explainers of the consent mechanism in automated phone calls, as these audio backgrounds can reach out to users with the lowest of device/bandwidth provisions, and the AA consent management bot - both of which prescribe for semi-assisted consent. As Vinay (Chief Engineer at Perfios) expressed, since the policies prescribed by policymakers for this ecosystem are market agnostic and liberal, there is scope for a lot of innovation, including when it comes to assisted consent that enables users to have a dialogue with trained professionals and, thus, express consent meaningfully.

From this discussion, it can be learnt that assisted consent and other such mechanisms may not have been adopted yet. However, both AA developers and Sahamati acknowledge their importance and are aware of the value that they may bring in seeking consent. Thus, it can be hoped Sahamati will continue to build on the hackathon efforts to ensure assisted consent will become a reality in the future.

3.5. Consent allows for negotiation by all parties involved

PRINCIPLE: In hetro-patriarchal regimes, consent maps are frequently preconceived (Beres et al., 2004). According to such consent maps, it is mostly men who initiate sexual acts and seek consent from their partner, who are mostly women. In addition, women are often made to feel obligated to complete what they have started. There is no real space to negotiate. However, to enable equality of and respect for both partners, it is imperative to imbibe the principle of reciprocity. Feminists such as Braun, Gavey and McPhillips (2003) highlight that to achieve reciprocity in practice, the parties involved must both have the ability to walk away from a negotiation and the power to influence and re-draft the terms of the consent agreement. In other words, negotiability is key.

RELEVANCE: Account aggregators must ensure that the interests of all parties are taken into consideration. To put that into action, all parties should have the ability to negotiate. This means that all parties in the ecosystem - i.e. users, AAs, FIPs, and FIUs - should have the ability to influence decision making as far as their rights and responsibilities are concerned. However, due to the nature of technology and of society, it is not possible for every individual user to negotiate in their best interest in practice. Therefore, the system should inherently be designed to cater to the interests of the vulnerable.

ASSESSMENT: Thus, we look at four conditions that can help us understand to what extent the current AA framework enables negotiability.

The user should have the ability to deny consent without bearing any penalty, and in case a user does not want to use the AA ecosystem, the user should be able to access the same services through alternative means

On the basis of conversations with Vinay (Chief Technologist, Perfios), Krishna Prasad (Founder, Onemoney) and Munish (Co-founder, Finvu) specifically, it is clear that the AA ecosystem, as of today

enables users to deny consent without bearing any penalty. Even a limitation on access to credit is not imposed, as non-AA-based alternatives are abundantly available.

In addition, at the moment, enrolling in the AA ecosystem in India is not mandatory. However, there are people who have proposed compulsory enrolment, said Krishna Prasad while discussing the future of AA services. According to him, mandatory enrolment in one of the AAs and the linking of all financial accounts to the AA ecosystem would prevent various financial frauds, as the AA ecosystem, by allowing for the creation of data trails for every transaction, makes it very easy to trace problematic transactions.

This proposal for future mandatory enrolment in the AA ecosystem is reminiscent of the roll-out of Aadhaar, which was first introduced as a voluntary program but was made mandatory later for a range of purposes, including to avail of essential services such as subsidies (Khera, 2017) and to file income taxes (Agarwal, 2019). However, the Supreme Court of India in *Puttaswamy J.* (2017), and later reaffirmed by multiple decisions including the *Puttaswamy J.* (2019) also known as the Aadhar judgement, held that access to and enjoyment of welfare schemes of the State cannot be refused merely on the ground of absence of Aadhaar. This precedent is a worthy safeguard against mandatory participation in any ecosystem that facilitates basic aspects of an individual's life and livelihood.

If mandatory adoption of AAs would be endorsed, it would also be counter to the stated aim of AAs, i.e. to enable individuals to share with their consent information currently residing in silos. As elaborated by some of the early adopters and policy-makers, AA systems are intended, among other things, to replace the traditional credit facilities with more accessible credit delivery systems. Thus, if a user can be denied credit simply because she is not a participant in the ecosystem, then it means that this ecosystem allows very limited flexibility in negotiating and providing meaningful consent. Of course, some people cannot access and use this ecosystem in the first place, as it requires a smartphone, an Internet connection, and financial literacy, among other things, which I will discuss later in greater depth.

The ability to deny consent without penalty and not having a compulsory mandate to access financial services through AAs are, of course, only meaningful if individuals can continue to access the same services through alternative means. In our conversation, Kamya Chandra, full time volunteer at iSPIRT and co-author of the DEPA book (NITI Aayog, 2020), highlighted: “credit can be termed as an equivalent of “aspirations”: it gives you an ability to seek education, aspiration for expanding your business, among others.” Considering that financial credit enables innumerable individuals to aspire, dream, and grow, it is imperative to ensure that credit is always accessible to all, especially to those who are vulnerable.

Thus, it appears that at least for now, the ecosystem grants users the ability to deny consent for sharing their information without penalty and does not mandate them to access financial services through AAs, while individuals are able to continue to access the same services through alternative means.

Consent artefacts serve users' interests and users have the ability to influence the drafts

To assess whether users have the ability to negotiate, it is crucial to learn who has the authority to draft consent artefacts and whose interests such artefacts will serve. Most interviewees agreed that in the current ecosystem, the authority to draft consent agreements rests primarily with the FIUs. Munish (Co-founder of Finvu) highlighted that there is no regulatory requirement for consent artefacts to be negotiable, but that the Reserve Bank of India reserves the authority to lay down the boundaries within which FIUs can draft these consent templates. The framework will include data governance guidelines (which are still being finalised) regarding matters such as how long FIUs can keep the data and what data definitely should be sought by FIUs prior to extending credit. Nevertheless, these will only be a set of guidelines; the RBI will not be exercising oversight upon every consent artefact. Moreover, different FIU are regulated by different sectoral financial regulators - for example, insurance companies are

regulated by IRDA, while other FIUs are regulated by other statutory bodies. However, none of the financial regulators other than the RBI provide data protection regulations, and there is no overarching data protection law. Thus, in the current situation, FIUs have indisputable power to draft the terms of the consent artefact.

