DVARA Research

4th Dvara Research Conference

Regulating Data-Driven Finance

April 5-6, 2019

Primer on Consumer Data Regulation

Anubhutie Singh, Malavika Raghavan & Beni Chugh

This primer presents an overview of the landscape, emerging concerns and some considerations for regulators in relation to consumer data regulation in India. A reference list of background reading materials is available on page 7.

This primer has been prepared for participants at the 4th Dvara Research Conference.

Overview

The use of personal data by government and private service providers in interactions with individuals is becoming ubiquitous in India. These advances can greatly improve efficiency and reduce costs when delivering services to harder-to-reach users. However, the pervasive nature of data processing has raised concerns regarding privacy, exclusion due to digital service failure and related harms. These issues have special relevance for finance, given the increasing digitisation of the sector and the growing use of non-financial information to support the delivery of financial services.

Without a robust framework to govern the regulation of consumer data, consumers and providers are exposed to significant risks and uncertainty. There has been significant policy movement in the past two years in reaction to some of these concerns, culminating in the release of a draft Personal Data Protection Bill that awaits introduction in the Indian Parliament. Within the financial sector, regulatory bodies have flagged relevant issues in the final report of the Inter-Regulatory Working Group on FinTech and Digital Banking, including those relating to consumer data protection, organisational data, shared utilities, big data analytics, data security and fraud prevention.

In this background, some pertinent concerns arise with respect to the regulation and use of consumer data in finance. Regulators and providers need to address the need to build trust for consumers on digital platforms given fears of fraud or financial loss. Providers have access to vast personal databases. In the absence of robust data protection regulations, provider considerations on the processing of data and the potential of system failures are crucial. Cost-efficient digital financial processes must not be created at the price of compromised consumer protection. A future regulation for data protection must be able to identify the unique risks Indian consumers might face while keeping in mind the potential of digital finance to promote financial inclusion.

1. Landscape

The need for data protection laws in India: The use of personal data by government and private service providers in interactions with individuals has become ubiquitous in India. These advances can greatly improve efficiency and reduce costs when delivering services to harder-to-reach users. However, the pervasive nature of data processing has raised concerns regarding privacy, exclusion due to digital service failure and related harms. Through our ground-level research study in 2017 titled *Privacy on the Line* (conducted with CGAP and Dalberg), it became clear that Indians cared deeply about their personal data and privacy when using digital services. These issues also became the subject of heated national debates that have taken place in India over the last two years.

Notable policy movements for data protection and finance: The culmination of the constitutional challenge to the Aadhaar project, during the course of which the Supreme Court of India's judgment also ruled on the fundamental right to privacy, provided an impetus for policy movement on data protection. Concerns have been rising given various reported occurrences of breaches of personal information from public and private databases, and connected concerns such as financial fraud and identity theft. For example, in 2017 it was found that a telecom operator with a Payments Bank licence used Aadhaar-based OTP verification to issue SIM cards were also automatically enrolling consumers into new payments bank accounts without consumers' consent, and in some cases directing benefit payments to these accounts.

Policy makers have responded to these developments at various levels. The establishment of a committee of experts on data protection in July 2017 by India's Ministry of Electronics and Information Technology (MeitY) began a year long process to build out a data protection framework for India, culminating with the release of a draft Personal Data Protection Bill 2018 (PDP Bill). The Bill is currently progressing through the parliamentary process but is yet to be introduced for consideration in the Indian Parliament. While the Bill awaits passage, specific sectoral regulators have begun acting on issues of data protection considered to be within their mandate.

In the financial sector, regulatory bodies have taken note of the increased use of data-driven techniques in finance as evidenced by the setting up of the Inter-Regulatory Working Group on FinTech and Digital Banking. The final report of the Working Group delivered in 2018 considered issues arising from rising digitisation including those relating to consumer data protection, organisational data, shared utilities, big data analytics, data security and fraud prevention. Separately the Telecom Regulatory Authority of India (TRAI) undertook a public consultation with its stakeholders on Privacy, Security and Ownership of the Data in the Telecom Sector in 2017. More recently, the Department of Industrial Policy and Promotion (DIPP) under the Ministry of Corporate Affairs released a draft National e-Commerce Policy in February 2019. However, the extent of regulatory coordination and sharing on these issues remains unclear.

