THE TOKENISATION FRAMEWORK AND ITS PRIVACY DISCONTENTS: ISSUES AND SOLUTIONS

*Sohini Banerjee, Shobhit Shukla & K.S. Roshan Menon**

The Reserve Bank of India's recent push for card-on-file tokenisation attempts to solve for the privacy and data security risk in India's payments sector. This article argues that while the tokenisation framework is motivated by necessary considerations, it is a sub-optimal method to solve for such risk as it does not meaningfully engage with the privacy-related dimensions of financial data protection. The optimal method to address such risk, we argue, is the enactment of a comprehensive data protection law, which encodes guiding principles recognised in data protection legisprudence across jurisdictions. To substantiate this, the article analyses select aspects of data protection frameworks and demonstrates their value in creating privacy-preserving financial services in India. While the (Indian) Data Protection Bill, 2021 ('DP Bill') may serve as a useful template for such a framework, the question of whether the provisions of the DP Bill meet this threshold, is beyond the scope of this article. The observations of this article are relevant for FinTech firms, sectoral regulators in India, and scholars of privacy law and financial regulation.

Table of Contents

* The authors are Research Fellows, Shardul Amarchand Mangaldas & Co., New Delhi. This research was supported by the Suresh Shroff Memorial Trust. The authors are grateful to Mr. Shardul S. Shroff for his generous support and encouragement that made this research possible. We thank Ms. Shilpa Mankar Ahluwalia, Mr. G.S. Hegde, Mr. Prashant Saran and Dr. Rajeev Uberoi for spirited conversations and thoughtful feedback. Shortcomings, if any, are solely attributable to the authors. The authors of this article are solely responsible for the contents thereof. The publication of this article shall not constitute or be deemed to constitute any representation by Shardul Amarchand Mangaldas & Co. or any of its Partners or Associates.

Note: The Data Protection Bill, 2021 ('DP Bill') is the reported version of the Personal Data Protection Bill, 2019 ('PDP Bill'). The DP Bill wasreported by a Joint Committee of the Houses as part oftheir Report of the Joint Committee on the Personal Data Protection Bill, 2019 ('Report'). The Report was presented to the Lok Sabha, and laid in the Rajya Sabha, on December 16, 2021. On August3, 2022, the PDP Bill, as reported by the Joint Committee, was withdrawn from the Lok Sabha. This has effectively meant that the DP Bill was also withdrawn from parliamentary consideration. Consequently, the judicial value of the DP Bill is now persuasive, since its clauses are akin to observations contained in a parliamentary committee report. The authors acknowledge the same andmake references to the DP Bill in a manner consistent with this perspective. *See generally*, Press Information Bureau Delhi, *Monsoon Session, 2022*, August 8, 2022, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1849999 (Last visited on August 17, 2022); *See also* Kalpana Mehta v. Union of India, (2018) 7 SCC 1.

I. INTRODUCTION

According to figures revealed by the government, as many as 6,07,220 cybersecurity incidents were reported in India in the first half of 2021.[1] Many such incidents resulted in the unauthorised disclosure of financial data stored on the servers of merchants and financial intermediaries.[2] Following these incidents, compromised financial data, including customers' credit card details, has often been found to be put up for sale on the 'Dark Web', and utilised for unauthorised transactions.[3] The frequency of financial data breaches, coupled with the enormity of their consequences, has prompted concern regarding better protection of financial data in an increasingly decentralised financial services sector.

To mitigate the severe consequences of such data breaches, the Reserve Bank of India ('RBI') has focused on finding solutions to reduce vulnerability in the ecosystem. Tokenisation is one such solution designed to enable efficient execution of card payments while avoiding unnecessary exposure of card details to entities in the transaction chain.

In simple terms, tokenisation refers to the replacement of a meaningful piece of information with a random array of characters, i.e., a 'token'.[4] In the

---

1 Lok Sabha Debates, *Cyber Security Incidents*, 1, July 28, 2021, Shri Rajeev Chandrashekhar, available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=25815&lsno=17 (Last visited on February 28, 2022).

2 Carnegie Endowment for International Peace, *Timeline for Cyber Incidents Involving Financial Institutions*, available at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (Last visited on February 28, 2022).

3 Bloomberg Quint (A.R. Palepu & V. Nair), *Indian Bank Review Leak after Details of 1.3 Million Cards Surface on Dark Web*, October 31, 2019, available at https://www.bloombergquint.com/business/indian-banks-review-leak-after-details-of-13-million-cards-surface-on-dark-web (Last visited on February 28, 2022); Inc 42 (H. Rakheja), *Domino's India Data Breach: 18 Cr Indian User Records Being Sold on the Dark Web*, April 12, 2021, available at https://inc42.com/buzz/dominos-india-data-breach-18-cr-user-records-being-sold-on-dark-web/ (Last visited on February 28, 2022).

4 M. Srinivas, *Tokenisation and its Impact on Online Payments*, Razorpay Blog, January 29, 2018, available at https://razorpay.com/blog/tokenisation-and-its-impact-on-online-payments/ (Last

context of card payments, tokenisation is intended to allow customer card details to travel through the transaction chain via a host of intermediaries in the form of a token while avoiding exposure of actual details to merchants and intermediaries (other than the card network and the issuer-bank).[5] Consequently, in the event of a data leak, only the 'tokenised' card details stand the risk of exposure. Without access to the underlying algorithm, such tokenised card details cannot be de tokenised to derive the actual details and potentially execute unauthorised card transactions.[6]

In recent years, tokenisation of card credentials has emerged as the solution favoured by the RBI in its efforts to minimise exposure of customer card data to only necessary entities in the transaction chain.[7] In the backdrop of the impending prohibition on storage of actual card details by merchants and intermediaries,[8] storage of tokenised card details is expected to enable cardholders to make payments to a merchant without requiring the mtore-enter their card details for each separate payment to such merchant. Thus, tokenisation is envisaged as a technological solution that will allow card payments to retain their efficiency

visited on February 28, 2022); Square, *Payment Tokenization Explained*, August 10, 2014, available at https://squareup.com/us/en/townsquare/what-does-tokenization-actually-mean(Last visited on February 28, 2022); EBANK, What is Payment Tokenisation and How does it Work, available at https://business.ebanx.com/en/resources/payments-explained/tokenization (Last visited on February 28, 2022).

5 Li-Hsiang Kuo, *Cracking Credit Card Number Tokenization*, Computer Science Department University of Wisconsin-Madison, 2011, available at https://pages.cs.wisc.edu/~lorderic/webpage/tokenization-crack.pdf (Last visited on February 28, 2022); P.R. Chowdhury & Y. Setlur, *India's Data Storage Conundrum: Analysing the RBI's Perplexing Regulations on Storage of Card Data*, IFLR, June 15, 2021 available at https://www.iflr.com/article/b1s7314jjg1fvq/indias-data-storage-conundrum-analysing-the-rbis-perplexing-regulations-on-storage-of-card-data (Last visited on February 28, 2022); A. Obhan & S. Bhutani, *India: Tokenisation of Cards in India: Explained*, Mondaq, October 29, 2021, available at https://www.mondaq.com/india/fintech/1125636/tokenisation-of-cards-in-india-explained (Last visited on February 28, 2022).

6 F. Liu, *Analysis of Tokenisation in Digital Payments*, Tufts University, 2016, available at https://www.cs.tufts.edu/comp/116/archive/fall2016/fliu.pdf (Last visited on February 28, 2022); Kuo, *supra* note 5; *See* N. Sahoo, *How does the Credit Card Tokenization Work*, Finance Derivative, April 14, 2021, available at https://www.financederivative.com/how-does-the-credit-card-tokenization-work/ (Last visited on February 28, 2022) (discussing a visual representation of the tokenization process).

7 *See generally* Reserve Bank of India, *Tokenisation – Card Transactions*, 2019, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11449&Mode=0 (Last visited on February 28, 2022) ('Tokenisation Circular 2019'); Reserve Bank of India, *Tokenisation – Card Transactions: Extending the Scope of Permitted Devices*, 2021, available at https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12152&Mode=0 (Last visited onFebruary 28, 2022)('Tokenisation Circular 2021');Reserve Bank of India, *Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services*, 2021, available athttps://rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0 (Last visited on February 28, 2022) ('CoF Directive').

8 *See* Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways*, 2020, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0 (Last visited on February 28, 2022) ('PA-PG Guidelines 2020'); Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways*, 2021, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0 (Last visited on February 28, 2022) ('PA-PG Guidelines').

while at the same time ostensibly eliminating the need for merchants and intermediaries to store actual card details for smoother checkout.

In this article, we argue that the RBI's tokenisation framework is a sub-optimal measure toward financial data protection. Part I of the article throws light on the evolution of the regulatory framework surrounding tokenisation, and how it has become central to the survival of the card payments industry. Part II points out the limitations of RBI's prescriptive framework as a measure to enhance data security. It proceeds to contend that *sans*a set of foundational privacy principles, the piecemeal framework fails to holistically address the inherent privacy risks involved in card payment transactions.

InPart III, we discuss the role played by our preferred solution, deployinga comprehensive data protection law, inenhancing the privacy and security of financial data. In this Part, we contend that principles recognised in data protection 'legisprudence' create living frameworks for data governance – providing a more dynamic and holistic framework than prescriptive technical standards to address concerns relating to financial data. Moreover, this Partpoints to certain key tools embedded within data protection laws, which enable them to overcome the inherent limitations of sector-specific regulation. In this manner, this article attempts to demonstrate that the optimal pathway to adequate protection of financial data lies in enacting a comprehensive data protection law for India.

II. A BRIEF HISTORY OF TOKENISATION

A. PHASE I: THE TOKENISATION CIRCULAR

The RBI's push towards seeking implementation of tokenisation as a method to secure payment data can be traced back to its circular dated January 8, 2019 (the 'Tokenisation Circular').[9] Through this instrument, the RBI permitted authorised card networks to act as token service providers ('TSPs') and provide tokenisation services to any token requestor [i.e., any merchant/third-party app provider ('TPAP') that desires to store customer card credentials in a tokenised form, upon the customer's request].[10] Such services could be offered for card payments for a variety ofcases, ranging from online payments to contactless transactions.[11]

The Tokenisation Circular set out the conditions under which tokenisation services were to be provided – including procedural requirements for TSPs and certification requirements for entities involved in the transaction chain.[12] As

[9] Tokenisation Circular 2019, *supra* note 7.
[10] *Id*., ¶2.
[11] *Id*.
[12] *Id*., Annex 1.

TSPs, the ultimate responsibility for compliance with these conditions was placed expressly on card networks.[13]

B. PHASE II: THE CARD DATA STORAGE PROHIBITION

While the Tokenisation Circular introduced rudimentaryregulatory architecture for tokenisation services, the mechanism assumed added significance with the issuance of the Guidelines on Regulation of Payment Aggregators ('PAs') and Payment Gateways ('PGs') on March 17, 2020 (the 'PA-PG Guidelines 2020').[14] Crucially, the PA-PG Guidelines 2020 included a prohibition on the storage of customer card credentials by merchants (as well as by PAs and PGs) on their respective databases or any server accessed by merchants.[15]

Prior to the issuance of these guidelines, it was common practice among merchants/TPAPs to save such credentials on their own servers.[16] This would ensure customer convenience by enabling them to complete subsequent transactions on the same portal without having to re-enter their credentials for each transaction. However, the guidelines effectively sign a led an end to this practice,casting a shadow on the efficiency of card transactions going forward.

To further underline its intention, the RBI issued a set of clarifications to the PA-PG Guidelines 2020.[17] These unequivocally reaffirmed that merchants, PAs, and PGs would not be allowed to store such credentials.[18] Storage of limited payment data would be permitted only for the purpose of transaction tracking and/or reconciliation for a limited period.[19]

C. PHASE III: BROADENING OF THE TOKENISATION AMBIT

As participants in the card payments ecosystem grappled with ways to provide a seamless experience to cardholders without storing such credentials,[20] the RBI expanded the scope of tokenisation to a wider set of permitted devices.[21] Further, by introducing card-on-file tokenisation, the regulator paved the way for

---

13 *Id*., ¶4.

14 PA-PG Guidelines 2020, *supra* note 8.

15 *Id*., Annex 1, ¶10.4 & Annex 2, ¶2.1.

16 *See* A. Venkatnarayan et al., *RBI's CoF and Tokenisation Guidelines – Analysing the Potential Impact on Digital Payments Industry*, The Dialogue/ Deepstrat, 2021, available at https://deepstrat.in/wp-content/uploads/2022/01/Tokenisation-_-Final-Draft.-1-2.pdf (Last visited on February 28, 2022).

17 The clarifications, issued on September 30, 2020, were subsequently incorporated into the PA-PG Guidelines dated March 31, 2021. The PA-PG Guidelines also extended the timeline for entities to purge stored card details, to December 31, 2021.

18 PA-PG Guidelines, *supra* note 8, at Annex 1, ¶¶6.2-6.3.

19 *Id*.

20 *See* Venkatnarayan, *supra* note 16 (discussing an overview of the challenges faced by entities in the card payments industry in complying with the card data storage prohibition).

21 Tokenisation Circular 2021, *supra* note 7.

the cardholder to allow storage of tokenised card details on a portal and use the same token across devices to make repeated payments on the portal.[22] Each portal would, however, require the TSP to obtain a separate consent artefact from the cardholder.[23]

In view of operational challenges faced by the industry and to allow industry participants to create awareness regarding tokenisation,[24] the RBI has repeatedly pushed the timeline for compliance with the prohibition against card data storage.[25] Crucially, within one of these directives, it has clarified that industry participants may devise additional mechanisms to handle any use-case that requires the storage of customer card credentials.[26] Although the RBI has remained steadfast in its position on card data storage, this clarification paves the way for the development of other solutions, which can be utilised for a wider variety of card payments, including EMIs, recurring e-mandates, and cashbacks.

Numerous tokenisation-based products have been launched in response to RBI's regulatory push.[27] These products continue to respond to the

---

22 CoF Directive, *supra* note 7; *See also* S.M. Ahluwalia & S. Shukla, *Card-on-File Tokenisation Introduced by RBI*, India Business Law Journal, November 18, 2021, available at https://law.asia/card-on-file-tokenisation-rbi/ (Last visited on February 28, 2022).

23 CoF Directive, *supra* note 7, at ¶3(e).

24 The operational challenges described in representations before the RBI, included challenges relating to the operationalisation of the technological infrastructure required for processing tokenised card transactions as well as challenges relating to the implementation of a system for 'guest checkout transactions'. Foran overview of the reasons for the extension, *see* India Business Law Journal (S.M. Ahluwalia & S. Shukla), *RBI Further Extends Deadline for Deletion of Card-on-File Data*,February 9, 2022, available at https://law.asia/rbi-further-extends-deadline-deletion-card-on-file-data/ (Last visited on February 28, 2022); V.J. Singh et al., *RBI's Card Tokenisation Mandate – A Bridge too Far?*, Mondaq, January 7, 2022, available at https://www.mondaq.com/india/shareholders/1148176/rbi39s-card-tokenization-mandate-a-bridge-too-far (Last visited on February 28, 2022); A. Singh, *Reserve Bank of India : Representation on Facilitating Compliance with Card-On-File Tokenisation (CoFT)*, NASSCOM Public Policy, December 9, 2021, available at https://community.nasscom.in/communities/policy-advocacy/reserve-bank-india-representation-facilitating-compliance-card-file (Last visited on February 28, 2022); *See also* Reserve Bank of India, *Restrictions on Storage of Actual Card Data*, June 24, 2022, available at https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12345&fn=9&Mode=0 (Last visited on June 30, 2022).

25 At the time of writing, the timeline for compliance with the prohibition on storage of card-on-file ('CoF') data has been extended to September 30, 2022. Further, for ease of transition in respect of 'guest checkout transactions', certain interim relaxations have been provided to merchants, their PAs and acquiring banks on the prohibition on storage of CoF data. *See* Reserve Bank of India, *Restrictions on Storage of Actual Card Data*, July 28, 2022, available at https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12211&Mode=0 (Last visited on August 18, 2022); Reserve Bank of India, *Restrictions on Storage of Actual Card Data*, June 24, 2022, available at https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12345&fn=9&Mode=0 (Last visited on June 30, 2022); Reserve Bank of India, *Restrictions on Storage of Actual Card Data*, December 23, 2021, available at https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12211&Mode=0 (Last visited on February 28, 2022).

26 RBI (2021), *supra* note 25, at ¶2b.

27 (S. Soni), *Digital Payments: What Tokenisation Solution has in Store for India's Vast Base of Merchants, Retailers*, November 18, 2021, Financial Express available at https://www.financialexpress.com/industry/sme/msme-tech-digital-payments-what-tokenisation-solution-has-in-

technology risks recognised by the RBI and are likely to create an ecosystem for security-preserving products based on the regulator's track record.

Effectively, the tokenisation framework acts as an impetus for market players to populate the financial sector with security solutions. Crucially, however, these solutions are designed to be limited in application. They create safeguards against a single technology risk – the breach of payments systems in India. They do so in the absence of a comprehensive law that can prioritise solving both: the technology-centric concern of data security and the human-centric concern of data privacy.[28]

On a micro-level, such narrowly tailored solutions require auditing for effective financial data protection. This regulatory strategy is myopic; a long-term vision of financial data protection would pursue regulatory dynamism, characterised by a principles-based framework within which industry participants can be encouraged to formulate specific solutions. On a macro-level, such regulations must be controlled for conflict since they rest on an internal logic that does not rely on accepted principles recognised by an underlying legislation geared towards personal data protection.[29] Consequently, different privacy regulations for

---

store-for-indias-vast-base-of-merchants-retailers/2371339/ (Last visited on February 28, 2022); National Payments Corporation of India,*NPCI Launches NTS Platform for Card Tokenisation*, October 20, 2021, available at https://www.npci.org.in/PDF/npci/press-releases/2021/NPCI-Press-Release-NPCI-launches-NTS-platform-for-tokenization-of-RuPay.pdf (Last visited on February 28, 2022); Team TechCircle, *Cash free Launches Tokenisation Solution for Merchants*, November 17, 2021, available at https://www.techcircle.in/2021/11/17/cashfree-launches-tokenization-solution-for-merchants/(Last visited on February 28, 2022); P. Abrar, *Phone Pe's 'Safe Card' Tokenisation Solution to help Users Meet RBI Norms*, Business Standard, November 2, 2021, available at https://www.business-standard.com/article/companies/phonepe-s-safecard-tokenisation-solution-to-help-users-meet-rbi-norms-121110200882_1.html (Last visited on February 28, 2022); *Visa Launches Card-on-File Tokenisation Services for Grofers, Bigbasket, MakeMyTrip: What it Means for You*, Economic Times Online, October 6, 2021, available at https://economictimes.indiatimes.com/wealth/save/visa-launches-card-on-file-tokenisation-service-for-grofers-bigbasket-makemytrip-what-it-means-for-you/articleshow/86808697.cms?from=mdr (Last visited on February 28, 2022).

[28] By a comprehensive data protection law, we mean to refer to a general law with the express objective of protecting personal data comprehensively. Examples of such a law include the EU's GDPR, the UK's Data Protection Act, 2018, and Australia's Privacy Act, 1988. In India, the landscape of data protection regulation is marked by fragmented frameworks – these include the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under the Information Technology Act, 2000, which provide largely for the rudimentary protection of only 'sensitive personal data', as well as directives issued by the RBI from time to time, which incidentally touch upon the protection of 'financial data' or 'payments data'.

[29] For instance, the RBI's Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022 requires card-issuers to be guided by *inter alia*, the need to "respect customer privacy", when card-issuers out source any operation to service providers. In a similar vein, the RBI's Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators dated August 3, 2021, requires payment system operators to ensure that their sales/marketing agents are trained to "handle their responsibilities with care and sensitivity, particularly for… privacy of customer information". In the absence of any statutory guidance on the

different sub-types of financial data risk privacy-arbitrage. The nature of such concerns and their impact on financial data protection are explored in the next section.