The question of whose interests these consent artefacts serve is more difficult to investigate, due to the nascent stage of the ecosystem. There are neither a lot of use cases nor many FIUs to compare. Moreover, interviewees had divergent views on this question. Srikanth (Cashless Consumer, 2020) argued that industry players can misuse their dominant position in financial markets to unanimously decide which data and type of consent should be sought. For example, while query consent or view-only consent may be sufficient to perform a particular service, industry players can unanimously decide to nevertheless request for store consent. Rahul Matthan and Krishna Prasad, in contrast, were optimistic. They were of the view that the platformization of ecosystem services and increased competition will force FIUs to provide services with competitive offers. According to them, the DEPA/AA framework will transform the marketplace from a seller's market to a buyers' market, and as a result, the user will always have an ability to negotiate.

However, the mere ability of users to choose their service provider among a multitude is not necessarily enough to ensure that the user's interests are being taken into consideration or that the user has the ability to negotiate. Rather than leaving the protection of user interests to market forces, there should be a framework that governs which data can be collected for what purpose and what type of consent can be sought for it. In addition, in order to enable negotiability, representatives of all stakeholder groups should be engaged in drafting consent templates. As of now, only FIUs have been involved in this process. This is a problematic approach and hence, needs to be reconsidered.

Data fiduciaries should not be allowed to change privacy policies unilaterally

Onemoney's terms of use state that Onemoney reserves the right, at their sole discretion, to change, modify, add or remove portions of their terms of use at any time, without any prior written notice to the user. From this clause, it is clear that Onemoney can unilaterally change its terms of use. In fact, the terms also shift the responsibility on users to review periodically for changes and updates. The only exception that is stated in the policy is that Onemoney will serve a notice to users prior to changes if a law obligates them to do so.

Since the RBI Master Directions and Technical Specifications are silent on the governance of revision of privacy policies by entities in the AA ecosystem, there is no means to prevent data fiduciaries in the ecosystem, i.e. AAs, FIPs, and FIUs, from adopting such practices. This is disconcerting. If, after users have consented, data fiduciaries can unilaterally change privacy policies without even informing users, this renders already obtained consent meaningless, as users are left with only the option to agree or to stop using the service, and in some cases, users will not even be aware that changes have been made, seeing that there is no obligation to notify users.

Such practices have of course been standard with most digital service providers (Solove, 2013). However, it is not ideal in the case of AAs, an ecosystem that aims to enable individuals with more control and autonomy over their data and is supposedly driven by meaningful consent. Such unilateral changes by the AA, thus, transgress into the user's right to privacy and will impact the ability of the user to provide meaningful consent (Norton, 2016).

In fact, such practices are increasingly criticised by both civil society and government outside of the AA ecosystem as well. In January 2021, the Facebook-owned messaging service WhatsApp unilaterally

changed its privacy policy in India, so as to share even more of users' sensitive personal information with the parent company. The policy received a lot of backlash from both civil society (Chaturvedi, 2021), and the government, with MeitY writing a strongly worded letter to the WhatsApp CEO, asking to withdraw the proposed changes in its privacy policy and reconsider its approach (while WhatsApp delayed the implementation of the new policy, it did not take these suggestions into account) (Rathee, 2021).

Despite the growing disquiet regarding such practices, the AA ecosystem thus provides no means to discourage such practices from taking place.

Users must have a possibility to object to third party data sharing

The involvement of third party data processors may be crucial for the functioning of digital services. However, in the absence of explicit mention of details of these third party data processors and the purposes for which they require a user's data, the user bears an unreasonable burden to protect her privacy. Moreover, in addition to not providing such details, most privacy policies include a saving clause excusing them from liability for the practices of third parties. This results in an opaque system that circumvents the essence of a user's consent (Kovacs & Jain, 2020). In this context, it is necessary that the user has access to mechanisms within the ecosystem to object to third party data sharing. These mechanisms should be made available to every individual as long as the third parties are processing personal data of individuals. This should be made possible through technical and regulatory tools.

In the AA ecosystem, Direction 7.6.2 of the RBI's Master Directions states that financial information that has been provided by an FIP to an account aggregator for transferring to the customer or an FIU shall not be used or disclosed by an account aggregator or the FIU except as may be specified in the consent artefact. This implies that an AA or an FIU shall ideally not be allowed to share users' information with third parties without their consent.

However, the Master Directions only require FIPs to maintain a log of all information sharing requests and the actions performed by them pursuant to such requests, and submit these to the account aggregator. This is problematic because a lot of data will be collected by FIUs, and although they are obligated not to share that with third parties without consent of the users, it will be difficult to hold them accountable for their acts if the FIUs are not required to maintain logs of their data sharing.

3.6. Consent should be free from physical force, such as coercion, abuse and intimidation, and social force, such as peer pressure or cultural norms and biases

PRINCIPLE: In my earlier work with Kovacs (2020), we highlighted that it is a common misbelief that all individuals have equal ability to make choices based on their free will. In practice, individuals are bound by multiple social, economic, cultural and historical factors, and it is these factors which play a significant role in determining the extent of freedom an individual has (Munuswamy, 2020).

RELEVANCE: Thus, for an AA seeking meaningful consent, it is vital to take into consideration factors such as economic and social power structures. For example, to meaningfully express consent to participate in an ecosystem, one must be able to comprehend what consent is being asked for, which requires, among other things, the ability to read in the language in which the consent request is furnished; understanding of the purpose for seeking consent; and what giving or denying consent would lead to. If a person fails to understand any of these aspects, the consent obtained from them cannot be termed meaningful or informed.

ASSESSMENT: As an individual's capacity to express or deny meaningful consent is contingent upon many factors, the following *five conditions* must, at a minimum, be observed by the AA ecosystem to ensure that consent is free from physical and social forces.

The applications and interfaces should be made available in vernacular languages

In order to enable, for example, financial inclusion across India, and to seek meaningful consent from people while introducing them to financial products, it is imperative to take into account the linguistic diversity of the nation. Almost a decade ago, Vijaya Bhaskar (2013), the then Executive Director of the RBI, already highlighted that vernacularisation of all banking forms is a must to enable financial inclusion in India. To enable people to access financial products and services, financial institutions, he argued, need to put an end to the use of English as the sole language of financial communication. Amitabh Kant, the CEO of NITI Aayog, has also acknowledged and advocated that, to increase market share and enable the integration of individuals in the financial sector, fintech companies must design in the vernaculars, as opposed to sticking to only English as a language of delivery (PTI, 2020). As recently as 2016, only 175 million of the 403 million Indian Internet users were comfortable with and habituated in using English to access the Internet and Internet based services (KPMG and Google, 2017). Yet currently, most financial institutions continue to provide services only in English and exclude a large part of the population. If, over the last decade, despite increased Internet penetration and efforts towards financial inclusion, India has failed to achieve high adoption of financial services from formal means such as banks and institutions, the continued dominance of English in financial communication is, then, a major reason (Bhasker, 2013). If the AA framework continues this trend of creating tools only in English language, it will be counterproductive to the goals of financial inclusion and enabling autonomy (Mathur, 2020).

The developers of account aggregator platforms are aware of and acknowledge the value of vernacularisation to enable autonomy. In fact, (Founder of Onemoney), noted that developers at Onemoney are building the application in Hindi and eleven other Indian languages, such as Punjabi and Tamil. However, the beta version of the app is available in only two languages, Hindi and English. Moreover, for other platform developers, localisation has not been a primary concern: they expect that with adoption and innovation, more regional languages will eventually be integrated. For example, Vinay (Chief Technologist at Perfios) noted that because consent management, which is at the heart of the AA ecosystem, is not a complicated technology mechanism, it will be simple for innovations to take place that will allow assimilation of regional languages. He also believes that with the reach expanding from urban to rural areas, more regional languages will be supported. Similarly, Munish (Co-founder of Finvu) argued that at the moment, this ecosystem is being designed for tier one cities and mostly for smartphones; since most smartphones have an in-built feature that translates content into multiple languages, there is not a pressing need for vernacularisation for such smartphone users. Although feature phones currently have very limited language choices and content cannot be translated automatically on them, Munish is also of the view that over time, automatic vernacularisation can be made possible on feature phones too.

Prioritising the smartphone-using urban population fails to consider, however, that increasing financial inclusion is a dire need among the semi-urban and rural population of the country in particular (Ravi, 2019), among whom smartphone penetration is at a dismal fourteen percent (GSMA Connected Women, 2020). Currently, as the service is not available on feature phones and does not have vernacular user interfaces, the AA system effectively excludes large parts of this section of the population. The stated goal of AAs is to enable autonomy over financial data and thereby achieve greater financial inclusion. But this can be achieved only when pre-existing structural and institutional flaws are tackled from the very beginning by designing the system to cater to those generally excluded. The lack of access to financial communication and services owing to language barriers can be overcome by designing systems

incorporating vernacularisation right at the initial stages of development. Not doing so defeats the stated purpose of financial inclusion underlying the ecosystem. By not facilitating meaningful access to the service in the first place, most users are also prevented from expressing informed consent.

AA services should be available and accessible for people with disabilities

In the first phase of iterations of the account aggregator applications, people with disabilities also have not been prioritised. Developers expect that with the evolution and adoption of the ecosystem, innovations will take place that will accommodate people with disabilities. However, as a peek into Aarogya Setu, the Covid-19 contact tracing app promoted by the Government of India, illustrates, it is essential to incorporate accessibility into design in the initial stages itself. In the days following its launch, Aarogya Setu was made essential to access many public spaces (Jain and Ranjith, 2020). It was also adopted en masse to facilitate access to private spaces for the ease of contact tracing. This caused concerns for disabled Indians in particular, as the application design did not cater to their needs (Malhotra, 2020), and therefore, a considerable population of the country was prevented from accessing public spaces. Such an approach tends to marginalise the already vulnerable, resulting in exclusionary systems. Moreover, technology once built and used by popular adoption seldom prioritises product design changes in later iterations. This leads to exclusionary public goods, as has been seen across the world in multiple technological interventions, and to continuing inaccessibility that further perpetuates systemic oppression of disabled people (Costanza-Chock, 2018). Developers must address these gaping holes in the system that prevent people with disabilities from expressing or denying their informed consent.

AA services and products should be easily accessible to people who may not have formal education

Interviews with individuals who have been involved in visualising, conceptualising and iterating AA consent tools made evident that the AA pilot applications and tools are being built for people who can read and write. As the previous sections of this paper made clear, the tools presume individuals can read the terms and consent forms. Although assisted consent and other features have been suggested, at the moment they are not functional. Onemoney, which is piloting its application, expects a user to read the terms of service.

But this is difficult for an individual who has not had access to formal education. The terms of service are convoluted and demand considerable comprehension of the financial system as well as of legalese. In India, access to formal education, so far, has been an indicator of higher financial literacy and better access to the formal financial systems (NABARD, 2018). When an overarching framework like that for AAs is designed and implemented, it should take this structural barrier into consideration if it is to actually enable users autonomy over their financial data and achieve the goal of financial inclusion. However, this is lacking to date, and thus, the framework may end up reinforcing pre-existing structural barriers to accessing formal financial systems instead.

AA systems must not wait to address this flaw, as this ecosystem is to enable control and autonomy of individuals over their data. The ecosystem should be made accessible for all and particularly those whose financial access has been severely hampered for decades now.

The tools and services should be available at lower Internet speeds to enable meaningful participation in the ecosystem of individuals from tier two and tier three cities and from rural areas

While Internet data might be very affordable in India, India lags when it comes to data speeds. The latest Speedtest Global Index from Ookla ranks India 131st in the world with respect to mobile data speeds (Business Today, 2020). India's average mobile data speed is 12.08 Mbps (Business Today, 2020), less

than half of the global average speed. Even in neighbouring countries like Pakistan and Sri Lanka, data speeds are higher according to the Ookla survey (MoneyControl News, 2020). The first step to user empowerment in a consent management system is unhampered access to the means to express consent. Thus, for every individual to be a part of the AA ecosystem, apart from a handheld device there is a need for AA apps that can be accessed at average available Internet speeds in India.