Implications for financial services: Financial sector regulators in India are yet to create cohesive sectoral regulations on financial privacy and data protection. Currently consumer data is governed by rudimentary rules under the Information Technology Act, 2000 which have limited practical effect and are not robustly enforced. These issues have special relevance for finance, given the increasing digitisation of the sector and the growing use of non-financial information to support the delivery of financial services. Without a robust framework to govern the regulation of consumer data, consumers and providers are exposed to significant risks and uncertainty.

For example, the absence of a clear regulatory approach to the use of personal data contained in the Aadhaar database for financial services resulted in significant disruption to financial services in the aftermath of the judgment in the *Justice K S Puttaswamy & Anr v. Union of India & Ors* (Puttaswamy) on the constitutionality of the Aadhaar project.[1] This resulted in the curtailment of private sector use of the Aadhaar system and Indiastack APIs, and the reversal of requirements to link Aadhaar numbers to mobile numbers and bank accounts. This created some consternation in the financial sector, where several entities (in particular tech-driven financial players) had built their processes to take advantage of the features of the Indiastack including e-KYC for customer onboarding, Aadhaar authentication for transactions, payments and mandates through the Unified Payments Interface (UPI) and Aadhaar-based e-NACH. Subsequently, in March 2019, the Government promulgated an ordinance to allow certain private sector companies to continue to use e-KYC and Aadhaar authentication services. However there remains uncertainty regarding the breadth of this ordinance and its applicability across different types of financial service providers.

This policy experience has highlighted the difficulties that arise in the absence of strong frameworks to regulate the collection, storage and processing individuals' personal data in the course of service delivery. As the country plans further public infrastructure for finance, through Account Aggregators and the proposed Public Credit Registry, there is a need to pause and create serious safeguards to protect the compromise and misuse of personal information. Failure to do so could reduce trust and result in disruptions for digital finance, creating concerns for individuals, providers and regulators.

[1] As background, the judicial challenge to the Aadhaar project began in 2012 when KS Puttaswamy (a retired judge) filed a petition challenging the validity of mandatory Aadhaar enrolment and stated that it was violative of the citizens' right to privacy. In 2015, this petition along with several others was raised to the Supreme Court of India. A 3-judge bench hearing the matter referred it to a larger constitutional bench of at least 5 judges to resolve this question. The 5-judge bench which was hearing the referral on the constitutionality of the Aadhaar Act further referred the discreet question of determining ***"whether there is any fundamental right of privacy under the Indian Constitution"*** to a 9-judge bench (in light of two pre-existing supreme court judgments on related questions by 8-judge and 6-judge benches, which would potentially need to be set aside). In August 2017, a 9-judge Supreme Court bench unanimously held that privacy is a fundamental right protected by the Indian Constitution. The matter was returned to the original 5-judge bench of the Supreme Court considering the constitutionality of the Aadhaar Act. The bench upheld the constitutionality of the Aadhaar Act 4-1, but struck down several provisions, including those enabling private sector use of the infrastructure. Certain uses of the Aadhaar system by the State were also restricted.

2. Emerging Concerns

Decline or absence of consumer trust on digital platforms: The Indian population has a relatively large number of first-time digital platform users. Respondents of this demographic in our Privacy on the Line study often approached digital platforms warily due to direct experience of financial fraud or the perceived threat of fraud. Such misgivings may not be inappropriate, given the reality of the liability and grievance framework for consumers in India. For e.g. in the case of transaction disruptions or failures, consumers can have difficulty understanding which entity to approach especially where multiple entities are involved in a single digital finance transaction. This is exacerbated by the redressal mechanisms that can be weak or impersonal.

The potential of misuse of personal data and related harms: Emerging research including studies by Barocas & Selbst (2016) and Crawford & Schultz (2014) (cited in the reference list to this primer) have examined the potential for personal data analytics in finance including predictive analysis and machine learning (which base themselves on pre-existing data points and trends) to result in harms to individuals. For instance, misleading inferences created due to bad data quality can cascade into non-availability or denial of services, digital redlining or *weblining* [2], to mention a few.

Segmentation and profiling of consumers: The granularity of data available today can give service providers insights on consumers' behaviour, their preferences and their usage patterns. These insights can assist providers to customise products for relevant segments, differential pricing and variation in service provision. However, they could also be misused to create exclusion (by screening out *undesired* consumer segments), unfair financial terms (through predatory pricing) or further misconduct through mis-sale, unsuitable sale and unlawful discrimination.

3. Considerations for Regulators

Dependence of digital finance providers on the notice-and-consent model: Most privacy notices seek explicit consent from consumers to collect and subsequently process their data. However, while the notice-and-consent model can provide agency in theory, in practice it fails to meaningfully inform consumers or give them real choices on how their data can be used (Solove, 2013). Failure to provide consent can result in denial of service for most consumers, making this a false choice. Despite acknowledgment of this, Indian policy makers (including in the PDP Bill) have reverted to a notice-and-consent model for data protection. There is a need for policy thinking on access control measures and provider obligations that work ***irrespective of consent*** for better consumer protection and responsible financial conduct.

[2]The practice of creating and perpetuating inequities between different demographic groups specifically through the use of digital technologies and the data captured through them about different consumer groups (*see further* Hernandez et. al., 2001).

Digital harms and ex-ante regulatory measures to mitigate them: The understanding of the kinds of harms a consumer may be exposed to due to the processing of their personal data is still growing. Regulators need better frameworks for the identification of different risks and harms that consumers are exposed to through inappropriate handling and usage of consumer data. There is a need to mitigate these risks and harms using a range of regulatory tools, including those that can be deployed before breach or misuse of personal data to avoid them from occurring.

Ambiguity in the regulatory mandates in digital finance: The intersection of finance and use of digital personal data gives rise to a number of questions with respect to the ambit of existing regulators. This raises the larger question of where the institutional responsibility for supervision of these types of data use should lie. The boundaries of regulatory mandates of a future data protection authority, financial sector regulators and other sectoral regulators need to be clarified for a coordinated and clear approach to regulation.

Against this context, the session on **consumer data regulation** in data-driven finance at the 4th Dvara Research Conference can deliberate on the following questions:

- As consensus widens on the broad areas of the data lifecycle during which users must be protected (i.e. collection, processing and sharing), what are the areas where ambiguity remains as regards principles for data protection?
- What are the key challenges facing the implementation of a data protection law? How can data protection be made more effective and more enforceable?
- In the context of data-driven financial services, what are the kinds of consumer harm that regulators should be aware of?
- Is it the role of the data protection framework or a financial conduct and consumer protection framework to protect individuals from these harms?
- How should regulatory design evolve to avoid gaps or inconsistencies between the rubric of financial regulation and data protection regulation?

Resources

1. Acharya, B. (2015, May 30). The Four Parts of Privacy in India. Economic and Political Weekly. Retrieved March 26, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2851288

2. Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making.
Retrieved March 15, 2019, from http://www.dtc.umn.edu/weis2004/acquisti.pdf

3. Cavoukian, A. (2011, January). Privacy by Design. Retrieved March 14, 2019, from Information and Privacy Commissioner of Ontario:
https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

4. CGAP, Dalberg Design, Dvara Research. (2017, November 16). Privacy on the Line. Retrieved March 15, 2019, from Dvara Research:
https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

5. Chaturvedi, A. (2017, June 10). Overview of the Legal Issues around Aadhaar. Retrieved March 14, 2019, from PRS Legislative Research:
https://www.prsindia.org/theprsblog/overview-legal-issues-around-aadhaar

6. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (n.d.). A Free and Fair Digital Economy. Retrieved from Ministry of :
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

7. Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston College Law Review, 93-128. Retrieved March 14, 2019, from https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4/

8. Hernandez, G. A., Eddy, K. J., & Muchmore, J. (2001). Insurance Weblining and Unfair Discrimination in Cyberspace. SMU Law Review, 1953-1972. Retrieved March 14, 2019, from
https://scholar.smu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1906&context=smulr

9. Ministry of Electronics & Information Technology. (2017, December 18). White Paper on Data Protection framework for India. Retrieved March 26, 2019, from Ministry of Electronics & Information Technology:
https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

10. Raghavan, M. (2017, December 23). The Privacy Judgement and Financial Inclusion. Economic and Political Weekly, 58-61. Retrieved March 26, 2019, from
https://www.dvara.com/research/wp-content/uploads/2019/03/The-Privacy-Judgement-and-Financial-Inclusion-in-India.pdf

11. Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 1880-1903. Retrieved March 15, 2019, from
https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf