Economic&PoliticalWEEKLY

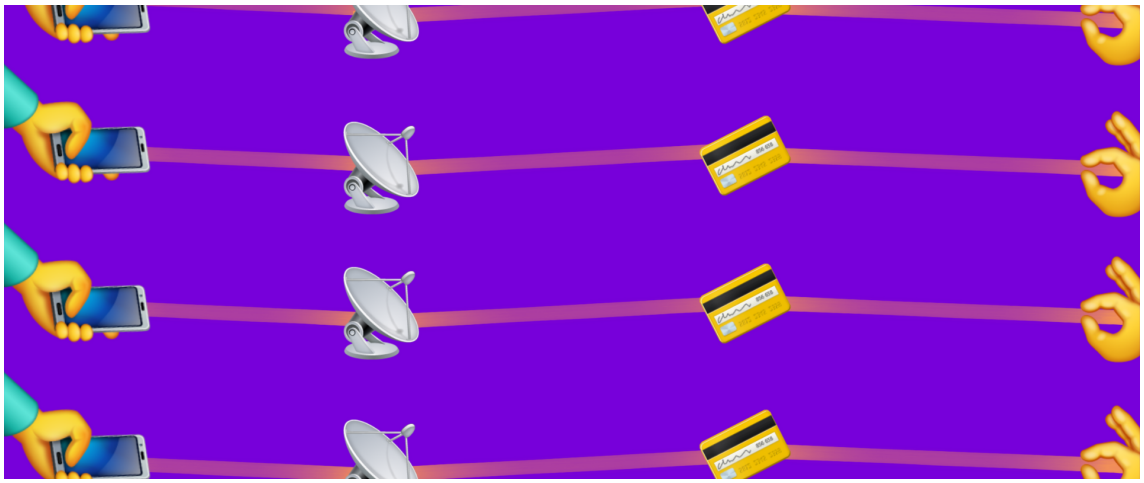
ISSN (Online) - 2349-8846

Digital Economy: India's Account Aggregator System Is Plagued by Privacy and Safety Issues

ROHAN JAHAGIRDAR
PRANEETH BODDULURI

Rohan Jahagirdar (rohan@baseaccount.com) and Praneeth Bodduluri (praneeth@baseaccount.com) run Base Financial Technology Consultancy based in Bengaluru.

Vol. 55, Issue No. 22, 30 May, 2020



In the digital economy, data inequity adversely affects consumers in the financial sector, especially the ones limited by choices due to their geographic location and/or socioeconomic status. To tide over these problems, India introduced the account aggregator system in 2016, enabling financial institutions to access information of individuals in exchange for offering financial instruments. Despite the novelty and benefits that come with it, there have been issues surrounding privacy and safety of individual's financial information.

This is part of a six-article series on questions surrounding data, privacy, artificial intelligence, among others. You can read the introduction here

As online users become increasingly comfortable with the idea of sharing their data in

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

exchange for financial services and benefits, financial institutions have been exploring different ways to make the process of collecting, verifying, and processing financial data of individuals streamlined. Financial companies today use a variety of ways, including the scraping of online accounts, manual uploading of statements, partnerships with banks, and directly connecting to the payroll software of the employers, to collect the financial data of individuals. However, these methods are cumbersome, and often proved incomplete in terms of data collection. Moreover, it has become increasingly difficult to verify the veracity of the financial documents of an individual.

Against this backdrop, the Non-banking Financial Company–Account Aggregator (NBFC–AA) Framework was introduced in 2016 by the Reserve Bank of India (RBI). An account aggregator is a financial entity, which obtains and consolidates all the financial data of an individual, and presents the same in a manner that allows the reader to easily understand and analyse the different financial holdings of a person. An individual's financial holdings could be scattered across various financial instruments with different financial intermediaries, and they may even come under the purview of various financial regulators.

For example, an individual may have fixed deposits with the Housing Development Finance Corporation (HDFC) Bank that comes under the purview of RBI; mutual fund investments with Nippon Asset Management Company that comes under the ambit of Securities and Exchange Board of India (SEBI); and life insurance cover with Life Insurance Corporation of India (LIC) under the Insurance Regulatory and Development Authority of India (IRDAI). Gathering all the scattered data from each of these investments and consolidating the same for the submission to a financial institution when applying for a loan could prove to be a time-consuming and rather a confusing task for an individual.