Vinay (Chief Technologist at Perfios) noted in an interview that the way AA apps are being built, they are very lightweight and do not require particularly high Internet speeds. Rather, "they require similar cellular bandwidth as is needed for UPI, [so] it should be fine. So even in your 2G or 3G network, it should work."

As no trials have been conducted thus far, it cannot yet be concluded with certainty that the applications or tools work with lower speed Internet such as 2G. However, the developers are aiming to devise the apps in a manner that their functionality is not compromised at lower speeds. This is appreciated, and is imperative to enable participation and facilitate meaningful expression of consent.

The ecosystem should allow users to manage their consent even without a personal phone number

Participation in the AA ecosystem, and thereby the exercise of control over expression of consent, is facilitated by accessing the ecosystem through a personal device. To enroll within the AA ecosystem in its current iteration, each user needs to register using their unique credentials. Currently, these credentials consist of the full name and unique mobile number to which the accounts and other financial data connected to the user are linked.

The availability of personal handheld devices in India is not coextensive with the number of users of Internet mediated technologies. Women's access to a personal device that can be used to connect to the Internet is much lower than that of men (GSMA Connected Women, 2020). This is troubling, as these women may then be excluded from the AA ecosystem. They would not have an opportunity to engage and exercise control over their financial data through the ecosystem, resulting in further marginalisation.

In India women have been specifically deprived of access to personal devices owing to patriarchal norms and societal structure (Kovacs, 2017). The conservative and patriarchal societal structure discourages (financial) independence of women, often perceived as a threat by men (Bhandari & Kovacs, 2021). Hence, ensuring the existence of mechanisms that preserve privacy and autonomy is imperative for the engagement of this demographic with the AA ecosystem. To enable financial inclusion for all, multiple users should all be able to access AAs with equal privacy from one device and sim.

Currently, apart from the web interfaces of OneMoney and Finvu, other AAs have been envisioned as mobile applications that will be made available on smartphones in the first phase and on feature phones in the probable future. Even where the interface is a web-based one, they will be connected to a mobile phone number, however. Considering that every individual will have a unique ID, it is possible to use the same device by different individuals, but that account holder still requires a separate phone number to create an account.

Therefore, this ecosystem as of today, demands every participating individual to personally own a mobile number, registered in their name, even if they have a shared handheld device. Since the current ecosystem does not factor in a considerable share of the women population of India, a majority of the women population of the nation would be left behind in exercising autonomy over their personal and financial data. Thus, AA applications must ensure that such a divide is not furthered by its implementation, defeating the purpose of free and meaningful consent from every user.

4. Lessons Learnt from the Assessment

After examining the AA ecosystem against the feminist principles of consent in the age of embodied data, it is clear that the AA framework is a positive step towards addressing some of the concerns regarding current consent regimes. For example, it makes clear gains where auditability and granularity are concerned. However, to fully meet the conditions that have been identified in this paper to ensure meaningful consent, making further modifications will be necessary. In section three of this paper, I have tried to identify the benefits of the ecosystem and to highlight the areas of concern that need to be revisited prior to the full-fledged roll-out of AA services. In this section, I will summarise the lessons that were learnt from the assessment.

First, the AA ecosystem does not embody the principle of relational autonomy. The focus of the ecosystem has been on the consent management intermediary, i.e. the AA, and how to make it secure, transparent and trustworthy. But the framework fails to take into consideration the impact that other data fiduciaries in the ecosystem, such as FIUs and FIPs, may have on seeking meaningful consent. FIUs are empowered to dictate the terms of consent artefacts and to obtain any information they deem fit from users. At the same time, the framework currently provides minimal information about the mechanisms used and the third parties (cloud service providers, data processors, etc.) involved with the system. Other insights that highlight the subordination of users in the ecosystem include the lack of a technology layer as well as a regulatory mechanism to assess whether FIUs are practicing purpose limitation in a substantive manner. Moreover, the regulatory requirements in the ecosystem do not obligate data fiduciaries to assess the risks associated with data processing either. Regulatory safeguards preventing the abuse of dominance by players is absent, nor is there a mandate to inform users about data breaches or leaks. This means that the ecosystem takes a very narrow approach: it positions AAs as the silver bullet to enable autonomy while failing to prevent the subordination of users at the behest of FIUs and FIPs.

Further, when assessing to what extent the AA ecosystem seeks consent proactively, it was found that the AA framework is more equipped to seek consent proactively in comparison to existing consent regimes. As far as opt-in and opt-out consent artefacts are concerned, the AA ecosystem prescribes for a mixed approach. It suggests the use of different consent artefacts for different use-cases. However, as discussed, the opt-out mechanism is insufficient to nudge people to proactively give consent, which must be addressed. The AA ecosystem also provides an audit mechanism. If the mechanism is enforced as envisioned, it will enable users and data fiduciaries with more clarity vis-a-vis data flows. Currently, however, it only enables users to keep a tab on the information and consents shared with different FIUs, and not on user details resting with FIPs. Thus, there is scope for further change to ensure consent is obtained proactively.

Some of its characteristics indicate that the ecosystem requires consent to be specific. Firstly, the framework requires FIUs and FIPs to seek consent on different occasions for different purposes and not upfront for all future behaviour. Secondly, as mentioned, users will have a consolidated view of their consent with respect to their data resting in silos, through a dashboard containing all consents for data that has already been shared with FIUs. Thirdly, users are empowered to revoke consent at any time. These measures can ensure that the consent sought is specific while maintaining the seamlessness of the mechanism. However, they are not enough for consent to be continuous and ongoing. The ecosystem needs to acknowledge that human conditions are not static, and may demand changes in previously taken decisions. Moreover, currently, there is no regulatory requirement or technical specification for the products or services to seek consent at every step. Thus, there is no mandate that every FIU should adopt this functionality to accommodate any changes in consent. Further, the ecosystem does not allow individuals to edit data once it is fed into the AA ecosystem; all they can do is revoke or pause consent.

Lastly, there is no provision for the user to view the data that an FIP will transfer to an FIU prior to the transfer, although this would aid substantially in ensuring purpose limitation.