III. MISSING THE FOREST FOR THE TREES: LIMITATIONS OF THE RBI'S APPROACH TO FINANCIAL DATA PROTECTION

The previous section illustrated how, in the absence of a comprehensive framework for the protection of financial data, the RBI has had to resort to piecemeal regulations to balance the imperatives of card data security and customer convenience. However, while this measure is motivated by necessary considerations, the regulator's approach prompts broader concerns regarding the regulation of financial data protection in India.

First, we must note that customer card credentials represent only one form of financial data relating to customers. Moreover, there are numerous risks to the security of the cardholder's financial data– these include risks associated with a novel range of fraudulent actions, such as POS-skimming[30] and phishing.[31] Thus, the leakage of customer card credentials from the servers of merchants and intermediaries represents only one of many risks to financial data security in card payments.[32] Even with the masking of card details pursuant to the RBI's directive on tokenisation, the card payment ecosystem would remain vulnerable to such other risks, illustrated above. It is unclear how such risks will be addressed without a set of guiding principles for financial data security.

meaning of 'customer privacy' or 'privacy of customer information', the nature and scope of the obligationimposed by such provisions remains unclear and open to conflicting interpretations.

30 'Skimming', in financial data security parlance, is understood as the unauthorised capture and transfer of payment data to another source. POS-skimming, specifically, refers to the unauthorised capture and transfer of card details by way of a skimming device installed at a Point-of-Sale ('POS').

31 'Phishing', has been defined as 'a scalable act of deception whereby impersonation is used to obtain information from a target.' In the context of card payments, phishing is understood as an act by way of which card details are fraudulently procured from a cardholder, using an ostensibly reliable/genuine website, portal, or email address. *See* E.E. Lastdrager, *Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature*, Crime Science, 3, 2014, available at https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0009-y(Last visited on June 10, 2022) (for a review of literature on the concept of phishing); *See* Data Security Council of India and PayPal Payments Private Limited, *Fraud & Risk Management in Digital Payments A DSCI-PayPal Joint Study*, 2020, available at https://www.dsci.in/sites/default/files/documents/resource_centre/Fraud%20%26%20Risk%20Management%20in%20Digital%20Payments.pdf (Last visited on June 9, 2022) (for a detailed discussion of similar fraudulent actions and risks associated with digital payments, including card payments, in India).

32 *See* M. Braunet al., *Understanding Risk Management in Emerging Retail Payments*, Vol. 14(2), Economic Policy Review (2008) (on the variety of risks to financial data security); T. Bradford et al., *Nonbanks and Risk in Retail Payments: EU and US* in Managing Information Risk and the Economics of Security (Springer, Boston, MA, ME Johnson ed., 2009); J.S. Cheney et al., *The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches*, Vol. 36(4), Economic Perspectives (2012).

Moreover, if the RBI continues to prescribe particular solutions to tackle specific risks, it threatens to create a disaggregated framework for financial data protection in India. Such a framework will be detrimental, both from the principled perspective of legal certainty and from the pragmatic perspective of compliance costs for financial service providers.

Second, there exist numerous measures that can aid the enhancement of cardholder data security, as observed across jurisdictions. These may be in the form of technological solutions,[33] or in the form of regulatory imperatives to increase transparency and accountability in the functioning of entities in the transaction chain.[34] Tokenisation, and the accompanying imperative to merchants to purge card data together represent only one such technological solution. Thus, any regulatory push towards its imposition must be preceded with (a) relative assessment of its costs and benefits and (b) comparison against other alternatives that seek to achieve the same purpose.[35]

However, there is no evidence of any such assessment by the regulator. This casts doubts on the suitability of the tokenisation framework, both as a privacy solution and as a step towards maintaining the efficiency of card payments against the backdrop of the prohibition on card data storage. In the event the RBI continues to push for the implementation of tokenisation, it risks disincentivising financial service providers from developing better alternatives that may be more scale-sensitive, less disruptive, and protect cardholder data more robustly. While the RBI has advised the industry to "*devise alternatives in addition to tokenisation*",[36] there is no clarity on or illustration of the nature of such alternatives. It is also not clear whether such alternatives will require certification from the RBI and/or supervision by any regulated entity, in their implementation.[37]

Finally, the tokenisation framework requires "explicit user consent requiring additional factor of authentication ('AFA')" for tokenisation of card

---

[33] For instance, the PCI Security Standards Council prescribes encryption as a technological solution towards enhancement of card data security. *See* PCI Security Standards Council, *Payment Card Industry Data Security Standard (Version 4.0)*, March 2022, available at https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf (Last visited on June 9, 2022).

[34] As an illustration of regulatory imperatives to enhance transparency and accountability in the processing of financial data, the Brazilian General Personal Data Protection Law 13709/2018, (as amended by Law 13853/2019) (the 'LGPD'),requires that any entity processing personal data must be guided by, *inter alia*, transparency (i.e. guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy) and accountability (i.e. demonstration of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures). Further, the LGPD empowers the national authority to carry out audits in relation to the processing of personal data by processing agents, including public authorities.

[35] *See generally* R. Sane et al., *Should Consumers be Prohibited from Storing Card Data on the Internet?* (xKDR Working Paper Series, Paper No. 3, 2021).

[36] RBI (2021), *supra* note 25, at ¶2b.

[37] Ahluwalia, *supra* note 22.

details.[38] This simplistic formulation does not account for the various dimensions of consent involved in the collection and processing of any form of financial data, including card data. The framework does not require the TSP to disclose to the cardholder the risks associated with the processing of their card data for tokenisation.[39] Further, it is silent on the consequences of denial of consent by the cardholder and fails to guarantee the many minimum standard of service, in the event of such denial. Viewed against the broader human-centric conception of consent under privacy law,[40] such limitations effectively dilute the quality of cardholder consent under the framework.

At the same time, by requiring the cardholder to separately provide their consent for tokenisation for each particular merchant/TPAP and for each particular use-case, the framework risks the development of consent fatigue amongst cardholders.[41] If the RBI continues to prescribe separate consent requirements for each form of processing of financial data, it would adversely affect user experience and make the delivery of financial services cumbersome.

IV. AN ALTERNATIVE APPROACH: USING DATA PROTECTION LAW TO SAFEGUARD PAYMENTS DATA

The discussion in the Parts above demonstrates two key points. *First*, the RBI has sought to regulate for legitimate data security risks at play in the financial sector – namely data breaches, and unauthorised card transactions. *Second*, while the approach favoured by the regulator is motivated by necessary considerations, it may be viewed as an inefficient privacy solution. In this Part, we present an alternative approach to safeguard payments data.

Adopting the principles-based approach central to data protection jurisprudence, we seek to address the risks that RBI has sought to regulate through

---

38 CoF Directive, *supra* note 7, at Annex ¶3(e).

39 For discussion on the various dimensions of consent involved in the processing of personal data, see *infra* Part IV.D. on "Improved consent framework"; Venkatnarayan, *supra* note 16.

40 *See* S. Human & M. Kazzazi, *Contextuality and Intersectionality of E-Consent: A Human-Centric Reflection on Digital Consenting in the Emerging Genetic Data Markets*, IEEE European Symposium on Security and Privacy Workshops, 307, 2021, available at https://ieeexplore.ieee.org/document/9583707 (Last visited on February 28, 2022) (on the human-centric conception of consent under privacy law); E.A. Whitley, *Informational Privacy, Consent and the "Control" of Personal Data*, Vol.14(3), Information Security Technical Report, 154 (2009); F.H. Cate & V. Mayer-Schönberger, *Notice and Consent in a World of Big Data*, Vol. 3(2), International Data Privacy Law, 67 (2013).

41 *See* B. W. Schermer et al., *The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data Protection*, Vol. 16, Ethics Inf. Technol., 171 (2014) (on consent fatigue); H. Choi et al., *The Role of Privacy Fatigue in Online Privacy Behavior*, Vol. 81, Computers in Human Behavior, 42 (2018); M.J. Taylor & J.M. Paterson, *Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection*, Vol. 16, Indian Journal of Law & Technology, 71 (2020).

its tokenisation framework. In doing so, we demonstrate the advantages of this approach, in comparison to the stance taken by the RBI.

A. PRINCIPLES-BASED APPROACH

With a principles-based framework at its core, data protection jurisprudence adopts a sector-agnostic outlook towards the governance of various privacy and data security risks. The essence of this approach may be illuminated through a glance at Balkin's views on the fiduciary relationship lying at the heart of data protection. Balkin has pointed out that entities in the digital domain "invite people to trust them with their data".[42] Subsequently, when individuals do repose their trust in such entities, they become vulnerable to the data processing practices of the latter. In other words, individuals are then exposed to the whims of company policy on securing, storing, or sharing personal data with third parties.[43] Consequently, Balkin argues that the law should treat such entities that collect and process the personal data of users as 'information fiduciaries'.[44]

Further, Buckley *et al.* have argued that financial regulation is generally motivated by one or more of the following four objectives — financial stability, financial integrity, customer protection, and financial efficiency, development & inclusion.[45] The objectives of financial stability and integrity are mirrored in the issuance of the tokenisation framework. Additionally, the RBI has been motivated by the object to ensure customer protection by making card transactions safer and more secure.[46] In other words, the regulator has sought to strengthen the fiduciary relationship between customers and financial entities, by enhancing the trust customers are able to repose in the protection and security of their own personal data.

We posit that the principles-based matrix of data protection jurisprudence is better suited to pursue this objective. Unlike bright-line rules that are prescriptive in nature, principles lend flexibility to regulated entities as well as regulators.[47] Principles provide broad guidance on what constitutes "normatively good conduct" in that context.[48] *Ergo*, a principles-based approach promotes positive outcomes and limits negatives outcomes without prescribing the precise route. Furthermore, a significant advantage of adopting such an approach lies in its ability to allow regulators to boost rapid innovation while imposing appropriate limi-

---

42 J. M. Balkin, *The Fiduciary Model of Privacy*, Vol. 134(11), HARVARD LAW REVIEW, 11 (2020).

43 *Id*.

44 *Id*.

45 R. P. Buckley et al., *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*, UNSW LAW RESEARCH PAPER, 19, 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640 (Last visited on February 28, 2022).

46 Tokenisation Circular 2019, *supra* note 7, at Annex I; Tokenisation Circular 2021, ¶2; CoF Directive, *supra* note 7, at Annex ¶3€.

47 D.W. Arner et al., *Governing FinTech 4.0: BigTech, Platform Finance, and Sustainable Development*, Vol. 27(1), FORDHAM J. CORP. & FIN. L., 1 (2022).

48 *Id*.

tations to prevent negative externalities.[49] In this regard, data protection principles have evolved over time to protect personal data of individuals in a manner that its collection, use and disclosure is limited.[50] These principles have been crystallised in various jurisdictions in response to the need for legal frameworks to keep pace with tectonic shifts in data processing.[51]

Broadly, modern data protection frameworks are composed of six fundamental principles constituting its building blocks. A glance at the EU General Data Protection Regulation ('GDPR') serves as a useful illustration.[52] First, personal data shall be processed in a lawful, fair, and transparent manner ('lawfulness, fairness, and transparency');[53] second, personal data shall be collected for specified purposes, and processed in a manner compatible with those purposes ('purpose limitation');[54] third, personal data shall be limited to only what is necessary to achieve the above-specified purpose(s) ('data minimisation');[55] fourth, personal data shall be accurate and kept up to date ('accuracy');[56] fifth, personal data shall be stored only for as long as necessary for the purposes of processing ('storage limitation');[57] sixth, personal data shall be processed in a manner that ensures its integrity, security and confidentiality through appropriate technical or organisational measures ('integrity and confidentiality').[58]

These six overarching principles form the bedrock of modern data protection legislations like the GDPR, UK Data Protection Act, 2018,[59] and the Indian (draft) Data Protection Bill, 2021 ('DP Bill').[60] They, directly and indirectly, influence other provisions set out under the respective laws. Insofar as the principles described above create living frameworks of data governance, and effectively draw a perimeter of fair and lawful processing, we believe that they would outlive rigid technical standards set by sectoral regulators on an *ad-hoc* basis.

---

49 *Id*.

50 *See* L.A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits (Information Law Series – 10, Kluwer Law International: The Hague/London/New York, 2002).

51 *See also* R. Gellman, *Fair Information Practices: A Brief History*, Bob Gellman, April 10, 2017, available at https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (Last visited on February 28, 2022) (the Code of Fair Information Practices based on Fair Information Practices Principles was a seminal document developed by an advisory committee appointed by the US government to study the deployment of automated systems to process personal data of individuals. It is considered to be the fountainhead of various principles informing data protection laws globally); Justice B. N. Krishna Committee, *White Paper of the Committee of Experts on a Data Protection Framework for India* (December 18, 2017).

52 Regulation (EU) 2016/679 (April 17, 2016), Art. 5 ('GDPR').

53 *Id*., Art. 5.1.a.

54 *Id*., Art. 5.1.b.

55 *Id*., Art. 5.1.c.

56 *Id*., Art. 5.1.d.

57 *Id*., Art. 5.1.e.

58 *Id*.

59 The United Kingdom Data Protection Act, 2018 (Cl. 12) (U.K.).

60 The Data Protection Bill, 2021, annexed to Joint Committee on the Personal Data Protection Bill, 2019, *Report of the Joint Committee on the Personal Data Protection Bill, 2019* (December 16, 2021).

The approach described above would prevent the formation of a mosaic of data frameworks by sectoral regulators. This would imbue clarity, coherence, and consistency into the outlook for regulated entities. Moreover, instead of solutions that seek to merely meet the requirement of bright-line standards, principles may encourage entities to pursue high-value solutions that exceed the efficacy required under law. Such solutions could be privacy-*enhancing*, as opposed to merely privacy-preserving technologies. Finally, principles centre the privacy and data security debate squarely within the realm of the individual. The individual is then viewed as the primary stakeholder, and the framework seeks to uphold their meaningful control over their personal data.

B. TRANSPARENCY AND ACCOUNTABILITY TOOLS

As a framework designed to address systemic privacy and data security risks, data protection jurisprudence is well equipped to continuously evaluate the security credentials of a financial entity. Accordingly, the transparency and accountability tools encoded within the data protection law can support the future of financial data security.[61] It is unclear, in comparison, how the RBI as a sectoral regulator can achieve the same results at scale under the tokenisation framework.

Illustratively, we examine three key tools contained in the DP Bill to address security evaluation of a financial entity. *First*, entities classified as significant data fiduciaries under the Billare required to undergo an annual audit of their policies and the way they process personal data.[62] Among other factors, the independent data auditor is required to examine security safeguards adopted by the data fiduciary, instances of personal data breach and response of the data fiduciary, including how promptly the entity has informed the Data Protection Authority ('DPA') of the same.

Second, the DP Bill mandated the conduct of a data protection impact assessment ('DPIA') in certain cases pertaining to activities of significant data fiduciaries.[63] Where a significant data fiduciary intends to deploy new technologies, large scale profiling, use of sensitive personal data, or any other processing carrying a risk of significant harm to individuals, such processing can commenceonly after a DPIA by the data fiduciary.[64] In fact, the DPA is empowered to specify classes of data fiduciaries, or processing operations, for which the requirement for

---

[61] D.A. Zetzscheet al., *The Future of Data Driven Finance: Lessons from EU Big Bang II*, Vol. 25, Stanford Journal of Business and Finance, 245 (2020).

[62] *See* Data Protection Bill, 2021, Cl. 29 ('DP Bill') (the criteria for determining significant data fiduciaries are provided under Clause 26 of the DP Bill. Some of the listed criteria especially relevant for financial entities are volume of personal data processed, sensitivity of personal data processed, risk of harm by the processing and use of new technology for processing).

[63] *Id*., Cl. 27.

[64] *Id*., Cl. 27(1).

a DPIA would be mandatory to begin with.[65] A DPIA would contain an assessment of potential harms to data principals and measures for mitigating such risks.[66]

A *third* key tool contained in the Bill related to the reporting of personal data breaches. Every data fiduciary is required to report any instance of a personal data breach to the DPA. Such a report must be made within seventy-two hours.[67] Keeping in mind the need to keep the individual informed, the law also empowers the DPA to direct the data fiduciary to inform the data principal of the breach, as well as conspicuously post the details of the breach on its website.[68]

A review of the above tools indicates that data security is a crucial issue in modern data protection jurisprudence.[69] It is thus not surprising that the RBI's object of regulating customer protection is addressed comfortably by the existing tools in a comprehensive data protection law like the DP Bill. The requirements to conduct an annual audit, data protection impact assessment, and prompt reporting of data breaches meet a dual purpose. On one hand, financial entities would need to ensure they have appropriate security safeguards in place. Failure to do so may attract stringent enforcement mechanisms under the proposed law.[70] Moreover, these tools achieve the goal of protecting customers through dynamic means – allowing the industry the legroom to devise specific methods.[71] Much like the advantages of the principles-based approach discussed above, the object here is to guide industry on the broader ends, as opposed to being overtly prescriptive on specific methods of achieving those ends.

On the other hand, customers are duly protected by the privacy and security safeguards envisaged under the proposed law. The three tools discussed above have been formulated based on an assessment of potential harm to the data principal. In fact, the requirements to report the data breach to the individual in certain cases and post the details of the breach conspicuously, underline the individual centric approach of the proposed law. It is unclear how the RBI with its sector-specific mandate can achieve the same scale of impact through disaggregated regulation.

---

65 *Id*., Cl. 27(2).

66 *Id*., Cl. 27(3).

67 *Id*., Cl. 25.

68 Apart from the key tools discussed above, the DP Bill contains a host of other relevant tools. These include the requirement for a privacy by design policy, the promotion of transparency in processing of personal data through context-specific information disclosure, and the appointment of a data protection officer.

69 Zetzsche *supra* note 61, at 20.

70 DP Bill, *supra* note 62, at Cl. 57.

71 The DP Bill allows the industry to submit Codes of Practice in furtherance of its obligations under the draft law; DP Bill, *supra* note 62, at Cl. 50(2)(b).

C. VIEWING FINANCIAL DATA AS SENSITIVE PERSONAL DATA

The alternative approach suggested in this article favours the governance of financial data at large, over specific forms of financial data. This differs from the approach adopted by RBI, wherein it has chosen to regulate for privacy risks specific to card data through the tokenisation framework. Data protection jurisprudence does not discriminate between types of financial data. Instead, it views financial data as sensitive personal data. This categorisation recognises that financial data can reveal immense detail about an individual's inner life, thus necessitating enhanced data protection *vis-à-vis* ordinary personal data.

Integrating data protection jurisprudence with the regulation of financial data would unlock the benefits of 'FinTech 4.0' – arguably the future of the finance industry.[72] Coined by Arner *et al*, the term represents a typology characterised by the development of new technologies in response to unique challenges in the financial services ecosystem. FinTech 1.0 was marked by the laying of the Atlantic undersea cables in 1867.[73] FinTech 2.0 saw the development of the handheld calendar by Texas Instruments.[74] FinTech 3.0 evolved as a response to the Global Financial Crisis and was underscored by the development of the Bitcoin.[75] FinTech 4.0 witnessed regulators shut down Ant's planned IPO in 2020 over dominance and concentration-driven concerns.[76] In essence, FinTech 4.0 spotlights the emergence of complex financial institutions, characterised by cross-border activity, digitization and datafication.

Arner *et al* have analysed how regulating financial data through data protection jurisprudence would enable the digitisation and datafication of finance.[77] Data protection regulation can boost competition by curtailing the risks of data monopolies, enhance trust in public institutions, and limit the negative impact of digital finance platforms.[78] Further, data protection would enable a sustainable approach towards technology by ensuring lawful and fair processing of personal data.

Such digitisation could reveal network effects and economies of scale, thus propelling the onset of 'FinTech 4.0', an era characterised by the prominence of digital finance platforms.[79] Regulatory frameworks in India should aim to support the onset of FinTech 4.0 through a principles-based approach, undergirded

[72] Arner *supra* note 47, at 6.
[73] *See generally* D.W. Arner et al., *The Evolution of FinTech: A New Post-Crisis Paradigm*, UNSWLRS, 62 (2016).
[74] Arner, *supra* note 47, at 8-9.
[75] *Id*., 15.
[76] *Id*., 6-7.
[77] *Id*., 6.
[78] *Id*., 40-42.
[79] *Id*., 6.

by privacy and data security. A comprehensive data protection law offers this very opportunity.

Second, the construct of financial data under data protection jurisprudence enables the application of uniform privacy principles to the entire financial sector. A review of the tokenisation trajectory in PartII reveals that regulation in the space has been fragmentedand difficult to comply with. The suggested approach would prevent the formation of a disaggregated regulatory framework with a mosaic of regulations on privacy and data security risks in the financial sector.

Instead, the application of uniform data protection principles would lend regulatory certainty and predictability to the benefit of market participants. The result is a win-win for both customers and industry – with customers gaining from the protection of sophisticated, modern privacy and data security norms, and industry gaining from the certainty of operating under a single umbrella legislation. Furthermore, the guidance provided by core principles would potentially-catalyse innovation while striking a balance with customer protection.

This focus on core principles is also pertinent in other contexts. To an extent, the principles articulate a provisional 'basic structure' for privacy protections. This basic structure has two dimensions: a positive dimension that outlines the privacy safeguards afforded to individuals, and a normative dimension that allows these safeguards to be animated further to create new rights. Consequently, in the context of the financial sector, these principles outline the first steps for privacy regulation for financial data in India. Further, as previously discussed,[80] they also set the tone for future steps, which may involve balancing novel rights with other considerations (such as national security). A discussion on these steps, and the ways in which extant data protection laws have considered them, is beyond the scope of this article.

Moreover, enacting this basic structure in any form, betters the privacy architecture prevalent for financial data in India. Put differently, a comprehensive data protection law represents a progressive step for financial data privacy in India. It takes regulators away from piecemeal or non-comprehensive regulation, and allows them to build customized privacy frameworks, undergirded by common principles.[81] The efficacy of such frameworks is yet to be fully assessed there is no comprehensive data protection law in India. However, due to the special status they provide to financial data, they are likely to meaningfully alter the privacy expectations associated with such data.

[80] See *supra* Part IV. A on "Principle Based Approach".

[81] Department Related Parliamentary Standing Committee on Commerce, *Promotion and Regulation of E-Commerce in India*, 2022, One Hundred and Seventy Second Report, 16 (July, 2022); Recently, a Parliamentary Standing Committee acknowledged the role of the Personal Data Protection Bill, 2019 – the Bill is a predecessor to the DP Bill – in providing, "the guiding principles for formulation of rules regarding the ownership and storage, use and access and cross border movements of data".

D. IMPROVED CONSENT FRAMEWORK

In Part III of the article, we have outlined that consent under the tokenisation framework is conceived in limited terms; visualising cardholders as 'out-of-the-loop' individuals who need not be appraised of the risks in processing financial data.In essence, consent under the tokenisation framework is myopic, relatively opaque and risks authentication fatigue.

The practical shortcomings of this framework are best addressed by adopting a consent framework consistent with one provided under data protection legisprudence. There are two significant reasons behind this.

First, a comprehensive data protection law creates a 'culture of informational self-determination' that the framework presently lacks. It is easier to explain this with an example: consider an individual consenting to the tokenisation request by entering a One-Time Password. At the time of giving theirconsent, it is unclear whether such individualis appraised of the privacy risks involved with tokenisation (such as the vulnerability of tokenisation vaults).[82] Further, the framework is unclear on whether explicit consent is sought to transfer the tokenised personal data of individuals to third parties.

Well-formed data protection laws address these concerns by coding risk-intimation into consent-procurement. The GDPR, for instance, advises that natural persons be, "made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."[83] The DP Bill also contained a similarly-designed provision for obtaining consent.[84] These provisions highlight the value that data protection places on risk-evaluation, compelling regulated entities to identify data-driven risks and appraise data principals of the same.

In her scholarly work studying the origins of consent, Kosta argues that the exercise of consent is, in essence, a participatory right.[85] Citing the German Constitutional Court's decision in the *Population Census* case, a judgement wherein the Court had held that informational self-determination was a constitutional right of German citizens, Kosta argues, that consent allows the careful application of personality liberty to, "decide and determine the release of their

---

82 *See generally* Liu, *supra* note 6.

83 GDPR, *supra* note 52, at Recital 39; C. Kuner et al., The EU General Data Protection: A Commentary, 315 (OUP 2020) (identifying this as the *transparency* principle and implying that it is difficult to implement).

84 DP Bill, *supra* note 62, at Cl. 11(3).

85 E. Kosta, Consent in European Data Protection Law, 51 (Martinus Nijhoff Publishers, 2013); *See also*, S. Breen et al., *GDPR: Is Your Consent Valid?*, Vol. 37(1), Business Information Review 20 (2020); H.Y. Lim, Data Protection in the Practical Context, 131 (Third Impression, Academy Publishing, 2019).

personal data".[86] Naturally, this framing of consent as a personal liberty concern allows individuals to take ownership of their personal data and independently assess privacy risks.[87]

Second, comprehensive data protection laws are better designed to guard against consent fatigue than the tokenisation framework. Such laws allow entities to seek uniformexplicit consent for a variety of data processing activities. Under the DP Bill, for instance, the standard for consent was adequately met if the individual explicitly consents to the tokenisation of their card data.[88] Such consent may be obtained *via* a detailed consent tray and does not rely on simplistic technological fixes (such as AFA).

In this context, the DP Bill's silence on AFA seems no accident. Soft policy instruments that have punctuated the development of this Bill have noted the possibility of consent fatigue, "if the principal will be continuously required to take affirmative action to demonstrate such consent".[89] Consequently, the Bill mooted a purpose-driven interpretation of consent, preserving cardholder autonomy and promoting practical convenience.

E. MEANINGFUL REGULATORY CO-OPERATION

Beyond the limitations identified in the previous Part, it is important to point out a salient weakness of piecemeal regulations such as the tokenisation framework. By setting up quasi-data protection laws of limited effect for the financial sector, such regulations may stymie the RBI's ability to co-operate with a data protection authority to better secure the financial data of individuals.

In fact, news reports have highlighted the tension between the RBI and a proposed data protection authority for India,[90] noting the former's request for an exemption from the India's proposed data protection law.

---

86 Kosta, *supra* note 85, at 22; Kuner *supra* note 83.

87 *See* OECD (2020), *Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis*, 21, available at www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-andthe-Role-of-Financial-Education.pdf (Last visited on February 28, 2022) (for an analysis of the role of the GDPR in securing financial data); *See also* Zetzsche, *supra* note 61.

88 DP Bill, *supra* note 62, at Cl. 11.

89 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 39 (July 27, 2018); *See* M.A. Sasse et al., *The Great Authentication Fatigue – And how to Overcome it* (Cross Cultural Design International Conference, Heraklion, 2014), available at https://discovery.ucl.ac.uk/id/eprint/1434817/1/The_Great_Authentication_Fatigue_Sasse_Krol.pdf (Last visited on February 28, 2022) (for a robust assessment of consent fatigue).

90 *RBI Seeks Exemption from Data Protection Law*, Hindustan Times, September 10, 2020, available at https://www.hindustantimes.com/india-news/rbi-seeks-exemption-from-data-protection-law/story-kwQzNs614s0C56VK6HTCJP.html (Last visited on February 28, 2022).

Such scepticism is, however, unwarranted. A brief look at the role of privacy regulators indicates that they are designed to co-operate with financial sector regulators. In Singapore, for instance, the Association of Banks in Singapore has published a Code of Banking Practices that outlines a series of data protection principles that must guide personal data processing among banks.[91] This Code envisages co-operation between the Singapore's financial sector and privacy regulators to secure financial data in Singapore.

Similarly, the DP Bill contains provisions that allow the DPA to issue codes of practice in collaboration with relevant sectoral regulators.[92] Moreover, the DPA is mandatorily required to consult other regulators enjoying concurrent jurisdiction on specific issues, and it is obliged to cede regulatory space to such regulators on issues involving the conduct of significant data fiduciaries.[93] Such regulatory delineation accounts for sector-specific concerns, while also drawing from the benefits of an overarching sector-agnostic data protection framework.

Relevantly, this curated privacy ecosystem benefits the RBI. The laws in the ecosystem outline a set of core privacy values that financial entities must adhere to. Additionally, data protection authorities, shoulder some of the enforcement risks that the RBI would otherwise have to manage under its financial data security mandate.

Understanding the impact of such risk-distribution involves appreciating the machinery of data protection law. Here, the regulatory innovation critical to the efficacy of such laws is the appointment of a Data Protection Officer ('DPO').[94] On an individual level, the DPO acts as a point of contact between the privacy regulator and the relevant data fiduciary.[95] Collectively, the officers represent a core of information privacy professionals who can be skilled to adeptly execute various regulatory commands, including those related to the protection of financial data. This is to the RBI's advantage; introducing a specialised training module for financial-sector DPOs can allow the RBI to groom relevantly skilled

---

[91] Code of Banking Practices – The Personal Data Protection Act, 2021 (Singapore); *See* Monetary Authority of Singapore, *Obligations of Financial Institutions under the Personal Data Protection 2012 – Amendments to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism*, June 2, 2014 (Consultation Paper P 005 -2014), available at https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/2-Jun-2014-CP-on-PDPA_Amendts-to-AMLCFT-Notices.pdf (Last visited on February 28, 2022); Notably, §4(6) of the Singaporean Personal Data Protection Act, 2012, proclaims that in the event of an inconsistency with other written laws, the provisions of those written laws shall prevail. This exemption has been cited by the Monetary Authority of Singapore to ideate on possible conflict avoidance mechanisms between AML/CFT regulation and privacy law.

[92] DP Bill *supra* note 62, at Cl. 50.

[93] *Id*., Cls. 56, 26(4).

[94] *See* GDPR, Arts. 38.1, 39; DP Bill, *supra* note 62, at Cl. 30.

[95] P. Lambert, The Data Protection Officer: Profession, Rules and Role, 12 (Taylor & Francis, 2017); B. Tan, *A Practical Perspective* in Data Protection Law in Singapore: Privacy and Law in an Interconnected World, 160 (S. Chesterman, 2nd ed., Academy Publishing, 2018).

regulatory personnel. At the same time, these DPOs can assume other regulatory objectives, allowing the pursuit of both privacy and financial data integrity.

Meaningful co-operation can also result in the development of frameworks for benchmarking financial data privacy. To illustrate this, consider the provisions of the DP Bill that enabled regulators to assign data trust scores to entities processing personal data.[96] The purpose of such a score is to inspire trust among its users; entities with a high trust score can market their privacy-preserving financial services to potential customers.

Prima facie, the provisions enabling data trust scores for entities are industry-blind. This is to say that the draft law does not explicitly motivate the regulator to account for industry-based sensitivities while formulating its scoring mechanism. Such oversight can create ineffective privacy scores, wherein less pertinent variables are assessed on an equal footing to more pertinent variables. A bank, for instance, may be awarded a moderate data trust score if it scores highly on a set of parameters (say protection of employees' personal data), while scoring lowly on other, more significant parameters (such as the protection of customers' personal data).

Here, regulatory co-operation can help identify the relevant variables/criteria that may be assessed to assign financial sector entities a data trust score. Further, the RBI may work closely with the DPA in recognising the weight and impact each assessed variable must be provided, to add a layer of robustness to the process of determining trust scores. Such assessment helps consolidate the regulatory vulnerabilities identified by multiple regulators, permitting a comprehensive evaluation of an entity's privacy credentials.

Overall, the RBI/DPA dual-regulation ecosystem solution relies on a shared utilisation of regulatory capacities between two regulators. Herein, a data protection law shall act as the base regulatory response to the financial security conundrum, onto which the RBI may further layer industry-specific regulations.

V. WAY FORWARD AND CONCLUSION

Our analysis of the tokenisation framework reveals its limitations in addressing privacy risks in India's payments industry. The optimal pathway to correct this, we believe, lies in enacting a comprehensive data protection law for India. Not only would this allow India's financial services industry to benefit from a principles-led approach to data security and privacy, but it also would also bestow customers with meaningful control over their personal data. More merit is accrued to this approach upon acknowledging the gains it makes on the counts of clarity and certainty – seeing complex data sets through the lens of financial data

[96] DP Bill, *supra* note 62, at Cl. 29(5).

guarantees a standard of protection consistent with other highly sensitive data sets. To summarise, customers and market players are better placed in an ecosystem wherein a privacy law undergirds data security safeguards developed for the payments industry.

Naturally, the pursuit of a data protection solution comes with a sense of curiosity over the ideal template for a data protection law. While this is not within the scope of the article, upon examining the provisions of the DP Bill, we believe that a regulation consistent with the Bill's stated objects, outcomes and regulatory design can solve for several privacy risks inherent in the financial sector. This is not to say that the Bill exemplifies an optimal data privacy law. Instead, it is to suggest that the way forward lies in enacting a framework consistent with the principles embodied in the Bill and meaningfully interpreting the provisions of such an enactment, particularly those enabling co-ordination with other sectoral regulators, to create pathways for efficient privacy risk-management. A shared regulatory mechanism, developed jointly by aspecialised data protection authority and the RBI, can efficaciously navigate such risks.