In this article, we examine some of the trade-offs that result from the architectural choices made by the institutions responsible for setting up and operating account aggregators. While the current framework is sound in principle, we find that it may, in its current form, delegitimise the agency of the user. It could result in users getting profiled and leaving them vulnerable to privacy-related risks.

Globally, other countries have implemented similar schemes to enable the sharing of bank account information through a new class of institutions. The account information service provider (AISP) system set up by the authorities in the United Kingdom (UK) is one such example. However, these AISPs only provide piece-meal information and none matches to the scale envisioned by the NBFC–AA, which makes it necessary for us to carefully examine the tenets of its programme.

It is not hard to see why the recently announced account aggregators' project has caught the imagination of entrepreneurs, policymakers, and the media in India (Baruah 2019; Rai 2020). In today's digital economy, data inequity adversely affects consumers in the financial sector, especially the ones that are limited by the choices due to their geographic location

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

or socioeconomic status. Upending the relationship that people have with their existing financial institutions is hard because the incumbents often use the historical data about their users, developed over the years, as an effective tool to persist a lock-in. As a result, newer players are squeezed out, even if their products are better than the ones offered by the legacy companies. Additionally, there is no standardised method for individuals to give consent to the companies to process their data, and sell them financial products securely.

Certainly, the problems that account aggregators aim to resolve are real. The need for a system that enables individuals to share their financial information securely, through meaningful consent, in exchange for delivery of financial products is palpable. With the RBI announcement of master directions and the Reserve Bank Information Technology Private Limited's (ReBIT) technical architecture for the account aggregator ecosystem recently this system could very well become the de facto method to use or purchase a range of financial services, including mutual funds, insurance, credit products, among others (RBI 2016; ReBIT 2019).

As regards the digital delivery of financial services is concerned, the account aggregator system has the potential to act both as the midwife and the executioner at the same time. It has never been easier to access data of a large number of individuals at such low costs, but these individuals have never been subject to a more comprehensive profiling programme either, which can reconcile multiple data sets from across the board.

There is a need to ask if the architectural foundations on which the account aggregators operate match up to the requirements of a programme that is likely to touch the lives of all citizens of India. Can we, as participants of this programme, be satisfied with the checks and balances that have been put in place to monitor the functioning of the account aggregator system?

The Personal Data Protection (PDP) Bill, 2019 provides a lens to understand how data privacy and security can be applicable to the users of NBFC–AA system.

Upending User Agency

When an individual buys a financial product, the seller requires the buyer to provide certain specific information about themselves that will allow the seller to price the risk of the transaction appropriately. Traditionally, before the advent of Aadhar's e-KYC (know your customer), this information was provided by the buyers or users directly to the seller (or provider, or affiliate appointed by the provider). The veracity of the documents provided was also attested to by the users themselves. Providing a fake bank account statement, for example, to avail a loan constituted a fraud. However, such a transaction in the past did not necessitate the presence of a third party to mediate or verify it. In other words, this traditional method of transaction did not upend the agency of the user.

A salient feature of the account aggregator architecture is that the users delegate the

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

sharing of their financial information to a third party (account aggregator).

The third party then takes the role of the first by securing the information from a financial provider, and then temporarily stores financial information before providing it to the entity that has requested it. The user is provided with bare details concerning consent mechanism that is likely to be miscomprehended, and enables the entire process.

The choice of such an architecture is reflective of the underlying thought process that places the account aggregator ecosystem's needs above that of the users. The fact that the user has no means to offer verified data directly to the third party financial institutions in lieu of a service or product, without the involvement of a third party, is reminiscent of the architecture that Aadhaar provided until the offline KYC process was introduced in 2018 after a long legal battle and public anger (Khera 2019).

Using the account aggregator ecosystem forces the individuals to only act through an intermediary. This invites onto itself multiple possibilities of errors, of both false positive and false negative kind at different touchpoints.

Technical glitches at account aggregator's end could cause erroneous responses, which could end up blocking the access of deserving individuals to financial products. While the technical standards do talk about security checks to prevent such events from happening, it is not hard to imagine such accidents as evidenced in the case of Aadhaar or United Payments Interface (UPI) set up (Alam 2018).

Although it could be said that individuals would have the choice of using a different system to share their data, it is highly likely that the account aggregator ecosystem will end up exerting a forceful network lock-in, which could make it much harder for individuals to employ alternatives to share their financial information securely.

The Architecture of Account Aggregator System

The account aggregator architecture, as proposed, creates a number of trade-offs that could delegitmise the privacy of the users, and also place the system itself at risk.

Issue of data ethics: The account aggregator system can be used as a large-scale mechanism for data mining by financial information providers (FIPs) and financial information users (FIUs). Suppose a food delivery app, like Zomato, starts offering you an option to purchase on credit. In order to enroll into such a programme, for instance, you are required to share your income and account statement to verify your credit worthiness. Sharing this information through an account aggregator would mean that Zomato can use your previous spending history and offer food at a differential price, or use that information for its targeted advertising. For instance, knowing that you often go to Italian restaurants, the company can specifically target you for advertisements from Italian restaurants even if you have not ordered Italian food using the application before.

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

While NBFC–AA technical specifications and PDP bill do have provisions on purpose limitation and the limitations on data collections and storage, there is nothing that can prevent an FIU (in this case, Zomato) from overreaching and taking a wider variety of permissions.

The UK's Financial Conduct Authority, which has been tasked with regulating open finance for the UK market in its "Call for Input on Open Finances," specifically highlights the issue of data ethics arising out of the interconnected systems. The use of machine learning, artificial intelligence, and the risk of perpetuating existing biases and prejudices present additional potential risks emanating out of open finances (FCA 2019).

Nothing in the account aggregator programme or the proposed PDP bill explicitly prevents FIUs of any kind from combining their existing data sets with financial information to profile their customers. This makes the account aggregator system conducive for data mining and ethical issues arising therein.

In fact, the specifications, currently, do not enforce any standards on how an FIU, after acquiring the financial information from an account aggregator, would be required to store and manage data (Raghavan and Singh 2018).

Possibility of abuse and data mining: The guidelines set forth by RBI's master directions disallow the account aggregator to permanently store the data that has been fetched and stored by it, in receipt of the user's consent. The account aggregator is required to stipulate a time frame within which the FIU must take the information from the transient store of the aggregator. The information may be stored with the account aggregator for a maximum of 72 hours. However, the technology guidelines fall short of mentioning a method to enforce the transience of the storage (NeSL 2018).

Problems with the Consent Collection

The master directions of RBI mandate FIPs to share financial information of a customer with an account aggregator when the latter presents a valid consent artefact. Further, it is required that FIPs verify the consent artefact before the requested information is shared with the account aggregator (ReBIT 2019).

However, the technical specifications, as proposed by ReBIT, provide no method as to how the consent artefact could be manifested, in terms of the actual interface design to the users. This is particularly worrying since it has been demonstrated multiple times that individuals consenting to the terms online often have a poor understanding of what they are consenting to (Bailey et al 2018).

If we are to solely rely on the consent collection specifications provided under Electronic Consent Framework, v1.1, published by the Ministry of Electronics and Information Technology (MeitY), it could turn out to be worrying. The specifications suggest that a

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

consent collector can possibly obtain the consent by merely "having the user click a button or by signing a paper form" (MeitY nd).

Furthermore, a number of ancillary problems related to consent collection have been identified by researchers in this process:

Consent friction and fatigue: We think that simple disclosure policies would not be enough for individuals to make a meaningful decision. Consent forms or pop-ups in most cases are likely to be ignored by users because it adds a layer of friction to the otherwise seamless browsing experience. The internet as a medium is known to favour interfaces that decrease friction, irrespective of the intention. This layer of friction coupled with consent fatigue could lead to a devaluation of consent, where the users just agree to whatever terms of service, and provide their consent without really bothering to read the details of what they are consenting to (Matthan 2017).

Misinterpretation of terms and policies: Most users find the consent mechanism useless when it comes to actually protecting their privacy. In fact, very often, not only do individuals fail to understand the fine print of privacy policies, we see that individuals often misunderstand the policies as guarantees of data protection, instead of liability disclaimers for firms, a phenomenon referred to as "privacy paradox" (Blank et al 2014).