We also learn that the AA framework does not conceive of consent as a process, as is evident from the relegation of user control over the expression of consent to a simple yes or no. The absence of an explicit human point of contact to navigate the technical intricacies sheds light on the fact that the concept of assisted consent has not yet been integrated into the framework. For a service catering to an extremely wide range of users and claiming to target specifically those previously excluded from access to financial services, it is imperative to develop assisted consent and other (technical) tools to improve access to the technology.

Merely perceiving consent as continuous and proactive is, however, not enough. Seeking consent is a process, and for the consent to be meaningful, a user should be able to say no to any practice that doesn't relate narrowly to the service being provided. This would contribute to the user's ability to negotiate the terms of the agreement. From section three of this paper it is clear that the users at present have limited ability to negotiate. Data fiduciaries remain excessively empowered to dictate the terms of consent in the AA ecosystem. According to the privacy policy of Onemoney, they have reserved the right to unilaterally change their privacy policies without informing users. Moreover, the ecosystem provides no means to object to or revoke consent for third party data sharing. Thus, reflecting existing practices in data governance more broadly, the ability of a user to negotiate barely exists in the ecosystem.

Finally, in some situations, providing notice and asking for consent do not adequately address the concern of free consent. In many cases individuals may not have the capacity to express consent because of the physical or socio-economic context they find themselves in. The AA ecosystem has not factored this in in its current iteration. Despite being aware of and acknowledging the value of vernacularisation, localisation is yet to find a place at the heart of the ecosystem. Rather, the expectation is that with adoption and innovation, more regional languages will eventually be integrated. Moreover, the ecosystem misjudges the ability of various marginalised communities to participate in the AA ecosystem. The pilot applications and tools are being built for people who can read and write and are currently only available on smartphones and websites. The AA ecosystem demands every participating individual to personally own a mobile phone number registered in their name. A sizable portion of semi-urban and rural India in particular will therefore be prevented from participating in the ecosystem, let alone being able to express meaningful consent, even though the ecosystem was supposedly conceptualised precisely to improve their ability to exercise autonomy over their financial data.

5. Recommendations

As the AA ecosystem is in the process of being iterated, it may not be possible to present all changes to seek meaningful consent at this time. However, as it continues to evolve and adapt, the following key recommendations should be implemented immediately to strengthen user autonomy and meaningful consent along the above lines.

5.1. Regulatory Changes

- Until the Personal Data Protection Act, regulating the flow of personal data in India, is promulgated, the RBI should set up a task force or committee comprising experts from the field. They must notify clear data protection rules such as purpose limitation, collection limitation, etc., and lay down penalties, before the full rollout of AAs. AAs as well as all other data fiduciaries within the ecosystem should comply with the said rules.

- If the draft version of the Personal Data Protection Bill, 2019 is promulgated, the financial regulators must, at the very least, ensure that the FIPs and FIUs do not over-collect and over-process personal data of individuals under the garb of section 14, to assess creditworthiness or for "other reasonable purposes". FIPs and FIUs should be obligated to seek consent from individuals for all personal data collected by them, and must expressly inform these individuals about the purposes for which they are collecting and processing data.
- As regulators, both the RBI and the Competition Commission of India (CCI) have an important responsibility to enable competition. They must identify and eliminate anti-competitive behaviour, such as monopoly pricing, cartelisation by players, customer-locking and any other market abuse (Uppal, 2020). In addition, a clear revenue model for the ecosystem should be delineated by the RBI after having public consultations.
- The RBI should delineate penalties for storage of data beyond seventy two hours of data transactions by AAs, and should also delineate norms regarding storage of data by FIUs and FIPs.
- To enable transparency, data fiduciaries should observe transparency in the processing of personal data, report personal data breaches, conduct data protection impact assessments and maintain clear records of all of the above measures.
- To enable easy exit from the AA ecosystem, the RBI should specify when and how the data of individuals should be removed after they revoke their consent to participate in the AA ecosystem.
- To prevent collection of unnecessary data and behavioural surplus from users, the RBI should, following public consultations, set a standard which delineates who can collect data, what data they can collect, for how long they can store it and what type of consent (view, storage or authentication) should be sought for each expected use-case in the AA ecosystem.
- The RBI should obligate data fiduciaries to inform users prior to changing their privacy policies and users should have the ability to opt-out prior to the change. Further, users should have the option to continue using the services for a reasonable time as per old policies, especially if the new policies may harm or have serious implications for users.
- Like FIPs, the RBI must mandate FIUs to maintain logs of their data sharing, to hold them accountable in case they fail to follow the data sharing norms prescribed by the RBI.

5.2. Technology Changes

- There should be a mechanism to learn when a user's data is being used by any data fiduciary and why. For example, when a machine learning algorithm is run by an FIU over a user's data, they should be notified of the same. Users should be able to keep track of the various occasions and purposes for which their data is being used.
- For all use-cases, consent should be obtained through an opt-in consent mechanism.
- Users should be allowed to view the data that is being transferred to an FIU prior to the transfer. In case the user is of the view that any of this data is incorrect, users should be able to raise a request to address and edit the discrepancies prior to transfer.
- To further enable user autonomy, there should be a mechanism that allows users to create their own encryption key for their data.
- To enable users of all demographics to manage their consent, there should be an option for users to speak with a person who is well versed with the nuances of data collection and processing and can assist the user in resolving their queries.
- All applications and interfaces should be made available in the twenty two official languages of India as listed in the VIIIth Schedule to the Constitution of India.
- Developers must ensure that people with disabilities can access the AA ecosystem. Design sprints and hackathons involving people with disabilities and experts who design applications for people with disabilities should be conducted, to enable them, too, to express or deny their

informed consent through the AA ecosystem.

- The ecosystem should allow users to manage their consent even without a personal phone number, to prevent exclusion of a considerable segment of the population of users in our nation.

Annexe I

Listed below are the six feminist principles on the basis of which the analysis of the AA framework in this research has been undertaken. It further lists the conditions used to analyse in detail whether and how each principle is translated into practice in the AA ecosystem.

1. Consent must be embedded in a notion of relational, rather than individual, autonomy

a. The ecosystem should provide means that prevent data fiduciaries from misappropriating and misusing user data.
b. The ecosystem should enable users to choose and switch AA at any time, without being bound by a penalty or lock-in periods. This implies that there should be a sufficient number of AAs competing with each other in the market. In addition, there should be many FIUs, so that users have the ability to choose from a variety.
c. Privacy respecting ecosystems are easier to promote and operationalise as users are less hesitant to give consent when they believe their data will be kept private. Thus, the ecosystem should provide regulatory and technical tools or frameworks to ensure privacy.
d. Transparency measures need to be proposed by the regulators, so that users can become aware of the conditions and mechanisms deployed by data fiduciaries and thus, express their consent freely.

2. Consent should be sought proactively

a. Consent mechanisms should be opt-in instead of opt-out.
b. Wherever consent is obtained, it should be clear that the response is “yes/affirmative”.
c. No convoluted terms or phrases, which may make it difficult for a person to understand what the exact purpose of data collection is, should be used while seeking consent.

3. Consent is specific, continuous and ongoing

a. Consent should be sought every time the purpose of usage of the data changes or when the user of the data changes.
b. Even after users express consent, they should be empowered with the ability to view, edit and delete their data.
c. Users should be allowed to revoke consent at any time, and the mechanism to exercise that right should be seamless.
d. Data fiduciaries should only gather the data that is necessary to provide the service or product.

4. Consent is a process

a. Users should have the ability to say “maybe”.
b. There should be an option for a user to speak with a person who works with the AA or FIU and is well versed with the nuances of data collection and processing.

5. Consent allows for negotiation by all parties involved

a. The user should have the ability to deny consent without bearing any penalty, and in case a user does not want to use the AA ecosystem, the user should be able to access the same services through alternative means.
b. Consent artefacts serve users' interests and users have the ability to influence the drafts.
c. Data fiduciaries should not be allowed to change privacy policies unilaterally.
d. Users must have a possibility to object to third party data sharing.

6. Consent should be free from physical force, such as coercion, abuse and intimidation, and social force, such as peer pressure or cultural norms and biases

a. The applications and interfaces should be made available in vernacular languages.
b. AA services should be available and accessible for people with disabilities.
c. AA services and products should be easily accessible to people who may not have formal education.
d. The tools and services should be available at lower Internet speeds to enable meaningful participation in the ecosystem of individuals from tier two and tier three cities and from rural areas.
e. The ecosystem should allow users to manage their consent even without a personal phone number.

References

Agarwal, Nikhil (2019, April 2). Quoting Aadhaar made mandatory for filing income tax returns (ITR) from this month: 5 things to know. *LiveMint*. https://www.livemint.com/money/personal-finance/income-tax-returns-itr-pan-card-aadhaar-aadhar-linking-1554178613782.html

Alcoff, Martin L. (2009). Discourses of sexual violence in a global framework. *Philosophical Topics, 37(2)*, 123-139. http://www.jstor.org/stable/43154560

Austin, Lisa M. (2014). Enough about me: Why privacy is about power, not consent (or harm). In Austin Sarat (Ed.), *A world without privacy: What law can and should do?* (pp. 131-189). Cambridge University Press. DOI: 10.1017/CBO9781139962964.004

Barboni, Giorgia, Field, Erica, Pande, Rohini, Rigol, Natalia, Schaner, Simone, & Troyer Moore, Charity (2018, October). *A tough call: Understanding barriers to and impacts of women's mobile phone adoption in India.* Harvard Kennedy School. https://epod.cid.harvard.edu/sites/default/files/2018-10/A_Tough_Call.pdf

Basu, Samraat & Sonkar, Siddharth (2020, April 1). Regulating consent managers in India: Towards transparency and trust in digital economy. *Oxford Business Law Blog.* https://www.law.ox.ac.uk/business-law-blog/blog/2020/04/regulating-consent-managers-india-towards-transparency-and-trust

Belgavi, Vivek & Narang, Avneesh (2019, November 4). Account aggregators: Putting the customers into charge. *PWC India.* https://www.pwc.in/consulting/financial-services/fintech/fintech-insights/account-aggregators-putting-the-customer-in-charge.html#sources

Beres, Melanie Ann, Herold, Edward & Maitland, Scott B. (2004). Sexual consent behaviors in same-sex relationships. *Archives of Sexual Behavior*, 33(5), 475–86. DOI: 10.1023/B:ASEB.0000037428.41757.10

Bhandari, Vrinda & Kovacs, Anja (2021, January). *What's sex got to do with it? Mapping the impact of questions of gender and sexuality on the evolution of the digital rights landscape in India.* Internet Democracy Project. https://internetdemocracy.in/wp-content/uploads/2021/01/Vrinda-Bhandari-and-Anja-Kovacs-Whats-Sex-Got-To-Do-with-It-2.pdf

Bhasker, P. Vijaya (2013, December 10). Financial inclusion in India: An assessment. https://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=862

Braun, Virginia, Gavey, Nicola & McPhillips, Kathryn (2003). The `fair deal'? Unpacking accounts of reciprocity in heterosex. *Sexualities,* 6(2), 237-261. DOI: 10.1177/1363460703006002005

Business Today (2020, October 26). India ranks 131 in global mobile internet speed; Fares worse than Nepal, Pakistan. *Business Today.* https://www.businesstoday.in/technology/news/story/india-ranks-131-in-global-mobile-internet-speed-fares-worse-than-nepal-pakistan-276698-2020-10-26 .

Bussel, Rachel Kramer (2008). Beyond yes or no: Consent as a sexual process. In Jaclyn Friedman & Jessica Valenti (Eds.), *Yes means yes! Visions of female sexual power & a world without rape* (pp. 43-52). Seal Press.

Cahill, Ann J. (2001). *Rethinking rape*. Cornell University Press.

Cashless Consumer (2020). Study circle on account aggregators. *Hasgeek.* https://hasgeek.com/cashlessconsumer/study-circle-on-account-aggregators/

Chaturvedi, Anumeha (2021, January 14). India Inc. cautions employees on WhatsApp privacy policy changes. *The Economic Times.* https://economictimes.indiatimes.com/tech/technology/india-inc-cautions-employees-on-whatsapp-privacy-policy-changes/articleshow/80205646.cms

Cohen, Julie E. (2019). Turning privacy inside out. *Theoretical Inquiries in Law*, 20(1), 1-31. DOI: 10.1515/til-2019-0002.