Making consent the condition of service: Overt reliance on a consent-based architecture implies that businesses are likely to resort to a "take it or leave it" approach, wherein the user is presented with the only alternative of not using the service at all unless they consent to its data processing rules. This indiscriminate usage of consent mechanism presents the individual with a false choice and only the illusion of control (Raghavan and Singh 2020).

Lack of feature phone support: Another concern that has been highlighted by researchers is that the consent architecture adopted by the account aggregator system may not address the needs of the feature phone users in India who may not have access to a reasonably good internet connection and electricity (Raghavan and Singh 2020).

We acknowledge that the NBFC–AA system considers informed consent as the cornerstone of the system. FIUs are required to obtain the consent of the individuals to lawfully collect, use, and disclose personal information in the course of activity.

Additionally, the proposed PDP bill lays down the guidelines for a data collection notice. However, the nature of technology and business models that call into question the feasibility of obtaining meaningful consent are concerning. We foresee that there will be several complexities in the effective translation of the principles, originally envisaged by the PDP bill, into practice. But these challenges should not be seen as a ground for abandoning or diluting the requirements of consent.

With the increasing penetration of the internet in the country, user profiles are increasingly

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

shifting towards young women and people from the rural areas. These groups are particularly marginalised, and are vulnerable to malicious attacks and social engineering online. Thus, addressing matters related to consent and notices become important (Kulkarni et al nd).

In these cases, it may be wise to consider adding a layer of friction at the time of consent collection to ensure the user's comprehension of the notice. This could be implemented as a "layered notice mechanism," wherein the ease of usage is balanced with the gravity of the transaction being undertaken (Parsheera et al 2018). Additionally, users from the marginalised sections may not be able to comprehend notices and consent forms in English, and it is essential that the account aggregators explore visual media, like standardised icons, to convey the notice, and the consequences of the consent.

In light of these circumstances, we recommend that a data protection authority (DPA) takes a proactive approach in setting up clear boundaries for consent and notice mechanisms from time to time.

Account Aggregator System and the Data Protection Bill

The consent architecture as defined by MeitY paper when seen in conjunction with the newly proposed data protection bill offers the possibility of some additional worrying scenarios that could play out:

Issue with credit scoring and debt collection: The draft PDP bill places "credit scoring" activities under a list of exceptions to consent collection for data processing (Outlook 2017). If interpreted narrowly, based purely on what the PDP draft says, this exemption would be a major aberration to the rights of the users using different financial applications.

One of the, if not the most important, applications of the account aggregator system is to provide individuals a safe and a secured method to share their financial information, drawn from different financial providers, towards calculation of credit scores. With that consent, digital applications could start enticing users with credit products even when they have not necessarily asked for it, but because the customer has a good credit score. This could possibly work the other way around as well, wherein, digital applications could offer customers with lower credit scores a more diminished experience.

A free pass to debt collection without any consent could possibly also mean lenders can call friends and relatives of users who have taken loans by looking up their contacts list. Despite regulations, lenders have previously engaged in such activities to coerce users to become part of debt-collection mechanism (Outlook 2017).

Issue with mergers and acquisitions: According to the PDP draft bill, a user's consent may not be required by the data fiduciary at the time of mergers (GoI 2019a). Read

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

narrowly, this could represent a grave risk to the data of the users who consented originally only to the company before a merger or acquisition event.

This choice of exemption by the PDP bill seems to be at odds with the practices adopted by other identity management systems, like I Reveal My Attributes (IRMA), set up by Privacy by Design Foundation (Privacy by Design Foundation nd). IRMA's protocols are designed so as to ensure that even if an issuer of identity attributes were to collaborate with the verifier, the blindness of the system would ensure that the user and their actions are not traced.

Contrasting this with the statutes of the PDP bill makes it seem that an act of merger or acquisition could possibly serve as a legitimate business strategy for a company looking to usurp the consents collected by a target company.

Revoking consent: The ReBIT specifications provide means for the revocation of consent provided by the users. As suggested, individuals can revoke their consent either directly on the account aggregator's application, or through the FIP, who will then inform the account aggregator about the revocation (ReBIT 2019). The account aggregator is required to communicate to the FIU about the revocation of the consent upon the receipt of the request either from the user or the FIP.

However, the specifications offer no guidelines on how the FIU would handle the data post revocation of the consent. It is not clear if this would necessitate the individual to separately reach out to the FIU to request the data erasure, and if the FIU is bound by any laws to comply with the user's request.

On the issue of "Right of Erasure and Correction," the PDP bill requires the data fiduciary collecting the erasure request to "take the necessary steps to notify all the relevant entities or individuals to whom such personal data may have been disclosed…"(GoI 2019b). True to its word, the account aggregator programme's specifications only mention that the FIU would be informed, however, one can only speculate as to how an FIU would actually use this data after having been communicated about the erasure.

Right to Information on Data Breach

The PDP bill requires that data fiduciaries should inform the data protection authority about the breach of any personal data processed by them, and where such breach is likely to cause the data principal (the user, consumer) any harm (GoI 2019c).

However, the bill leaves it entirely to the data protection authority to determine whether the information regarding the breach should be reported to the principal. This is a clear digression from the notion that the notification about data breaches should be considered as a "right" of the data principals, an idea that has been increasingly gaining ground since the European Commission introduced this in 2015 (Whittaker nd). This gives data subjects the right to know when their data has been hacked, through notification by the data controller

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

to the user or the national supervisory authority. This allows data subjects to take immediate action to limit the damage, and also to prevent data controllers to hide their mistakes.

This is a particularly important concern since financial institutions, including banks and payment systems, are known to be hacked on numerous occasions, and the users' personal data is compromised or placed under the risk of compromise (Bhandari and Sane 2016).

The account aggregators are designed to carry very sensitive data about their users, and are likely to be targeted by external hackers. We recommend that data protection authority makes it mandatory for all the players in the account aggregator ecosystem to give notice to users when an attack has been learnt of.

Structural Challenges

In addition to the above comments, we foresee some important challenges arising due to the structural set up of the account aggregator system. These emanate either directly from the architectural choices or due to other externalities that may adversely impact the running of the account aggregator programme.

Overuse of customer data: As it has been observed numerous times in developing economies across the world, when the authorities subsidise the cost of public resources, like water, the supply of the water goes up, but it also decreases the social value, and so people end up consuming more water, and the demand increases. The social cost of this subsidy shows up in what economists call "deadweight loss," a reflection of increased consumption at lower social value driven by artificial costs (Tabarrok and Cowen 2017).

Although data, unlike water, is not necessarily a limited resource, it would be wise to inculcate a similar mindset when dealing with the financial information of the users. We worry that the availability of the infrastructure could encourage the FIUs to abuse the system in drawing up as much data about the user as possible. Decreasing the costs of accessing users' data and its consequent availability in plenitude would decrease its value. While such an approach may help the FIUs or account aggregators, it will come at an extraordinary cost to the individuals, and the society as a whole.

It would be wise for the account aggregator system to structurally incentivise FIUs, which require fewer data points over the ones that need more. For example, a lender, using the account aggregator system, which requests for a fewer data points to decide the credit worthiness of an applicant should be encouraged over one that asks for multiple data sets. Relying exclusively on users to make this decision for themselves may not really work, especially since users would not be able to appropriately price their own privacy.

Interoperability concerns: There could be many reasons why FIPs may not share, or make it difficult to share consumer data with other firms. The primary reason for this is

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

commercial. Sharing data could possibly disrupt the business models or market share of a data-rich incumbent. The firms may wish to avoid the setting up and maintenance costs of sharing the data, or may be dissuaded by the return of investment (ROI) from sharing the financial information of the users.

Interoperability problems among financial institutions were noticed during the initial days of UPI set-up when a major bank had blocked transactions from one of the UPI apps (Variyar 2017). Such a situation could very well play out again with the account aggregator ecosystem.

Organisational structure of the account aggregator: The master directions of the RBI stipulate a number of organisational requirements for a company that wishes to apply for an account aggregator license. However, the rules do not preclude companies that are already operating in the consumer finance space from applying for an account aggregator license. There are two possible threats that we see emanate out of this.

The first is that the account aggregator with a parent company, which offers a service or a product that directly competes with the one offered by an FIU, makes it difficult for the FIU to obtain customer's data. This is the interoperability concern which we have expressed above. The second threat is that the account aggregator, upon learning that the user is interested in an external entity's offering that competes directly with its own, could proffer or incentivise the customer with targeted messaging to switch from the external FIU to the account aggregator parent company.

Take, for example, the case of Jio, a wholly-owned telecom subsidiary of the Reliance Industries. Jio operates the country's largest phone network, has a payment banking license, has a license to issue payment cards, and has also applied for a license to operate as an account aggregator and has received the approval (Pathak and Borate 2020). Jio could possibly use the account aggregator license in addition to its existing muscle to build a walled garden around its customers, exerting a strong lock-in that could make it very hard for the customers to exercise their choices freely.

Disproportionate Penalties

Given the criticality of the data handled by account aggregators, it is essential that the security of the system be considered seriously. The proposed PDP bill takes an iron-fist approach by prescribing stringent punishments and the imprisonment for acts that have been defined very vaguely (GoI 2019d).

The bill seeks to penalise a person who "knowingly or intentionally" re-identifies personal data which has been de-identified previously. Furthermore, with regards to the offences committed by the companies, the bill seeks to hold "every person connected with the offence, including the person in charge, was responsible to, the company for the conduct of the business of the company, and the company itself" guilty (Pathak and Borate 2020).

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

The offences under the act are cognisable and non-bailable. As it has been noted by the researchers, the criminal charges to be slapped through data protection laws in India are severe and disproportionate to the magnitude of the offences. When compared to such laws and penalties across the globe, India's penalties are disproportionate. We believe that this approach will create twin effects. The first is that the high costs of security breaches and the lack of clear definition on how the rules will be interpreted by the data protection authority will act as a high entry barrier for new account aggregators to enter the market. This would mean a diminished number of choices for the users and ultimately resulting in a poor experience.

Second, the laws that criminalise ethical hacking and other forms of security would make it very hard for different players to maintain systems up to date with the latest security standards. This would mean that the players in the account aggregator ecosystem could adopt the approach of securing systems through a patchwork of laws and fines, instead of relying on technological solutions to enforce the guidelines.

The Road Ahead

Today, India faces multiple financial problems—poor price discovery mechanisms, lack of choices in terms of financial instruments, especially for the marginalised, network lock-ins—for which the account aggregator system could offer a solution.

In fact, the only thing nearly as scary as building the account aggregator system is the prospect of not having any standardised data sharing mechanism. Nevertheless, those who are into the account aggregator ecosystem will have the responsibility to anticipate dangers stemming from it. With account aggregators coming onto the scene, the most powerful methods (such as, a single click-based financial data sharing) are precisely those that entail the major risk to its users.

The lack of availability of a structured data sharing system also implies that setting up a new system for the same can be seen as a step in the positive direction. However, with numerous problems associated with the system, as highlighted above, especially when read in conjunction with the PDP bill, concerns remain of the possible negative impact of the account aggregator system to the rights and freedoms of its users.

What is disconcerting is the playing out of a scenario where the account aggregator links would end up like the railway lines under the British rule in India. No doubt that the railway lines commissioned by the British imperial power had a monumental impact in developing the consciousness of the people of India during the freedom struggle. The railways had played a significant role in connecting people from different regions from across the country. However, the enterprise was not really set up to benefit the people of India. Any benefits accrued in that regard were only incidental, and the primary beneficiaries of the enterprise were the British empire, which effectively used railways to plunder the wealth of India. We hope that account aggregators would not become modern India's British

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

railways.

References:

- Alam, Tausif (2018): "Growth Comes with Glitches: It's Not Easy to Recover Money Lost in UPI Transfer," *ENTRACKR*, 11 March, https://entrackr.com/2018/03/upi-transaction-failure/.
- Baruah, Ayushman (2019): "Rapid Adoption of Account Aggregators can Make India Leader in Digital Economy: Nandan Nilekani," *Livemint*, 4 December, https://www.livemint.com/companies/news/-rapid-adoption-of-account-aggre....
- Bailey, Rishab, Smriti Parsheera, Faiza Rahman and Renuka Sane (2018): "Disclosures in Privacy Policies: Does "Notice and Consent" Work?" *National Institute of Public Finance and Policy*, https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf.
- Bhandari, Vrinda and Renuka Sane (2016): "Towards a Privacy Framework for India in the Age of the Internet," https://macrofinance.nipfp.org.in/PDF/BhandariSane2016_privacy.pdf.
- Blank, Grant, Gillian Bolsover and Elizabeth Dubois (2014): "A New Privacy Paradox: Young People and Privacy on Social Network Sites," *Global Cyber Security Capacity Centre*, https://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%....
- GoI (2019a): "Section 14(2), The Personal Data Protection Bill, 2019," Government of India.
- Privacy by Design Foundation (nd): "About IRMA," https://privacybydesign.foundation/irma-en/.
- —(2019b): "Section 18(1), The Personal Data Protection Bill, 2019," Government of India.
- —(2019c): "Section 25(1), The Personal Data Protection Bill, 2019," Government of India.
- —(2019d): "Section 84(1), The Personal Data Protection Bill, 2019," Government of India.
- Bailey, Rishab, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman (2018): "Response to the Draft Personal Data Protection Bill, 2018," *The Leap Blog*, 20 October, https://blog.theleapjournal.org/2018/10/response-to-draft-personal-data....
- FCA (2019): "Call for Input: Open Finance," *Financial Conduct Authority*, 17 December, https://www.fca.org.uk/publications/calls-input/call-input-open-finance.
- Khera, Reetika (2019): *Dissent on Aadhaar: Big Data Meets Big Brother*, Hyderabad: Orient BlackSwan.
- Kulkarni, Amol, Sidharth Narayan and Swati Punia (nd): "'Users' Perspectives On Privacy and Data Protection," *CUTS International*, https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf.
- MeitY (nd): "Electronic Consent Framework Technology Specifications—Version 1.1,"

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

Ministry of Electronics and Information Technology, http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%2....

- Matthan, Rahul (2017): "Beyond Consent: A New Paradigm for Data Protection," *The Takshashila Institution*, http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-....
- NeSL (2018): "Request for Proposal for Selection of Vendor for Design, Development, Installation, Integration, Configuration, Support and Maintenance of Account Aggregation Software," *National e-Governance Services Limited*, https://www.nesl.co.in/wp-content/uploads/2018/06/NADL_RFP_26062018-upda....
- Pathak, Kalpana, Neil Borate (2020): "Jio May Diversify into Mutual Funds, Other Financial Products," *LiveMint*, https://www.livemint.com/companies/news/jio-may-diversify-into-mutual-fu....
- Parsheera, Smriti, Faiza Rahman, Renuka Sane, Amba Kak and Vrinda Bhandari (2018): "Response to the White Paper on a Data Protection Framework for India," https://macrofinance.nipfp.org.in/PDF/BKPRS2018WhitePaperResponse.pdf.
- Rai, Saritha (2020): "India's About to Hand People Data Americans Can Only Dream of," *Bloomberg*, 13 January, https://www.bloomberg.com/news/articles/2020-01-13/india-s-about-to-hand....
- RBI (2016): "Master Direction: Non-Banking Financial Company–Account Aggregator (Reserve Bank) Directions," *Reserve Bank of India*, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.
- ReBIT (2019): "NBFC–Account Aggregator: API Specifications," *Reserve Bank Information Technology Private Limited*, 8 November, https://specifications.rebit.org.in/NBFC-AA%20API%20Specification_Core_F....
- Raghavan, Malavika and Anubhtie Singh (2020): "Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector," 7 January, https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infras....
- *Outlook* (2017): "RBI Asks NBFCs Not to Use Coercion during Loan Recovery," 9 November, https://www.outlookindia.com/newsscroll/rbi-asks-nbfcs-not-to-use-coerci....
- Tabarrok, Alex and Tyler Cowen (2007): *Modern Principles of Economics*, New York: Macmillan Learning.
- Variyar, Mugdha (2017): "ICICI Bank Resumes UPI Transactions on PhonePe," *Economic Times*, 1 February, https://economictimes.indiatimes.com/small-biz/startups/icici-bank-resum....
- Whittaker, Zack (nd): "India's Largest Bank SBI Leaked Account Data on Millions of Customers," *TechCrunch*, https://techcrunch.com/2019/01/30/state-bank-india-data-leak/.

Economic&PoliticalWEEKLY

ISSN (Online) - 2349-8846

EPW engage