Costanza-Chock, Sasha (2018). Design justice, A.I., and escape from the matrix of domination. *Journal of Design and Science.* DOI: 10.21428/96c8d426.

Eveleth, Rose (2019, June 13). Credit scores could soon get even creepier and more biased. *Vice.* https://www.vice.com/en_us/article/zmpgp9/credit-scores-could-soon-get-even-creepier-and-more-biased

Finvu (n.d). *How it works.* Retrieved April 13, 2021, from https://finvu.in/howitworks

Gruber, Aya (2016). Consent confusion. *Cardozo Law Review*, 38 (2), 415-457. https://scholar.law.colorado.edu/articles/11

Global Privacy Enforcement Network (2017, October). *GPEN Sweep 2017: User controls over personal information.* UK Information Commissioner's Office. https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20- %20International%20Report.pdf

GSMA Connected Women (2020, March). *The mobile gender gap report 2020.* GSMA https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf

Income Tax Department (2020, August 31). *Section 138 of the Income-Tax Act, 1961: Disclosure of information respecting assessees to specified officer, authority or body performing functions under any other law - Notified authority under Section 138(1)(A)(II).* Ministry of Finance, Government of India. https://www.incometaxindia.gov.in/Pages/utilities/Authorities-For-Disclosure-Of-Information.aspx

Jagirdar, Rohan & Bodduluri, Praneeth (2020, May 30). Digital economy: India's account aggregator system is plagued by privacy and safety issues. *Economic Political Weekly,* 55(22). https://www.epw.in/engage/article/digital-economy-indias-account-aggregator-system

Jolls, Christine & Sunstein, Cass R. (2005). *Debiasing through law* (Working Paper No. 11738). National Bureau of Economics Research. http://www.nber.org/papers/w11738

Justice K.S. Puttaswamy (Retd.) and Ors vs. Union of India & Ors 2017 (10) SCC 1

Justice K.S. Puttaswamy (Retd.) and Ors vs. Union of India & Ors 2019 (1) SCC 1

Kahneman, Daniel, Knetsch, Jack L., & Thaler, Richard H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic Perspectives, 5*(1), 193-206. DOI: 10.1257/jep.5.1.193

Kaye, Jane, Whitley, Edgar A., Lund, David, Morrison, Michael, Teare, Harriet, & Melham, Karen (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics,* 23, 141–146. DOI: 10.1038/ejhg.2014.71

Khera, Reetika (2017, December 14). Impact of Aadhaar on welfare programmes. *Economic Political Weekly,* 52(50), 61–70. https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html

Kohli, Renu (2018, May 19). Women and banking: India's financial inclusion suffers from a gender gap. *Financial Express.* https://www.financialexpress.com/opinion/women-banking-indias-financial-inclusion-suffers-from-a-gender-gap/1173467/

Kovacs, Anja (2017, February). *"Chupke, chupke": Going behind the mobile phone bans in North India.* Gendering Surveillance, Internet Democracy Project. https://genderingsurveillance.internetdemocracy.in/phone_ban/

Kovacs, Anja & Jain, Tripti (2020, November). *Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data* (Working Paper No. 13). Data Governance Network. https://datagovernance.org/files/research/1606371436.pdf

KPMG & Google (2017, April). *Indian languages: Defining India's Internet*. KPMG in India & Google. https://assets.kpmg/content/dam/kpmg/in/pdf/2017/04/Indian-languages-Defining-Indias-Internet.pdf

Lacey, Nicola (1998). *Unspeakable subjects: Feminist essays in legal and social theory*. Hart Publishing.

Lakshmanan, Srikanth (2018, November 19). Exclusive: RBI issues in-principle licenses to 5 account aggregators. *Medianama.* https://www.medianama.com/2018/11/223-exclusive-rbi-issues-in-principle-licenses-to-5-account-aggregators/

Mahesh, B.G. (2020, March 27). What is an Informed Consent & Consent Artefact? *Sahamati.* https://sahamati.org.in/blog/what-is-an-informed-consent-consent-artefact/

Malhotra, Nipun (2020, May 25). Disabled Indians can't be afterthought in Covid. Disability secys needed in all ministries. *The Print.* https://theprint.in/opinion/indias-disabled-cant-be-afterthought-in-covid-crisis/428162/

Mathur, Nandita (2020, May 5). India now has over 500 million active Internet users: IAMAI. *LiveMint.* https://www.livemint.com/news/india/india-now-has-over-500-million-active-internet-users-iamai-11588679804774.html

Matthan, Rahul (2017, July 19). *Beyond consent: A new paradigm for data protection* (Discussion Document 2017-03). The Takshashila Institution. http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

Mehra, Preeti (2018). Outcasts in a digital world. *The Hindu BusinessLine.* https://www.thehindubusinessline.com/opinion/columns/from-the-viewsroom/outcasts-in-a-digital-world/article9709231.ece

MeitY (2018). *Electronic Consent Framework. Technology specifications version 1.1.* https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Ministry of Health (2019). *National Digital Health Blueprint*. https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf

MoneyControl News (2020, October 26). Ookla speedtest: Pakistan and Nepal have faster internet speeds; India among the lowest. *MoneyControl.* https://www.moneycontrol.com/news/technology/ookla-speedtest-global-index-india-ranked-131-out-of-138-countries-in-mobile-internet-speeds-6015041.html

NABARD (2018, August). *NABARD All India rural financial inclusion survey 2016-17*. National Bank for Agriculture and Rural Development (NABARD). https://www.nabard.org/auth/writereaddata/tender/1608180417NABARD-Repo-16_Web_P.pdf

National e-Governance Services Limited (2018). *Request for proposal for selection of vendor for design, development, installation, integration, configuration, support and maintenance of account aggregation software.* NESL Asset Data Limited. https://www.nesl.co.in/wp-content/uploads/2018/06/NADL_RFP_26062018-update.pdf

Nedelsky, Jennifer (1989). Reconceiving autonomy: Sources, thoughts and possibilities. *Yale Journal of Law and Feminism,* 1(1), 7-36. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1004&context=yjlf

Christopher, Nilesh (2020, November 13). As WhatsApp Pay enters India, local fintech companies aren't happy. *Rest of World.* https://restofworld.org/2020/whatsapp-pay-enters-india/

NITI Aayog (2020). *Data Empowerment and Protection Architecture, Draft document for discussion.* https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf

NITI Aayog (2018, July). *National Health Stack strategy and approach.* https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf

Norton, T.B. (2016). The non-contractual nature of privacy policies and a new critique of the notice and choice privacy protection model. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 27, 181-210. https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5

Pineau, Lois (1989). Date rape: A feminist analysis. *Law and Philosophy,* 8(2), 217-243. DOI: 10.2307/3504696

Product Nation/iSPIRT (2017, August 22). *Data Empowerment & Protection Architecture (DEPA)*. Slideshare. https://www.slideshare.net/ProductNation/data-empowerment-protection-architecture-depa

PTI (2019, February 8). High Court to examine the issue of banks sharing customers' PAN data with credit rating agencies. *Economic Times.* https://economictimes.indiatimes.com/industry/banking/finance/banking/high-court-to-examine-issue-of-banks-sharing-customers-pan-data-with-credit-rating-agencies/articleshow/67903734.cms

PTI (2020, June 12). Forget English, go vernacular: NITI Aayog CEO to fintech firms. *Financial Express.* https://www.financialexpress.com/industry/sme/forget-english-go-vernacular-niti-aayog-ceo-to-fintech-firms/1989866/

Raghavan, Malavika (2019, November 29). Why more smartphones and bank accounts haven't brought financial digital inclusion in India. *The Print.* https://theprint.in/opinion/why-more-smartphones-and-bank-accounts-havent-brought-financial-digital-inclusion-in-india/327919

Raghavan, Malavika & Singh, Anubhutie (2020, November 16-18). *Regulation of information flows as Central Bank functions: Implications from the treatment of account aggregators by the Reserve Bank of India*. [Conference Paper] 2020 Central Bank of the Future Conference, co-hosted by University of Michigan's Centre on Finance, Law & Policy and the Federal Reserve Bank of San Francisco. https://www.dvara.com/blog/2020/11/18/regulation-of-information-flows-as-central-bank-functions-implications-from-the-treatment-of-account-aggregators-by-the-reserve-bank-of-india/

Rathee, Kiran (2021, January 20). Withdraw new policy, Centre tells WhatsApp. *The Financial Express.* https://www.financialexpress.com/industry/technology/data-privacy-withdraw-new-policy-centre-tells-whatsapp/2174489/

Ravi, Shamika (2019, March 5). Accelerating financial inclusion in India. *Brookings Institution India.* https://www.brookings.edu/research/accelerating-financial-inclusion-in-india/

Reserve Bank of India (2015, July 2). RBI Central Board meets at Chennai: RBI to allow account aggregator NBFCs; to set up Financial Inclusion Advisory Committee [Press release]. *Reserve Bank of India.* https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=34345

Sahamati (2019a). Frequently asked questions. *Sahamati.* Retrieved April 13, 2021, from https://sahamati.org.in/faq

Sahamati (2019b, July 23). Sahamati: Collective of the account aggregator ecosystem. *Sahamati.* Retrieved April 13, 2021, from https://sahamati.org.in/

Sahamati (2020a). Account aggregators in India. *Sahamati.* Retrieved April 13, 2021, from https://sahamati.org.in/account-aggregators-in-india/

Sahamati (2020b). FIPs and FIUs in the account aggregator ecosystem. *Sahamati.* Retrieved April 13, 2021, from https://sahamati.org.in/fips-and-fius-in-the-account-aggregator-ecosystem/

Singh, Sudhir (2018). Policy hacks session on GDPR & DEPA. *Ispirt Productnation*. https://pn.ispirt.in/policy-hacks-session-on-gdpr-depa/

Sircar, Sushovan (2020, September 9). NITI Aayog's new "India model" for personal data sharing explained. *The Quint*. https://www.thequint.com/tech-and-auto/depa-data-empowerment-and-protection-architecture-niti-aayog-personal-data-sharing

Solove, Daniel. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880-1903. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Strahilevitz, Lior J. (2013). Toward a positive theory of privacy law. *Harvard Law Review, 126*(7), 2010-2042. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_strahilevitz.pdf

TRAI (2017, August 9). *Consultation paper on privacy, security and ownership of the data in the telecom sector.* TRAI. https://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

TRAI (2018). *Recommendations on privacy, security and ownership of the data in the telecom sector*. TRAI https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

Uppal, Mahesh (2020, June 10). Keeping India's payments market competitive. *Financial Express.* https://www.financialexpress.com/opinion/keeping-indias-payments-market-competitive/1986606/

Yanhao, Wei, Yildirim, Pinar, Van den Bulte, Christoper & Dellarocas, Chrysanthos (2015). Credit scoring with social network data. *Marketing Science*, 35(2): 234-258. DOI: 10.1287/mksc.2015.0949

Zuboff, Shoshana (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile Books.

Acknowledgements

My journey has been a long one, made possible only with the help of dozens of friends and colleagues along the way who have exhorted me to keep my eyes on the prize. At the very top of what will be a truly prodigious list, pride of place goes to my interviewees, who have shared their valuable inputs, expertise and time with me and this research. I am also grateful to Anja Kovacs, my mentor and guide: you have guided my progress with a keen eye for detail and style, never fearing to puncture an idea that merely sounded good, and reminding me of the larger picture at every turn.

About the Authors

Currently, Tripti Jain is a Senior Associate, Public Policy at the technology policy vertical at Chase India. She works towards developing policy advocacy and communication strategy to build credibility and thought leadership for tech and fintech companies. All her research under the theme 'data as bodies', including this paper, was conducted while she was a researcher at the Internet Democracy Project. Her responsibilities at IDP included planning, conducting, and presenting research. Prior to joining the Internet Democracy Project, Tripti was a counsel at Sflc.in. She was managing their Internet Shutdowns project and was involved in various projects that included research and advocacy on issues such as privacy, and civil rights on the Internet. Tripti is a lawyer by education.

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork