IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 18 | Issue 1 | 2022

Special Issue on FinTech

[Cite as: 18 IJLT, < page no. > (2022)]

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BANGALORE

Price: Rs. (in 2 issues)

The mode of citation for this issue of The Indian Journal of Law and Technology, 2022 is as follows:

18 IJLT, <page no.> (2022)

Published by:

Student Bar Association
National Law School of India University
Nagarbhavi, Bangalore – 560072
Website: www.ijlt.in
Email: ijltedit@gmail.com

Distributed exclusively by:

Eastern Book Company
34, Lalbagh, Lucknow - 226 001
U.P., India
Website: www.ebcwebstore.com Email: sales@ebc.co.in

The views expressed by the contributors are personal and do not in any way represent the institution.

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
WWW.IJLT.IN

Volume 18 | Issue 1 | 2022

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 18 | Issue 1 | 2022

Contents

ARTICLES

Rise of Decentralised Finance | Reimagining Financial Regulation

Shehnaz Ahmed[*]

ABSTRACT *Based on decentralised ledger technology (DLT), decentralised finance (DeFi) involves the provision of financial services without reliance on centralised intermediaries (such as banks). While DeFi seeks to complement existing financial services, its reliance on crypto asset speculation and arbitrage coupled with instances of security, operational and governance failures, may pose risks to consumers and the financial system. Therefore, the proliferation of such markets without any regulatory oversight requires immediate consideration. While existing literature focuses on the innovation potential of DeFi, there is little discussion about the legal implications of DeFi. This article seeks to address this gap in the literature and recommends possible regulatory approaches. The article highlights that DeFi will challenge traditional financial regulations designed for centralised systems where identifying the subject of regulatory obligations is straightforward. Further, participants in a DeFi system can be spread across multiple jurisdictions, challenging the determination of the relevant jurisdiction whose law will apply. As the DeFi market is still evolving, this article argues that regulatory focus must be on specific aspects. This includes regulatory clarity for cryptoassets, regulating gatekeepers of the DeFi ecosystem i.e., service providers (like exchanges, wallets, custodians), and issuance of regulatory guidance on the applicability of existing laws to DLT systems. These regulatory approaches must be supplemented with measures such as designing internationally well-recognised standards for DeFi services, harnessing technology ("Regtech" and "Suptech") for better supervision and compliance and leveraging existing regulatory sandboxes for a cost-benefit analysis of such innovations and determining regulatory responses.*

[*] Shehnaz Ahmed leads the Fintech research at the Vidhi Centre for Legal Policy, where she undertakes cutting-edge research on issues such as digital currencies, blockchain, and digital payments. At Vidhi, she works with the Government of India and financial sector regulators on designing legal reforms for the financial sector.

Background

As policymakers continue to debate the regulatory response to crypto assets, the financial system is witnessing another manifestation of the crypto economy with the emergence of decentralized finance ("**DeFi**"). Based on the Distributed Ledger Technology ("**DLT**"), DeFi seeks to provide financial services and products to users without the need for centralised intermediaries.

In the summer of 2020, DeFi applications started to gain traction with an increase in its users. The total value of crypto assets 'locked' in DeFi transactions [a common industry measure referred to as total value locked ("**TVL**")] rose from less than $1 billion in 2019 to over $15 billion at the end of 2020 and over $100 billion in December 2021.[1] While the TVL has dropped, reports indicate that there are around 4 million unique addresses (a proxy for the number of users) using DeFi applications,[2] indicating a gradual adoption of such applications. DeFi is a niche market with relatively lower volumes of transactions compared to the global financial system. However, the growth of the market, its innovation potential, and the risks to the financial system from such developments have sparked interest among policymakers, financial institutions, and researchers. Given that such markets mainly operate outside the regulatory perimeter, they have come under regulatory scrutiny. The Financial Stability Board ("**FSB**") notes that "without sufficient regulation and market oversight, DeFi and associated platforms might present risks to financial stability."[3] For instance, DeFi markets have already witnessed several operational and cybersecurity incidents, that have resulted infinancial losses to the users. DeFi related hacks made up over 75% of the total $681 million known hack and theft volume of crypto asset still

[1] FSB, *Assessment of Risks to Financial Stability from Crypto Assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022; David Gogel *DeFi Beyond the Hyp*e (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[2] Adith Podhar and Kamini Shivalkar, 'Why DeFi is the Biggest Thing in the History of Finance' (*The Economic Times*, 22 February 2022) <https://economictimes.indiatimes.com/markets/cryptocurrency/why-defi-is-the-biggest-thing-in-the-history-of-finance/articleshow/89745980.cms> accessed 8 March 2022.

[3] The FSB is an international body which promotes international financial stability. It works with national financial authorities and internationalstandard-setting bodies to recommend supervisory, regulatory, and financial policies. See FSB, "About Us', <https://www.fsb.org/about/> accessed 8 March 2022.

July 2021.[4] If the sector continues to grow outside regulatory frameworks, the vulnerabilities and risks emanating from the markets may have consequences for the broader financial system. Further, DeFi may also crystallise threats emanating from crypto assets (used for DeFi transactions), which may include impacts on financial stability. Therefore, the rapid growth of the DeFi markets warrants attention from market participants and policymakers to promote responsible innovation and avoid the development of a reckless market that may later become too big to regulate.

The purpose of the article is to present an overview of the DeFi ecosystem, examine the risks and opportunities presented by it and study the legal implications of DeFi. The developments in the DeFi sector must be studied in light of the risks to investors, market integrity, security and financial stability. The vision of intermediation without centralisation underlying DeFi services will challenge traditional financial regulation based on centralisation, where the subject of regulation is easily identifiable. Therefore, DeFi may dilute the traditional forms of accountability and the effectiveness of existing financial regulations and their enforcement. To examine the legal and regulatory implications arising from DeFi, it is crucial to analyse the DeFi ecosystem as it currently exists, especially laying emphasis on its integral components. Such an examination will lead to the identification of critical legal and regulatory issues that DeFi poses. Based on such analysis, this article discusses how regulations and policies must respond to these technological innovations.

Against this background, the article is structured as follows. *Firstly,* it deconstructs the concept of DeFi along with examining the integral components of the DeFi ecosystem. *Secondly*, the article briefly explains the current DeFi services since a study of such services is important to assess the opportunities and risks presented by such services. In doing so however, the article does not comment on the desirability of such services. *Thirdly*, it identifies key legal and regulatory issues raised by such services and how they may (or may not) fit within the existing financial regulatory architecture. *Finally,* the article concludes with possible policy and regulatory responses to promote responsible innovation in the DeFi ecosystem.

[4] Jamie Crawley, *DeFi Has Accounted for Over 75% of Crypto Hacks in 2021* (*CoinDesk*, 10 August 2021) <https://www.coindesk.com/markets/2021/08/10/defi-has-accounted-for-over-75-of-crypto-hacks-in-2021/> accessed 8 March 2022.

Understanding DeFi

The existing financial system operates through centralised, regulated intermediaries such as banks and financial institutions. Such centralised intermediaries act as agents of trust and provide liquidity, settlement, and security for financial transactions. These intermediaries bring together a range of participants - persons with financial resources (banks, investors) and persons seeking financial resources (borrowers and entrepreneurs). Therefore, traditional finance is marked by the presence of intermediaries "that centralise functions and services."[5] Contrary to this, DeFi envisages a financial system where financial services are provided without reliance on centralised intermediaries through automated protocols (or rules) on DLT and crypto assets to facilitate transactions. DLT is a technological innovation that allows the recording and sharing of information across multiple ledgers. "It allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants."[6]

As the DeFi market continues to evolve, there is no standard definition of decentralised finance. DeFi is broadly used to refer to financial services provided through decentralised financial applications ("**DApps**") that rely on open protocols.[7] As per the International Organization of Securities Commission ("**IOSCO**"), DeFi commonly refers to the "provision of financial products, services, arrangements and activities that use distributed ledger technology ("DLT") in an effort to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions."[8] The Bank for International Settlements ("**BIS**") defines DeFi to mean "financial applications run by smart contracts on a blockchain, typically a permissionless (i.e., public) chain."[9] Most DeFi

[5] Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, 'Decentralized Finance' (*Journal of Financial Regulation, Volume 6, Issue 2*, 20 September 2020) <https://academic.oup.com/jfr/article/6/2/172/5913239> accessed 8 March 2022.

[6] World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain*, (Fintech Note No. 1, 2017) <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 8 March 2022.

[7] David Gogel, *DeFi Beyond the Hype* (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[8] International Organisation of Securities Commission, *IOSCO Decentralised Finance Report* (March 2022) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> accessed 10 April 2022.

[9] Established in 1930, the BIS is owned by 63 central banks, representing countries from around the world. It seeks to support "central banks' pursuit of monetary and financial stability through international cooperation, and to act as a bank for central banks". See BIS, 'About BIS-overview' <https://www.bis.org/about/index.htm> accessed 8 March 2022; Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion* (BIS Quarterly Review, 6 December 2021) <https://www.bis.org/publ/

services are built on the Ethereum blockchain that allows for the creation of 'smartcontracts'. Smart Contracts are automated contracts written as computer code on blockchain ledgers and automatically executed on the happening of pre-defined trigger events in the code.[10]

The DeFi architecture consists of multiple layers, with each layer serving a distinct purpose. Together, these layers create an open, composable and interoperable infrastructure that allows DeFi users to build on or propose changes to the layer.[11] Broadly, the DeFi stack consists of the following layers -the blockchain and token layer, the applications and protocol layer, and the aggregation layer.[12] The base layer consists of the relevant DLT or blockchain layer along with its native protocol that serves as the foundation of the application. Ethereum is the most commonly used blockchain in DeFi applications, and Ether is its native protocol. The protocol layer sets standards for specific use cases such as decentralised exchanges, debt products, derivatives, etc. The standards are implemented by smart contracts and can be accessed by any DeFi participant.[13] Applications are used to create the interfaces through which users interact with these protocols.[14] The aggregation layer enables aggregators to create user-centric platforms that connect to several applications and protocols.[15]

qtrpdf/r_qt2112b.htm> accessed 8 March 2022. OECD, 'Initial Coin Offerings (ICOs) for SME Financing' (2019) <https://www.oecd.org/finance/ICOs-for-SME-Financing.pdf> accessed 8 March 2022.

[10] OECD, 'Initial Coin Offerings (ICOs) for SME Financing' (2019) <https://www.oecd.org/finance/ICOs-for-SME-Financing.pdf> accessed 8 March 2022.

[11] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[12] KPMG, 'Crypto Insights #1. An introduction to Decentralised Finance (DeFi)' (October 2021) <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-1-an-introduction-to-decentralised-finance.pdf> accessed 8 March 2022.

[13] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[14] KPMG, 'Crypto Insights #1. An introduction to Decentralised Finance (DeFi)' (October 2021) <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-1-an-introduction-to-decentralised-finance.pdf> accessed 8 March 2022.

[15] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

DeFi services have unique features that distinguish them from centralised traditional financial services (“**CeFi**”).[16]

- **Non-custodial**: There is no central authority or intermediary in DeFi systems that is responsible for managing the transactions, private keys, funds, or information. Participants control and manage their private keys and crypto assets for executing transactions. This is different from CeFi services, where a regulated intermediary or custodian holds such funds on behalf of the owner. DeFi systems record transaction details on the blockchain, whereas, CeFi systems rely on the private records of intermediaries (such as centralised exchanges and other platforms).[17]

- **Decentralised ownership and governance**: With no centralized responsible authority, DeFi systems tend to rely on the community of participants for creating network effects. There is a semblance of a governance framework in DeFi applications when governance tokens (discussed in detail later) issued by DeFi applications enable token holders to participate in decisions relating to the application. Such holders typically exercise some form of control over the DeFi protocol.[18] The operation of a DeFi application based on blockchain technologies does not automatically qualify a service to be DeFi. For applications to be decentralized, the governance must be community-based without any central authority controlling the system.[19] The BIS argues that “decentralization in DeFi is illusory” as most DeFi applications have an element of centralisation that revolves around the governance token holders who vote on proposals relating to the DeFi protocol.[20] Unlike DeFi services, CeFi services are governed by rules specified by regulators.

[16] FSB, *Assessment of Risks to Financial Stability from Crypto Assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022; David Gogel ‘DeFi Beyond the Hype’ (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022; OECD, Why Decentralised Finance (DeFi) Matters and the Policy Implications (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[17] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, ‘DeFi Risks and the Decentralisation Illusion’ (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/qtrpdf/r_qt2112b.htm> accessed 8 March 2022.

[18] Salami, I. (2021), ‘Challenges and Approaches to Regulating Decentralized Finance’. (*AJIL Unbound*, 115, 425-429) <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/challenges-and-approaches-to-regulating-decentralized-finance/1FC6B3EF8DEE460EF534A1F0A5E9DC72> accessed 8 March 2022.

[19] OECD, ‘Why Decentralised Finance (DeFi) Matters and the Policy Implications’ (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[20] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, ‘DeFi Risks and the Decentralisation Illusion’ (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/

- **Composable:** This feature enables the creation of innovative financial products over DeFi applications, thereby increasing the value proposition of such applications. The open-source nature of DeFi applications enables participants to look at the code and use it to develop new applications. For instance, a DeFi user can lock up her crypto assets in a lending protocol to earn rewards. A user locks up her Ether crypto assets on the MakerDAO application in exchange for DAI stablecoins and the governance tokens of MakerDAO.[21] The user can then pledge the DAI as collateral in another DeFi application.

Building Blocks of Defi

The DeFi system is an extension of the growing crypto asset economy. To understand the regulatory implications of DeFi, it is important to study the conceptual framework of DeFi, its building blocks and the nature of services that DeFi can provide.

DLT and Blockchain: DeFi systems rely on DLT, particularly public and permissionless blockchain, to provide financial services.[22] Broadly, DLT is a database or ledger that is distributed across multiple sites, countries, or entities with no centralized controller.[23] The BIS defines DLT to "refer to processes and related technologies that enable nodes in a network(or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's node."[24] A node is a computer participating in a DLT arrangement. There are different ways to design DLT-based systems. Blockchain is a type of DLT and refers to a particular form of structuring data on a DLT platform.[25] The popular crypto asset "Bitcoin" uses blockchain technology. DLT systems may be of different types based on their design and architecture. Features like "openness" of the platform (public or private) and the level of permissions required to add

qtrpdf/r_qt2112b.htm> accessed 8 March 2022.

[21] 'The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System' <https://makerdao.com/en/whitepaper> accessed 8 March 2022.

[22] FSB, Assessment of Risks to Financial Stability from Crypto Assets (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022.

[23] Leon Perlman, 'Regulation of the Financial Components of the Crypto-Economy' (*School of International and Public Affairs Entrepreneurship & Policy Initiative,* Working Paper Series 2019) <https://sipa.columbia.edu/sites/default/files/25222_SIPA-White-Paper-CE-Regulation-web.pdf> accessed 8 March 2022.

[24] Committee on Payments and Market Infrastructures, BIS, Distributed Ledger Technology in Payment Clearing and Settlement – An Analytical Framework (February 2017) <https://www.bis.org/cpmi/publ/d157.pdf> accessed 8 March 2022.

[25] *Cryptoassets Taskforce, 'Final Report'*, (October 2018), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final _report_final_web.pdf > accessed 8 March 2022.

information to the ledger (permissioned or permissionless) may impact the type of DLT.[26] DLT systems may be public or private depending on whether the ledgers can be accessed by anyone or only by the participating nodes in the network.[27] Further, DLT systems may be permissioned or permissionless based on whether network participants need permission to make changes to the ledger.[28] Ethereum, the popular DeFi blockchain, is a permissionless blockchain where network participants can "join or leave the network at will, without being pre-approved or vetted by any entity."[29] Systems built on decentralised technologies raise legal issues relating to jurisdiction, the applicability of laws, ownership of ledger and liabilities, and compliance with laws. For instance, since the nodes of a decentralised ledger may be spread across multiple jurisdictions, determining which jurisdictions' law applies to a given transaction may often be challenging. Further, in a public permissionless DLT system, several network participants have access to the ledger, and no single entity takes responsibility for the system, including its security. Therefore, it becomes challenging to identify the ownership of the ledger, the entities in control of it, and the legal liabilities in case of default. In many cases, the concept of such decentralised technologies may not be compatible with existing laws. For instance, data protection laws typically require the party controlling an individual's personal data to comply with legal obligations relating to data security and privacy. Identifying the subject of regulation in a permissionless DLT system where transactions may happen on a peer-to-peer basis is often difficult. Similar issues will also arise for compliance with other laws, including laws relating to anti-money laundering. Since decentralised technologies underpin DeFi solutions, many of these legal issues will also arise in DeFi regulation. This article uses the terms DLT and blockchain used interchangeably.

Crypto assets: Crypto assets representing value are often used for DeFi transactions. While there is no globally accepted definition of crypto assets, it may be helpful to refer to the definition provided by FSB, which the BIS and IOSCO have also adopted. FSB defines crypto assets as "a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value."[30] While different

[26] OECD, 'OECD Blockchain Primer' <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf> accessed 8 March 2022.

[27] World Bank Group, 'Distributed Ledger Technology (DLT) and Blockchain', (Fintech Note No. 1, 2017) <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 8 March 2022.

[28] ibid.

[29] ibid.

[30] FSB, 'Work Underway, Regulatory Approaches and Potential Gaps' <https://www.fsb.org/wp-content/uploads/P310519.pdf>, (May 2019) accessed 8 March 2022.

definitions of crypto assets have emerged, common points of convergence include digital representation of value, issued by a private entity, and reliance on DLT.[31]One of the most popular cryptoassets is Bitcoin (BTC) which was designed to operate as a peer-to-peer payment solution without the need for known and trusted third parties. Examples of other popular cryptoassets are Ether (ETH), XRP, and Litecoin (LTC). The regulation of cryptoassets has been a subject of intense policy debate worldwide. Typically, the classification of financial instruments is essential for financial regulation since such classification determines the nature of regulations that will apply to such instruments. Unfortunately, there appears to be no consensus on the classification of cryptoassets. While certain features may be common for all cryptoassets (such as its underlying decentralised technology), there is no uniformity in its use cases and the players involved. Therefore, it is difficult to pigeonhole such cryptoassets as a single type of financial instrument. For instance, a crypto asset may exhibit features of a payment token (primarily meant for facilitating payments) or a utility token (a payment token that allows access to a service or product provided by the token's issuer). It has been pointed out that crypto assets that may be used for multiple use cases (often referred to as "hybrid token") may raise regulatory challenges if laws seek to make a strict demarcation between different types of crypto assets.[32]. Further, certain crypto assets like Bitcoin do not have any underlying asset, whereas the value of stablecoins (as discussed below) are backed by an underlying asset. The difficulty in categorising crypto assets under traditional laws and asset classes and its pseudonymous nature with a global nature (that can blur geographical boundaries) creates challenges in designing regulations for crypto assets and enforcing them. Such features discussed above and the potential ability of some crypto assets (such as privacy coins) to mask the identity of users and transactions heighten concerns of regulators around its misuse for money laundering and financial crimes.[33] In many countries, including India, crypto assets remain unregulated without checks and balances, exposing

[31] Shehnaz Ahmed, Swarna Sengupta, 'Blueprint of a Law for Regulating Cryptoassets' (*Vidhi Centre for Legal Policy*, 29 January 2022) <https://vidhilegalpolicy.in/research/blueprint-of-a-law-regulating-cryptoassets/> accessed 8 March 2022.

[32] Prof. Dr Houben R., Snyers A., 'Crypto-assets – Key Developments, Regulatory Concerns and Responses' (Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf> accessed 10April 2022.

[33] IMF, 'The Crypto ecosystem and the Financial Stability Challenges', (October 2021) <https://www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx#:~:text=Challenges%20posed%20by%20the%20crypto%20ecosystem%20include%20operational%20and%20financial,and%20disclosure%20for%20some%20stablecoins.>> accessed 10 April 2022.

investors and the financial system to multiple risks. Therefore, the regulatory response to crypto assets is also important for monitoring the DeFi market.

Stablecoins: Stablecoins are a type of crypto asset whose value is pegged to an asset or commodity. Crypto assets such as Bitcoin and Ether have been infamous for the volatility in their prices. In April 2021, Bitcoin's value touched USD 65,000, followed by a drop of 50% later in the year due to events such as the announcement of a ban by China.[34] To deal with volatility risks associated with crypto assets, stablecoins seek to "maintain a stable value relative to a specified asset, or a pool or basket of assets."[35] Tether (USDT), USD Coin (USDC) and Dai (DAI) are some popular stablecoins. For instance, every Tether token is "1-to-1 pegged to the dollar."[36] Stablecoins may be broadly classified as asset-linked stablecoins and algorithm-based stablecoins based on their stabilisation mechanism.[37] The value of asset-linked stablecoins is linked to assets such as a single fiat currency, basket of currencies, commodities or even crypto assets. Algorithm-based stablecoins rely on an algorithm to maintain a stable value by increasing or decreasing the supply of stablecoins in response to changes in demand.

Stablecoins play an important role in the DeFi ecosystem by facilitating funds transfer between platforms and users. Many stablecoins are "off-chain" stablecoins. They are asset-backed stablecoins that "require a custodian for their safekeeping and are in possession of the issuer of the stablecoins as long as the user does not redeem the stablecoins."[38] DeFi transactions tend to rely on "on-chain" stablecoins that are stablecoins backed by assets which are "recorded in a decentralised manner and do not need either an issuer or a custodian to satisfy a claim".[39] To deal with the volatility of

[34] Damanick Dantes, *Volatility Ruled Crypto Markets in 2021, From $69K Bitcoin to Elon Musk's 'Dogecoin to the Moooonn'* (*CoinDesk*, 1 January 2022) <https://www.coindesk.com/markets/2021/12/31/volatility-ruled-crypto-markets-in-2021-from-69k-bitcoin-to-elon-musks-dogecoin-to-the-moooonn/> accessed 8 March 2022.

[35] FSB, *Addressing the Regulatory, Supervisory and Oversight Challenges Raised by "Global Stablecoin" Arrangements; Consultative Documents* (April 2020) <https://www.fsb.org/wp-content/uploads/P131020-3.pdf> accessed 8 March 2022.

[36] Tether', <https://tether.to/> accessed 8 March 2022.

[37] FSB, Regulation, *Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations* (October 2020) < https://www.fsb.org/wp-content/uploads/P140420-1.pdf> accessed 8 March 2022.

[38] European Central Bank, 'Stablecoins –No Coins, but are They Stable?' (Issue no 3, November 2019) <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191128.en.pdf> accessed 8 March 2022.

[39] ibid.

the underlying crypto assets, DeFi stablecoins rely on an over-collateralised pool of crypto assets.[40]

The rise of stablecoins raises concerns about its impact on the financial system and its stability. The FSB notes that widely adopted stablecoins with reach and use across multiple jurisdictions (also known as global stablecoins) could pose systemic risks.[41] In such a case, prudential regulation of stablecoin arrangements is important. Considering that various DeFi transactions rely on stablecoins, understanding regulatory issues arising from stablecoins is important. Currently, there is variation in the process of redemption of different stablecoins. This includes variance regarding the person who may present a stablecoin for redemption, the limit on the number of stablecoins that maybe redeemed and the presence of any right against the issuer.[42] There are also concerns regarding the accuracy of disclosures made by such issuers. Stablecoin regulation raises important issues for consideration such as eligibility of issuers, exposure of banks and financial institutions to such stablecoins, redeemability of such stablecoins, provisions on governance arrangements, market integrity, consumer and investor protection, anti-money laundering framework, provisions to deal with resolution or winding down of such arrangements, etc.

Smart Contracts: To effectuate transactions, DeFi systems use open protocols and DApps.[43] These protocols and DApps are powered by smart contracts—programs built on existing blockchains that automatically execute all or certain parts of an agreement when certain pre-defined conditions are met.[44] The idea of smart contracts was envisaged by computer scientist, and cryptographer Nick Szabo who used the example of a vending machine to

[40] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, 'DeFi Risks and the Decentralisation Illusion' (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/qtrpdf/r_qt2112b.htm> accessed 8 March 2022.

[41] FSB, Regulation, *Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations* (October 2020) <https://www.fsb.org/wp-content/uploads/P131020-3.pdf > accessed 14 January 2022

[42] President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, 'Report on Stablecoins', (November 2021), <https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf> accessed 18 January 2022.

[43] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[44] Stuart D. Levi and Alex B. Lipton, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance*, 26 March 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 8 March 2022.

argue that many agreements could be "Many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make a breach of contract expensive (if desired, sometimes prohibitively so) for the breacher."[45] Today, smart contracts may ensure payment of funds upon the happening of trigger events identified in the code. It replaces the intermediary role of centralised financial institutions with automated protocols built into a blockchain. Smart contracts may take different forms with different levels of automation. To a certain extent, existing legal frameworks recognise electronic contracts; therefore, it has been argued that courts may recognise codes that execute provisions of a smart contract.[46] However, the United Kingdom Law Commission notes that as the level of automation in a contract increases and where the entire life cycle of contract formation solely exists on DLT systems with no negotiations in "natural language", it may give rise to novel legal issues about formation, interpretation, remedies and jurisdiction of contracts.[47] For instance, it notes that when parties enter into an agreement in "natural language", which is then performed by a computer code, it will not be difficult to prove that the parties intended to enter into legal relations. However, if an agreement between parties is due to their interaction on a DLT system, challenges may arise in inferring intention, willingness and consent to enter into a contract. Challenges may also arise in the determination of the jurisdiction and the applicable laws in case nodes are spread across different jurisdictions. Even if one argues that smart contracts can be accommodated within the ambit of existing contract law, the major challenge is the disconnect between the operation of smart contracts and the manner in which parties transact business. Typically, most contracts have a provision for amendment or rectification of contractual provisions, which may be challenging where terms are coded on an immutable ledger. Further, smart contracts may not provide the flexibility necessary in contract performance. For instance, such contracts may not be able to take into common contractual terms of substantial performance such as "best efforts", "reasonable care", or "reasonable time".

[45] Nick Szabo, 'The Idea of Smart Contracts' (1997) <https://nakamotoinstitute.org/the-idea-of-smart-contracts/> accessed 9 August 2022.

[46] Stuart D. Levi and Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance*, 26 March 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 10 April 2022.

[47] Law Commission, 'Smart Legal Contracts Summary' (2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final.pdf> accessed 10 April 2022.

Governance tokens: As discussed above, the governance of the DeFi protocol is based on voting by governance token holders. Such tokens confer voting rights on token holders to manage changes to smart contracts or other DeFi protocols.[48] Such token holders can vote on "proposals relating to upgrades, changes in the mechanisms underlying the protocol, introduction of additional stablecoins for trading, change in the level of collateralisation or fees."[49] These tokens are tradeable on certain crypto exchanges.[50] Such tokens incentivise activity in DeFi ecosystems and allow developers to cede more control over DeFi protocols to token holders. The rights associated with the governance tokens will help analyse who controls the system's activities. One of the earlier governance tokens was the MKR token issued by MakerDAO, as explained below, which gives the token holder voting rights.

Types of Services provided by Defi

The previous section presents a conceptual framework of DeFi and its ecosystem. However, it is also important to examine the manifestation of such services in the real economy. This examination is relevant to assess the opportunities and risks presented by DeFi services and accordingly determine appropriate policy response.

A recent paper by the Organisation for Economic Co-operation and Development ("**OECD**") notes that lending is one of the fastest growing DeFi products, followed by other products such as decentralised exchanges, derivatives, asset management, insurance and payments.[51] Such transactions are collateralised by crypto assets, both stablecoins and different types of unbacked crypto assets. Use cases of DeFi are still evolving. While proponents argue about its potential to create more efficiencies for the financial system, sceptics often question its real economy utility and scalability. The BIS notes that while DeFi may complement traditional financial services, at present, "it has few for the real economy and, for the most part, supports speculation and arbitrage across multiple crypto assets".[52] While DeFi ser-

[48] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[49] OECD, 'Why Decentralised Finance (DeFi) Matters and the Policy Implications' (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[50] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>accesrsed 8 March 2022.

[51] OECD, 'Why Decentralised Finance (DeFi) Matters and the Policy Implications' (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[52] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, 'DeFi Risks and the Decentralisation Illusion' (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/

vices may not be very different from the services provided by CeFi systems, it seeks to change how CeFi services are provided.

Lending: Decentralised loan platforms do not require borrowers or lenders to identify themselves. "Everyone has access to the platform and can potentially borrow money or provide liquidity to earn interest. As such, DeFi loans are completely permissionless and not reliant on trusted relationships."[53] DeFi lending activities rely extensively on collaterals. Typically, users provide liquidity to the platform by locking their crypto assetsas collaterals and receiving rewards (such as tokens native to the platform) for providing liquidity to the system. This is similar to interests earned on deposits with banks. The rates at which users are rewarded are based on the demand and supply of liquidity rather than the creditworthiness of the borrower.[54] DeFi borrower scan access locked up crypto assets from the pool by payment of a fee.[55] Common mechanisms used by DeFi systems to provide loans include lock-up yields that "pays interest for immobilizing digital assets in pools, where they serve as liquidity or collateral for a DeFi service" or liquidity mining "that pays the interest in the form of tokens issued by the DeFi service itself."[56] For instance, MakerDAO is a popular DeFi service provider. MakerDAO is "an open-source project on the Ethereum blockchain and a Decentralized Autonomous Organization, " managed by a community of participants around the world holding its governance token MKR.[57] This DeFi system is based on atwo-token model - MKR governance token and Dai stablecoin. Dai is a collateral backed stable coin built on the Ethereum blockchain whose value is pegged to the US Dollar.[58] The Maker protocol is one of the largest DApps on the Ethereum blockchain.[59] The protocol allows anyone to deposit collateral (which can be in the form of crypto assets) into a Maker Vault (which is a "smart contract that escrows collateral and keeps

qtrpdf/r_qt2112b.htm> accessed 8 March 2022.

[53] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets* (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[54] OECD, 'Why Decentralised Finance (DeFi) Matters and the Policy Implications' (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[55] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[56] ibid.

[57] 'The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System' <https://makerdao.com/en/whitepaper#abstract> accessed 8 March 2022.

[58] 'What is Dai?' <https://makerdao.world/en/faqs/dai> accessed 8 March 2022.

[59] 'The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System' <https://makerdao.com/en/whitepaper#abstract> accessed 8 March 2022.

track of the USD-denominated value of the collateral") in return for a "loan" in a Dai stablecoin.[60] Users are required to over-collateralize their positions to open a Maker Vault, and if the value of the collateral falls below a specified threshold, the Vault is liquidated. The borrower must repay the Dai along with interest to retrieve the collateral.[61] MKR tokens grant governance rights to the token holders over the Maker protocol.[62] This may include the right to vote to set the interest rate, collateralization ratio, allowable collateral types, and other attributes.[63]

Unlike traditional lending platforms, DeFi lending platforms bring prospective borrowers and lenders together without a central intermediary such as a bank. Another key difference between traditional and DeFi lending is that there is limited ability to screen or assess the creditworthiness of borrowers in DeFi lending. Typically, the identity of the parties is "hidden behind cryptographic digital signatures", making it difficult to examine the credit information of borrowers.[64]Therefore, DeFi lending is heavily dependent on collaterals. Through smart contracts, platforms fix a margin determining the amount of collateral a borrower must pledge to receive a loan. As discussed, since cryptoassets are provided as collaterals, which tend to have fluctuating value, there tends to be over-collaterisation. To protect the interests of the lender, platforms set a "liquidation ratio" relative to the borrowed amount.[65] Typically, when the collateral falls below the liquidation ratio, the platform will allow anyone to "act as liquidator and seize the collateral, repay the lender and pocket a share of the residual collateral."[66] Interestingly, in DeFi lending transactions, the lender does not exercise the ultimate right to liquidate a loan, and the liquidation decision is dependent on the value of the collateral.

Decentralised Exchanges: Crypto assets can be traded using both centralised and decentralised exchanges. Centralised exchanges (such as Coinbase and Binance) work like CeFi services where a single authority manages the

[60] Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro, *DeFi and the Future of Finance* (Wiley 2021) 39.

[61] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[62] Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro, *DeFi and the Future of Finance* (Wiley 2021) 39.

[63] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[64] Sirio Aramonte, Sebastian Doerr, Wenqian Huang and Andreas Schrimpf, 'DeFi Lending: Intermediation Without Information?' (*BIS Bulletin No, 57,* 14 June 2022) <https://www.bis.org/publ/bisbull57.pdf > accessed 08 August 2022.

[65] ibid.

[66] ibid.

platform and facilitates the transaction. To trade on a centralised exchange, traders must deposit assets with the exchange, forfeit direct access to their assets, and trust the exchange operator.[67] Decentralised exchanges are not owned or operated by one entity. They use "automated liquidity pools, where investors 'lock' in their crypto assets (in exchange for fees) to facilitate trading".[68] DeFi exchanges avoid taking custody of user assets.[69] Users remain in exclusive control of their assets until the trade is executed. Trade execution happens through a smart contract. Depending on the design of the exchange, the smart contract may assume additional roles, "effectively making many intermediaries such as escrow services and central counterparty clearing houses (CCPs) obsolete".[70] For instance, Uniswap is a popular decentralised exchange that relies on smart contracts that define a standard way to create liquidity pools, provide liquidity, and swap crypto assets."[71] There is no central order book, no third-party custody, and no private order matching engine.[72]

Assessing Opportunities and Risks Presented by DeFi

DeFi services seek to provide efficiencies by enabling the transfer of value through automated processes without the reliance on intermediaries. Such disintermediation and automation in the financial system may lead to "faster, potentially cheaper and frictionless transactions".[73] Automating processes using smart contracts may also be helpfulin reducing costs associated with issuance, administration, and execution of transactions. To a certain extent, DeFi enables the realisation of value propositions presented by DLT. The FSB notes that decentralised technologies may reduce some of the financial

[67] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets* (2021) Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[68] FSB, *Assessment of Risks to Financial Stability from Crypto-assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022.

[69] David Gogel 'DeFi Beyond the Hype' (May 2021) <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> accessed 8 March 2022.

[70] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets* (2021) (*Second Quarter 2021, Vol. 103, No. 2 Federal Reserve Bank of St. Louis Review*) <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> accessed 8 March 2022.

[71] 'Frequently Asked Questions' <https://uniswap.org/faq> accessed 8 March 2022.

[72] ibid.

[73] OECD, *The Tokenisation of Assets and Potential Implications for Financial Markets* (17 January 2020) <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf> accessed 8 March 2022.

stability risks associated with traditional financial institutions and intermediaries.[74] The growth of financial service providers could increase the diversity in the financial system and reduce concentration risks. Further, DLT-based DeFi systems could reduce the reliance on existing intermediaries to "channel short-term funding into lending, thereby reducing solvency and liquidity risks arising across their balance sheets."[75] The extent to which such benefits are realised depends on the degree of decentralisation. Further, the decentralisation of records / information in DLT-based DeFi systems may be more resilient as there is no single point of failure or attack found in CeFi services. Proponents often argue about the potential of DeFi to provide better access to financial services, primarily in countries where the depth and breadth of the financial system are not well developed. [76] DeFi services enable users to access services without reliance on traditional intermediaries, and its composable nature enables the development of innovative products that are better suited to meet the needs of the customer. However, such a broad claim may be an overstretch given that developing and underdeveloped economies often face infrastructure and financial literacy challenges, which could be the biggest impediment for their citizens to use such services. However, DeFi services may complement CeFi services by providing small businesses with an alternative to transact outside the traditional banking and payment systems. Small businesses could use major DeFi exchanges to make direct payments, convert payment amounts to USD-backed stablecoin for cross-border remittances, or use DeFi lending protocols for financing.[77] Most of the benefits associated with such services broadly emanate from the value proposition of the underlying technology, i.e., DLT. As the DeFi space is still evolving, it is difficult to predict if these purported benefits will be achieved at a large scale and, if yes, whether they will outweigh the potential risks discussed below.

[74] FSB, *Assessment of Risks to Financial Stability from Crypto-assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022.

[75] FSB, *Decentralised Financial Technologies* (6 June 2018) <https://www.fsb.org/wp-content/uploads/P060619.pdf> accessed 8 March 2022.

[76] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022; Rebecca Liao 'How Decentralized Finance Will Transform Business Financial Services – Especially for SMEs' (*World Economic Forum*, 19 July 2021) <https://www.weforum.org/agenda/2021/07/decentralized-finance-transaction-banking-smes/> accessed 8 March 2022.

[77] Rebecca Liao 'How Decentralized Finance Will Transform Business Financial Services – Especially for SMEs' (World Economic Forum, 19 July 2021) <https://www.weforum.org/agenda/2021/07/decentralized-finance-transaction-banking-smes/> accessed 8 March 2022.

DeFi systems give rise to several risks, including regulatory, operational, investor protection, and systemic risks. Some of these risks are inherent to DLT systems, others such as crypto assets being peculiar to DeFi services. Increased activity in the DeFi sector without regulatory oversight has increased the likelihood of bad actors misusing these developments for fraudulent and illegal activities. There have been numerous reports of DeFi-related scams such as exit schemes and rug pulls, Ponzi schemes, and other fraudulent schemes and theft of private keys.[78] Due to their peculiar characteristics facilitated by crypto assets and DLT, the DeFi system enables such "rug pulls" or "exit schemes". This involves convincing users to place their funds in seemingly legitimate DeFi services, which are then fraudulently withdrawn by developers or influencers promoting such schemes, leaving no recourse for the investor.[79] It has been reported that investors were scammed of around $2.8 billion worth of crypto assets in 2021, through rug pull schemes that accounted for 37% of all crypto asset scams revenue in 2021 as compared to 1% in 2020. There are also reports of crypto assets worth $80 million being stolen from a decentralised finance platform in 2022.[80] Without any regulatory oversight over DApps or crypto assets, there are no standards for risk management or capital reserves. There are no transparency requirements, and most investors do not know how their money is being handled, exposing them to newer kinds of risks facilitated by DeFi services.

Given the decentralised nature of such services, the DeFi ecosystem operates outside the regulatory frameworks of most countries. In many cases, DApps may provide services similar to traditional financial services yet remain outside the regulatory perimeter, putting users at risk. For instance, in the case of DeFi lending, as discussed above, many applications arguably provide banking / lending services,i.e., accepting deposits and rewarding the deposit holders (i.e., users that lock crypto assets with the application to provide liquidity) and then lending them.It is argued that such deposit activities in return for a fixed or variable return may also constitute "issuance of a

[78] International Organisation of Securities Commission, *IOSCO Decentralised Finance Report* (March 2022) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> accessed 9August 2022.

[79] World Economic Forum, *Decentralised Finance (DeFi) Policy-Maker Toolkit* (June 2021) <https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf> accessed 09 August 2022.

[80] *Rug Pull Scams Accounted for the Highest Scam Revenue at $2.8 Billion in 2021: Report* (*Financial Express,* 27 May 2022) <https://www.financialexpress.com/digital-currency/rug-pull-scams-accounted-for-the-highest-scam-revenue-at-2-8-billion-in-2021-report/2539575/> accessed 08 August 2022; 'Hackers Steal $80 Million Worth of Crypto from DeFi Platform Qubit Finance', (The Indian Express, 29 January 2022) <https://indianexpress.com/article/technology/crypto/hackers-steal-80-million-worth-of-cryptocurrency-from-defi-platform-qubit-finance-7747355/> accessed 09 August 2022.

debt instrument or an investment contract that may involve offers and sales of securities" in some jurisdictions.[81] While banks and non-bank companies providing financial intermediation are heavily regulated, both from a prudential and conduct perspective, the DeFi applications remain outside the regulatory perimeter. This gives rise to financial risks and risks to investor protection.

The lack of regulatory safeguards for investor protection leaves investors and financial consumers exposed to newerforms of loss. For instance, there is an absence of recourse in case of unauthorised transactions, lack of recovery or resolution mechanism and market manipulation. In many cases, the average retail customer may not understand the risks emanating from DeFi services due to the lack of information or the technical complexities involved in such services. This exposes retail users to liquidity and credit risks. In case of default or fraud, no credible recourse is available to such users. In most cases, it is often difficult to identify a responsible party to turn to for such defaults. Further, there is no mechanism through which losses may be recovered, exposing participants to complete loss of funds invested in case of a default.

Due to their pseudonymous nature with a global reach through digital means, DeFi services may facilitate money laundering, financing of terrorism and tax evasion. As they operate outside regulatory frameworks, DeFi services are not mandated to comply with anti-money laundering laws, which require financial service providers to undertake customer due diligence and report suspicious transactions to regulators. Without such verifications and checks, anyone with the necessary infrastructure can use DApps and avail DeFi services.[82] DeFi services offer much greater anonymity to users than CeFi services.[83] The non-custodian nature of DeFi allows for pseudonymous participation of users in DeFi, as they do not need to go through a regulated or custodial service provider. DeFi participants can remain fully anonymous or pseudonymous without any link to their identity and information

[81] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[82] Salami, I. (2021), 'Challenges and Approaches to Regulating Decentralized Finance'. (*AJIL Unbound, 115, 425-429*) <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/challenges-and-approaches-to-regulating-decentralized-finance/1FC6B3EF8DEE460EF534A1F0A5E9DC72> accessed 8 March 2022.

[83] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, 'DeFi Risks and the Decentralisation Illusion' (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/qtrpdf/r_qt2112b.htm> accessed 8 March 2022.

about the source of funds.[84] Therefore, while DeFi transactions are traceable and verifiable on the chain, they are anonymous or pseudonymous, without recourse to find out the participant's identity. News reports indicate that DeFi protocols are playing an increasing role in money laundering, with the total value of cryptocurrency laundered rising year over year by 30% in 2021 and DeFi protocols receiving $900 million from illicit addresses in 2021, a 1,964% increase in value from 2020.[85]

DeFi services that rely on volatile cryptoassets may heighten the risks for retail consumers, exposing them to financial loss. Further, hacks are also common in such marketplaces. In 2021, Poly Network, a DeFi platform, was hit by a major attack where hackers stole more than $ 600 million worth of digital assets.[86] In August 2021, it was reported that around 75% of crypto hacks occurred in the DeFi space.[87] It has been pointed out that while DeFi services rely on DLT systems where information is recorded in a decentralised manner, participants typically use identical technology / computer code. Technological advances may "threaten the cryptographic underpinnings of DLT, raising concerns about operational risks.[88]

In its recent report, the FSBalso highlights potential risks to financial stability from unregulated DeFi markets.[89] The sector has already seen numerous operational and cybersecurity incidents and failures of governance. With the expansion of the sector, these risks are likely to become more pronounced. Further, DeFi may also increase risks to financial stability from cryptoassets as many services rely on such cryptoassets. While the crypto asset industry is still small compared to the global ecosystem, it is often feared that as the ecosystem and the interconnectedness of the crypto ecosystem with CeFi grows, it could have implications for global financial stability.[90]

[84] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[85] Mengqi Sun, *DeFi Increasingly Popular Tool for Laundering Money, Study Finds* (*The Wall Street Journal,* 26 January 2022) <https://www.wsj.com/articles/defi-increasingly-popular-tool-for-laundering-money-study-finds-11643202002> accessed 8 March 2022.

[86] Ryan Browne, 'Hacker Behind $600 Million Crypto Heist Returns Final Slice of Stolen Funds' (*CNBC,* 23 August 2021) <https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html> accessed 8 March 2022.

[87] Jamie Crawley, *DeFi Has Accounted for Over 75% of Crypto Hacks in 2021* (*CoinDesk,* 10 August 2021) <https://www.coindesk.com/markets/2021/08/10/defi-has-accounted-for-over-75-of-crypto-hacks-in-2021/> accessed 8 March 2022.

[88] FSB, *Decentralised Financial Technologies* (6 June 2018) <https://www.fsb.org/wp-content/uploads/P060619.pdf> accessed 8 March 2022.

[89] FSB, *Assessment of Risks to Financial Stability from Crypto-assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022.

[90] ibid.

Technological and operational risks are also associated with such services. Like DLT, DeFi services are also still evolving. It has been pointed outthat audits and due diligence processes are not common in such a market since governance is decentralised with no clear accountability.[91] Further, regulators run the risk of reputational risk and loss of public confidence in the financial system if DeFi services lead to substantialinvest or losses and fraud.

It is evident from the aforesaid that DeFi services tend to complement existing financial services. However, in most cases, it relies on crypto asset speculation and arbitrage, heightening concerns about the risks to users of such customers. While currently, there may be limited real economy use cases of such services, the potential of such a market to proliferate without any regulatory scrutiny requires immediate consideration. Accordingly, even in India, the Working Group on Digital Lending constituted by the Reserve Bank of India ("RBI") has recommended that RBI study the risks presented by DeFi to determine an appropriate policy response.[92]

DeFi raises Important Legal Issues

The DeFi market is still evolving, with new cases being explored by market participants. The preceding sections highlight the potential opportunities and risks associated with DeFi services. By enabling the provision of financial services without the involvement of multiple intermediaries, DeFi systems may have the potential to bring in more efficiencies in the speed of execution and costs of transactions. However, DeFi services also give rise to several risks and challenges for participants and the markets, which call for policy and legal consideration. While some of the challenges may be common with CeFi services, given the unique characteristics of DeFi services, such challenges may become more pronounced. Risks associated with the crypto asset market and DLT based applications also tend to flow to DeFi markets. It has been pointed out that DeFi may undermine the rule of law by posing a "challenge to state-based systems, in that in its strong form (as fully decentralized finance), it seeks to eliminate the role of the state as rule-maker and enforcer."[93] The decentralized nature of DeFi services brings unique challenges for

[91] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[92] RBI, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (18 November 2021) <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF> accessed 10 April 2022.

[93] Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, *Decentralized Finance* (*Journal of Financial Regulation, Volume 6, Issue* 2, 20 September 2020) <https://academic.oup.com/

regulators to design regulations for such servicesand also enforce such regulations. This section highlights key legal issues that regulators arelikely to face while designing regulatory and policy frameworks for DeFi markets.

Identifying the entities for regulation: In the case of CeFi services, the financial regulatory framework tends to focus on regulating the specific entities that provide such services. Even financial regulatory frameworks envisaged for newer intermediaries like payment gateways or aggregators focus on centralised systems. Therefore, existing regulations have centralised financial intermediaries at the core and oversight of the provision of CeFi services is regulated through licensing, registration and regulation of such intermediaries. The presence of intermediaries carrying out such functions is contrary to the concept of DeFi. Given the decentralised and community-driven nature of DeFi services, it is often challenging to identify an entity or individual accountable for meeting regulatory obligations. This makes an oversight, attribution of liability and imposition of reporting or disclosure requirements, which have often formed the bedrock of conduct regulation of financial intermediaries, extremely challenging. Further, the composable feature of DeFi services heightens concerns related to supervision and enforcementdue to the complexity of products and services developed on the top of the layers, which makes it difficult to assess the operator of such products or services. Even when operators or intermediaries can be identified, they may lack the ability to modify DeFi protocols or stop transactions because of the decentralised nature of the protocols. While existing DApps are not entirely decentralised, going forward, if a DeFi platform is completely decentralised, no single person or entity could be held responsible for the functioning or malfunctioning of the protocol.[94] Developers do not claim responsibility, and it will be difficult to attribute liability to a specific entity when transactions are anonymous or pseudonymous. This challenges the existing regulatory architecture, which seeks to regulate entities. Further, even if regulations are designed, examining the entities against which regulators should proceed will be challenging.

Investor and financial consumer risks: In traditional financial systems, the interests of investors are sought to be protected through various means, including conduct and prudential regulation. In addition to ensuring that regulated entities are financially prudent, regulators also ensure that there is a disclosure of information to consumers about risks, rights and liabilities associated with the services. This is critical for retail investors / customers

jfr/article/6/2/172/5913239> accessed 8 March 2022.

[94] FSB, *Assessment of Risks to Financial Stability from Crypto-assets* (16 February 2022) <https://www.fsb.org/wp-content/uploads/P160222.pdf> accessed 8 March 2022.

to make an informed decision to avail of such services. However, in the case of DeFi services, transparency around the DeFi protocols and underlying blockchains may not translate into customer or investor awareness of financial riskssince an average retail customer or investor may not have the requisite level of technological and financial literacy to assess the risks associated with the service.[95] Further, in the absence of any entity responsible for the system's management and governance, designing rights and determining liabilities in case of investor loss will be challenging. Such a framework is critical for issues relating to dispute resolution, unauthorised transactions, breaches of customer data, etc.

For instance, as discussed above, DeFi lending is heavily based on the value of the collateral (typically highly volatile cryptoassets). Even the decision to liquidate a loan can be taken by anyone the moment the collateral falls below a certain threshold. Therefore, the lending relationship does not have much value, and the system is collateral driven. The pseudo-anonymous nature of such services means that the identity of the parties is hidden, and there is no scope for assessing the creditworthiness. Being highly asset driven with no ability to screen borrowers, it does not present much innovation potential for solving problems relating to underserved customer segments. While there are measures to protect the interests of lenders, as discussed earlier, it may also be useful to design common standards for the protection of interests of parties involved in such transactions, including standards for assessing the value and nature of collaterals, robust mechanisms for loan recovery, examining possibilities of designing products specifically to serve underserved customer segments who may not have enough assets to present as collaterals, dispute resolution mechanisms, etc.

Jurisdiction and applicable laws: In DeFi services, determining the jurisdiction of courts and applicable law is challenging. Unlike regulated CeFi services, which may be provided within specific territorial limits (unless otherwise authorised), DeFi services are not confined to geographical boundaries. In the case of distributed ledgers such as Ethereum, which is used for DeFi services, the nodes of the ledger may spread across multiple locations. This may make identifying the applicable law to a DeFi service challenging. A single transaction may involve multiple parties operating in different jurisdictions. There is a risk that DeFitransactions carried through DLT could fall under the law of every jurisdiction in which a node in the DLT network is situated, resulting in an overwhelming number of laws that might apply to

[95] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

such transactions.[96] In the absence of international cooperation and coordination, such an interpretation will give rise to a potentially fragmented regulatory framework that may not be able to address DeFi risks. It will also lead to inefficient regulation, increasing risks of regulatory arbitrage and gaps.[97]

Data Protection and privacy: Decentralisation means that data is accessible at many points rather than one. This may have implications for data protection laws. For instance, in a permissionless public blockchain system, there is no single responsible party, and several participants will have access to the data on the network. In the case of personal data, such a structure conflicts with the design of data protection laws that require an entity controlling the personal data of an individual to safeguard the security and privacy of that data by adhering to accepted data protection principles.[98] For instance, under the European Union General Data Protection Regulation and the proposed data protection law in India, different obligations are envisaged for an entity that determines the purposes and means of processing personal data and entities that are responsible for processing personal data on behalf of the controller. This makes it important to determine the activities of entities in a DeFi ecosystem vis-à-vis the personal data of users. However, the unique characteristics of DeFi services and the different types of blockchains that such services rely on will make it challenging to determine such activities of entities, which in turn makes it difficult to apply data protection principles to such services.

Smart Contracts: Legal issues are also likely to arise with the adoption of smart contracts that are the foundation of DeFi services. As discussed above, when the entire lifecycle of a contract formation happens on DLT systems without any real-world negotiation, it will raise issues relating to the formation, interpretation, performance, remedies and jurisdiction of contracts under the existing contract law. Further, as discussed above, smart contracts may not afford parties with such flexibility as required for commercial transactions.

[96] John Salmon and Gordon Myers, 'Blockchain and Associated Legal Issues for Emerging Markets' (January 2019) <https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F> accessed 8 March 2022.

[97] Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, *Decentralized Finance* (*Journal of Financial Regulation, Volume 6, Issue 2,* 20 September 2020) <https://academic.oup.com/jfr/article/6/2/172/5913239> accessed 8 March 2022.

[98] ibid; John Salmon and Gordon Myers, 'Blockchain and Associated Legal Issues for Emerging Markets' (January 2019) <https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F> accessed 8 March 2022.

Enforcement: Even if regulations are designed for DeFi services, enforcing such regulations will be challenging. Existing financial regulatory approaches tend to focus on the entity providing the service, the customer to whom such service is provided or the market in which such service is provided. Identifying each of these components is problematic in a DeFi ecosystem. As discussed above, in a network economy, there are multiple entities providing different parts of the service, to clients spread across the globe. It has already been discussed how it is difficult to identify the entity that may be held accountable or responsible for the provision of DeFi service in question. In the case of CeFi services, another approach that regulators have used to regulate entities that provide ancillary services across the lifecycle of a transaction is through outsourcing guidelines. Such an approach relies on the regulated entity to ensure compliance with regulations by service providers. Even if such an approach is contemplated for DeFi services by fixing liability on a specific entity which is then made liable for other actors, a question that may arise is if a supervised entity can be held responsible for the actions or inactions of multiple network participants spread across the world and subject to different applicable laws.[99]

Way Forward and Conclusion

With improvements in blockchain technologies, tokenisation of financial assets and suitable regulations for safeguarding the interests of users and the financial system, DeFi services may play an important role in the financial system. As DeFi services are still evolving, regulators and policymakers across the globe are trying to assess the opportunities and risks presented by DeFi. For the time being, regulatory focus has been on specific building blocks or elements of decentralised finance, as discussed below. Going forward, it will be useful to focus on the following aspects of regulation to promote responsible innovation in the DeFi markets and mitigate risks that emanate from the sector.

First, the regulation of DeFi is closely connected to the regulation of cryptoassets. Currently, the approaches to crypto asset regulation are fragmented across the world. Broadly, approaches adopted globally may be categorised under three broad heads.[100] Under the first approach, regulators rely on

[99] Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, *Decentralized Finance* (*Journal of Financial Regulation, Volume 6, Issue* 2, 20 September 2020) <https://academic.oup.com/jfr/article/6/2/172/5913239> accessed 8 March 2022.

[100] Shehnaz Ahmed, Swarna Sengupta, 'Blueprint of a Law for Regulating Cryptoassets' (*Vidhi Centre for Legal Policy*, 29 January 2022) <https://vidhilegalpolicy.in/research/blueprint-of-a-law-regulating-cryptoassets/> accessed 8 March 2022.

existing laws (such as securities law) to clarify their applicability to certain types of crypto assets, primarily security tokens issued during an initial coin offering. This includes clarifications issued by the United States Securities and Exchange Commission and the Australian Securities and Investment Commission.[101] .Under the second approach, regulators amend existing laws (mostly anti-money laundering laws) to bring cryptoasset related services within its ambit. For instance, South Korea has amended its Act on Reporting and Using Specified Financial Transaction Information Act 2001 to define "virtual assets" and to bring "virtual asset providers" within the ambit of the law.[102] The third approach is to adopt a standalone bespoke law to regulate crypto assets. In 2021, the Council of European Union adopted its position on the draft Regulation on Markets in Crypto Assets (MiCA) - a framework governing issuance and provisions of crypto asset related services.[103] Previously, Malta and Thailand have also enacted standalone frameworks for crypto assets.[104] It has been pointed out that existing laws are not designed to capture different types of crypto assets, and accordingly, the first two approaches may not be adequate to address all risks emanating from the crypto sector. Going forward, it may be useful to enact a bespoke regulatory framework for crypto assets.[105] The law should focus on regulating the entry and exit points to the cryptoasset ecosystem. This will include regulation of gatekeepers (such as exchanges, custodians, and wallet providers), issuers (of stablecoins) and any other service provider that participates in the exchange between crypto assets and fiat currency and exchange between different types of crypto assets. The law should require such intermediaries to be specifically authorised to carry out functions under the law.

For India, keeping in mind the size of the market, the law should rely on the expertise of the RBIand the Securities and Exchange Board of India ("SEBI") to regulate the cryptoasset market. In this process, RBI may be made responsible for prudential regulation, with SEBI responsible for market

[101] Securities and Exchange Commission, *Framework for "Investment Contract" Analysis of Digital Assets*'<https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1> accessed 8 March 2022.; Australian Securities and Investments Commission, 'Crypto assets',', <tps://asic.gov.au/regulatory-resources/digital-transformation/crypto assets/#part-a> accessed 8 March 2022.

[102] Financial Services Commission, 'FSC Proposes Additional Rules Change on Virtual Asset Service Providers' (17 February 2021) <https://www.fsc.go.kr/eng/pr010101/75410> accessed 8 March 2022.

[103] Council of European Union (19 November 2021) <https://www.consilium.europa.eu/media/53104/st14066-en21.pdf> accessed 8 March 2022.

[104] Virtual Financial Asset Act, 2018; Emergency Decree on Digital Asset Business, 2018.

[105] Shehnaz Ahmed, Swarna Sengupta, 'Blueprint of a Law for Regulating Cryptoassets' (Vidhi Centre for Legal Policy, 29 January 2022) <https://vidhilegalpolicy.in/research/blueprint-of-a-law-regulating-cryptoassets/> accessed 8 March 2022.

conduct regulation. For instance, RBI can be empowered with the regulation of stablecoin arrangements, whereas SEBI may be responsible for regulating other market intermediaries (such as exchanges, custodians, etc.). Such regulated intermediaries must comply with regulations relating to capital requirement, governance, safekeeping of consumer funds, grievance redressal, disclosure of information to consumers and regulators, customer due diligence (including know your customer requirements), risk management framework, attribution of liabilities in case of unauthorized loss to customers, and protection of consumer data.

While enacting a law for crypto assets may not be able to address all risks associated with DeFi, it is a step in the right direction, considering most DeFi services rely on cryptoassets for their transactions. A crypto asset law will at least mitigate risks emanating from such assets for the DeFi sector, bring in accountability from regulated entities, and provide necessary guidance to design standards and policies for systems based on decentralised ledgers. Such a regulatory framework is also important for regulators to understand the penetration of such markets and their interconnectedness to the financial system. As cryptoassets remain outside the regulatory perimeter, it is often challenging for regulators to access information about the extent and scope of such markets. The enforcement of such a law also implies that regulators must invest in developing the necessary skillset, expertise, forensic tools and technological solutions to implement such laws. Given the cross-border nature of crypto assets and DeFi transactions, it is equally essential to have global standards of regulation for this sector. The Financial Action Task Force ("**FATF**") has already issued its guidance on designing anti-money laundering frameworks that may apply to crypto asset service providers. [106] This serves as guidance for FATF member countries to design their regulatory framework. Similarly, the FSB has announced its plans to issue possible regulatory approaches for regulating crypto assets and global stablecoin arrangements. While such efforts will be instrumental indesigning global standards for crypto assets, it is equally important to create systems and processes for a global exchange of information relating to activities of crypto asset service providers and assistance for cross-border enforcement of actions against such providers for any illegal activity.

[106] The FATF is an international watchdog and standard-setting body for countering global money laundering and terrorist financing. It formulates recommendations and standards to prevent illegal activities, organised crime, corruption and terrorism. See FATF, 'Who we are?", < https://www.fatf-gafi.org/about/> accessed 8 March 2022; FATF, 'Updated Guidance for a Risk-Based Approach Virtual Assets and Virtual Assets Service Providers' (October 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 8 August 2022.

Second, it will be necessary to identify access points for supervision of DeFi services. This may include identifying a participant or participants (such as developers of protocol, exchanges, governance token holders, etc.) who can be accountable from a regulation perspective. Risks associated with DeFi services may be mitigated by bringing in some semblance of centralisation by identifying such access points that can be brought within the regulatory ambit. Such identification and regulatory oversight will have to be designed to not completely undermine the decentralised nature of such services.The BIS has pointed out that complete decentralisation may be an "illusion" as many Defi platforms have stakeholders (such as governance token holders) that are usually responsible for taking governance decisions regarding the system.[107]Therefore, a possible approach that may be considered is to regulate gatekeepers to the DeFi ecosystem - i.e., service providers that work as entry and exit to the DeFi ecosystem. This may include exchanges, custodians, and other service providers that act as points to access the DeFi ecosystem when cryptoassets are converted to fiat currency or vice versa. The BIS notes that several stakeholders in the DeFi ecosystem take and implement decisions, thereby enjoying governance benefits and who can become entry points for regulations.[108] The FATF, in its latest guidance,[109] clarifies that a DeFi application (software programme) is not a "virtual asset service provider" ("**VASP**") under the guidance. However, it clarifies that "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services. This is the case, even if other parties play a role in the service or portions of the process are automated." Therefore, such entities will be responsible for complying with relevant know your customer and anti-money laundering standards in the guidance. If this approach is adopted, DeFi protocol developers may be treated as banks and other financial institutions that handle consumer funds and, therefore, subject to anti-money laundering regulations. To determine who maintains control or influence in DeFi arrangements, FATF suggests considering factors like control or sufficient influence over assets or aspects of the DeFi protocol, the existence of an ongoing business relationship between themselves and users (even through smart contracts), and whether any party profits from the

[107] Sirio Aramonte, Wenqian Huang, Andreas Schrimpf, 'DeFi Risks and the Decentralisation Illusion' (*BIS Quarterly Review*, 6 December 2021) <https://www.bis.org/publ/qtrpdf/r_qt2112b.htm> accessed 10 April 2022.

[108] ibid.

[109] FATF, *Updated Guidance for a Risk-Based Approach Virtual Assets and Virtual Assets Service Providers* (October 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 8 March 2022.

service or has the ability to set or change parameters, etc. As DeFi markets continue to grow, this may be a preliminary step to regulating the markets.

Third, the regulation of the DeFi system will also require a close analysis of legal issues emanating from DLT based solutions. DLT based systems often raise challenging questions about jurisdiction, data protection, determination of rights and liabilities, etc., as has been discussed earlier. Such issues are also common to DeFi services. Therefore, designing public policy frameworks for accommodating such blockchain-based solutions will also be an important step towards addressing legal uncertainties associated with the DeFi system. This may require countries to identify standards or benchmarks such technologies should meet. This should address issues relating to the determination of rights and liabilities of participants, dispute resolution mechanism, the procedure for handling customer data, security audits, risk management framework for operational resilience, and agreement on jurisdictional issues. Currently, most DLT-based systems rely on contractual arrangements for such matters. While such an arrangement maybe useful for permissioned DLT systems, there will be challenges in designing and implementing governance frameworks (whether through contractual arrangements or policy frameworks) for permissionless DLT systems. Accordingly, regulators will have to rely on soft measures such as public-private collaboration, international cooperation and innovative technological solutions, as discussed below, to monitor such solutions. Currently, most countries are exploring possible legal issues emanating from DLT-based systems and accordingly examine if existing laws need any amendments to accommodate such developments. Data protection regulators in France and Singapore have clarified the applicability of data protection laws to DLT-based systems.[110]

Fourth, international cooperation is criticalgiven the global reach of the DeFi markets and the limitations of existing regulatory approaches to regulate this ecosystem. This is important to create standards that can

[110] Personal Data Protection Commission Singapore, *Guide on Personal Data Protection Considerations for Blockchain Design* (2022) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Blockchain-Guide_final.ashx?la=en> accessed 08 August 2022; Commission nationale de l'informatique et des libertés(CNIL), 'Premiers élémentsd'analyse de la CNIL' (September 2018) <https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf> accessed 08 August 2022; CNIL, 'Blockchain et RGPD : quelles solutions pour un usage responsableenprésence de donnéespersonnelles?' (24 September 2018) <https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles> accessed 08 August 2022; Baker Mckenzie, 'French Data Protection Authority Issues Guidance on GDPR and Blockchain' (24 October 2018) <https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/french-data-protection-authority-issues-guidance-on-gdpr-and-blockchain_2/> accessed 08 August 2022.

guide the development of legally compliant DeFi protocols. For instance, the Principles for Financial Market Infrastructures[111] are the international standards for financial market infrastructures, i.e., payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories. The principles have been issued by the Committee on Payments and Market Infrastructures[112] and the International Organization of Securities Commissions and adopted by the international community and regulators to strengthen and preserve financial stability. Similarly, international standards or principles coupled with adopting a global cooperation framework among regulators will be essential to supervising the DeFi markets.

Fifth, DeFi may present an opportunity for regulators to rely on regulatory technologies or popularly referred to as RegTech and SupTech - the use of technology for regulatory compliance and supervision.[113]This may be achieved by designing regulatory systems that can leverage technological innovations. For instance, in a paper, BIS argues for "embedded supervision" for DLT based systems in which the regulatory framework "provides for compliance in tokenised markets to be automatically monitored by reading the market's ledger, thus reducing the need for firms to actively collect, verify and deliver data."[114] This enables automated compliance monitoring and supervision. Taking this idea forward, Dirk Andreas Zetzscheet al proposes "embedded regulation" - where regulatory objectives "of market integrity, market conduct, and financial stability are included as part of the design of any DeFi system."[115] Such an approach envisages that a DeFi system is built in a manner that includes features of transparency, disclosure, and compliance as a part of its automated structure. Another approach to regulation that is recommended by OECD to regulators is to leverage technological

[111] BIS, 'Principles for Financial Market Infrastructures' <https://www.bis.org/cpmi/publ/d101.htm> accessed 8 March 2022.

[112] It is an international standard setter that promotes, monitors and makes recommendations about the safety and efficiency of payment, clearing, settlement and related arrangements. It also serves as a forum for central bank cooperation in related oversight, policy and operational matters. See BIS, 'CPMI-Overview' <https://www.bis.org/cpmi/about/overview.htm> accessed 8 March 2022.

[113] Dirk Broeders and Jermy Prenio, 'Innovative Technology in Financial Supervision (SupTech) – the Experience of Early Users' (BIS, FSI Insights on policy implementation No 9, July 2018) <https://www.bis.org/fsi/publ/insights9.pdf> accessed 8 March 2022.

[114] Raphael Auer, *Embedded Supervision: How to Build Regulation into Blockchain Finance* (*BIS Working Papers No 811*, September 2019) <https://www.bis.org/publ/work811.pdf> accessed 8 March 2022.

[115] Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley, *Decentralized Finance* (Journal of Financial Regulation, Volume 6, Issue 2, 20 September 2020) <https://academic.oup.com/jfr/article/6/2/172/5913239> accessed 8 March 2022.

innovations to regulate such services by participating "as nodes in a network and / or intervene at a smart contract level."[116]

Sixth, regulators may consider using regulatory sandboxes to allow companies to test DeFi services in a controlled environment with regulatory oversight. A regulatory sandbox will enable businesses to live test new products and services in a "controlled" environment where regulators may or may not permit regulatory relaxation for testing.[117] Regulatory sandboxes enable regulators and businesses to collect evidence on the opportunities and risks provided by fintech innovation. Findings from the testing can also inform laws and policies designed by regulators for such innovation. Financial sector regulators may use such a regulatory sandbox testing framework to test innovations in the DeFi market to identify use case cases, opportunities and risks of DeFi services. Evidence gathered from such testing may help design regulations for the DeFi market.

Seventh, as the DeFi markets continue to evolve, it may not be possible for regulators to design comprehensive regulations that cover every aspect of DeFi. The unique properties of the DeFi services mean that regulators will have to adopt a co-regulatory approach where public authorities work closely with the private sector to design interventions through which public policy frameworks can interact with the governance structures of DeFi. While the regulator may lay down broad principles that may be followed while designing DeFi protocols and providing DeFi services, it will have to rely on self-regulation through collaboration between different stakeholders of the DeFi ecosystem to develop technical standards for implementing such principles for effective enforcement.

DeFi seeks to improve the efficiency of financial markets by building upon the work done in blockchain and fintech. Whether it achieves this promise is yet to be seen. The DeFi ecosystem is still nascent, and in many cases, complete decentralization is not witnessed in most DeFi applications. There is no common understanding of the nature of such DeFi services and their interconnectedness with the existing financial system. Therefore, in most countries, policy responses correctly have not focused on the DeFi ecosystem as a whole but some of its building blocks, as discussed above. However, a study

[116] OECD, 'Why Decentralised Finance (DeFi) Matters and the Policy Implications' (19 January 2022) <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> accessed 8 March 2022.

[117] Reserve Bank of India *Enabling Framework for Regulatory Sandbox* (8 October 2021) <https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1187#:~:text=The%20RBI%20shall%20bear%20no,with%20the%20relevant%20regulatory%20requirements.> accessed 8 March 2022.

of the opportunities and risks presented by DeFi and the legal issues underscore that it will pose similar regulatory challenges tocrypto assets, perhaps more heightened due to its ability to mirror existing financial services.

Going by existing reports indicating that India is sixth in terms of DeFi application, India needs to closely follow the developments in the DeFi sector.[118] However, as the market is still evolving, a comprehensive regulatory response to the DeFi ecosystem is not warranted at this stage. Instead, as the first step, it is important to focus on spending regulatory resources and attention on the building blocks of DeFi– which include crypto assets, stablecoins, smart contracts and the DLT system. Regulating these building blocks will also help monitor the entry and exit points to the DeFie cosystem. This must be coupled with other policy approaches suggested above – leveraging technological innovations to regulate regulatory sandboxes and adopting a co-regulation model. The future and growth of the DeFi market and its role in promoting public policy objectives are closely tied to the policy and regulatory response to such markets. Implementing the recommendations discussed above will enable policymakers to design some form of regulatory oversight before the market attains systemic importance or becomes too big to regulate.

[118] *India* 6th *Biggest Country in Terms of DeFi Adoption: Chainalysis* (*Livemint,* 28 August 2021) <https://www.livemint.com/market/cryptocurrency/india-6th-biggest-country-in-terms-of-defi-adoption-chainalysis-11630121581732.html > accessed 12 April 2022.

India's Policy Responses to Big Tech: And an Eye on the Rise of 'Alt Big Tech'

Smriti Parsheera[*]

Abstract *The term 'big tech' offers a helpful and widely used label for describing the world's most powerful technology companies. The challenges posed by big tech across the domains of competition, innovation, human rights, and social and political impact are real and immediate. So is the need for building more effective checks against them. India is still in the early stages of formulating its strategy on big tech, through the traditional playbook of competition, enforcement, and domain-specific regulatory interventions. But it has also adopted a more novel strategy of relying on open APIs and interoperability standards to counter the market features that enable the concentration of power in the hands of dominant tech players. The paper studies the Unified Payments Interface, the Data Empowerment and Protection Architecture, and the Open Network for Digital Commerce as examples of such technical systems. It argues that while recognising the innovation and progress of these new systems, it is also important to keep an eye on their potential to emerge as 'alt big tech' – systems that create new opportunities for dominance and power play that can bear significant consequences for competition, innovation, and public interest in the long run.*

[*] Smriti Parsheera is a lawyer and public policy researcher. She is currently a Fellow with the Cyber BRICS Project, FGV Law School, Brazil and a PhD Candidate at the Indian Institute of Technology Delhi. The author is grateful to Bhargavi Zaveri-Shah, Renuka Sane and Ajay Shah for valuable conversations that have informed this analysis, to the editorial team at the Indian Journal of Law and Technology for their excellent feedback on the first draft of the paper, and to an anonymous peer reviewer for their comments. The author also thanks Divyanshu Dembi for research assistance in studying the literature on the characteristics of big tech.

I. Introduction

Current news is awash with references to big tech's supersized ambitions,[1] their toll on privacy,[2] the onslaught on democracy,[3] and the need for a regulatory crackdown.[4] In most of these contexts the term 'big tech' is commonly used to describe a set of large United States-based corporations, notably, Alphabet (Google), Amazon, Meta (Facebook), and Apple that are collectively dubbed the 'GAFA' (or now 'GAMA') firms. These businesses stand out in terms of their large market capitalisation, significant user base, market power, and conduct that bears significant implications for individual rights, competitive outcomes, and democratic values.

Depending on the context, other firms like Microsoft, Twitter, Netflix, and Uber may sometimes be added to the list. Similarly, China is said to have its counterparts in the 'BATX' – Baidu, Alibaba, Tencent, and Xiaomi – firms that are often touted as its big tech response to the American technology giants. India also has its own tribe of domestic technology-driven businesses that operate using the same playbook of data aggregation, cross-sectoral linkages, acquisitions, and control. However, the general usage of the term big tech in the media and policy discourse in India is almost exclusively reserved for the foreign-owned multinational corporations described earlier.[5]

The global footprint of big tech firms and demonstrated instances of abuse of power have prompted a flurry of activities aimed at their regulation and governance. China has been in the news for what has been labelled as a 'regulatory storm' of imposing new legal requirements in areas such

[1] 'Big Tech's Supersized Ambitions' (*The Economist*, 22 January 2022), <www.economist.com/leaders/2022/01/22/big-techs-supersized-ambitions> accessed 29 January 2022.

[2] Tom Chavez, Martiza Johnson and Jesper Andersen, 'Toward Data Dignity: How We Lost Our Privacy to Big Tech' (*Fortune*, 28 January 2022). <https://fortune.com/2022/01/28/big-tech-data-privacy-ethicaltech/> accessed 29 January 2022.

[3] *Can Democracy Survive the Big Tech Onslaught?* (*Deccan Chronicle*, 28 January 2022) <www.deccanchronicle.com/opinion/op-ed/270122/can-democracy-survive-the-big-tech-onslaught.html> accessed 29 January 2022.

[4] Richard Waters, 'Moment of Truth for Proposed Big Tech Crackdown' (*Financial Times*, 20 January 2022) <www.ft.com/content/5b3fb340-8165-4399-b54e-3ab51fa9c7d5> accessed 29 January 2022.

[5] As an exception to this practice, Aneja and Chamuah include the Indian telecommunication giant, Reliance Jio, and the National Payments Corporation of India in their analysis of India-specific big tech entities. See Urvashi Aneja and Angelina Chamuah, *A Balancing Act: The Promise and Peril of Big Tech in India* (*Tandem Research*, 2020) <https://tandem-research.org/assets/Tandem-Research-Big_Tech_report.pdf> accessed 2 February 2022.

as competition law, privacy, and algorithmic regulation.[6] In the US, the report of the House Committee's Investigation on Competition in Digital Markets was followed by the appointment of big tech critic Lina Khan as the chair of the Federal Trade Commission and the introduction of a bouquet of bills seeking to control big tech's antitrust activities.[7] And the European Commission has adopted a new digital regulation package consisting of the Digital Services Act and the Digital Markets Act.[8]

Tackling the bigness of technology firms has also been the motivator (or feature) of several policy initiatives in India. One part of this is playing out in the domain of competition law, where we are seeing the Competition Commission of India ('the CCI') opt for a more proactive stance towards competition enforcement in the technology sector.[9] Most recently, the CCI imposed penalties of Rs. 13.38 billion and 9.36 billion, respectively, on Google for anti-competitive conduct linked to its Android ecosystem and Play Store policies.[10] However, the influence of big tech extends far beyond the domain of competition and market effects. Curtailing the behaviour of big tech firms has, accordingly, formed the backdrop for many other actions that are taking shape outside the domain of competition law. The governance of non-personal data, discussions around India's e-commerce strategy and enhanced obligations for 'significant' players in contexts like intermediary liability and data protection are some examples. While mapping these

[6] Martin Chorzempa, *China's Campaign to Regulate Big Tech is More than Just Retaliation* (*Nikkei Asia*, 3 August 2021) <https://asia.nikkei.com/Opinion/China-s-campaign-to-regulate-Big-Tech-is-more-than-just-retaliation> accessed 2 February 2022; Arjun Kharpal, 'China's Next Regulatory Target — Algorithms, The Secret of Many Tech Giants' Success' (*CNBC*, 7 January 2022) <www.cnbc.com/2022/01/07/china-to-regulate-tech-giants-algorithms-in-unprecedented-move.html> accessed 2 February 2022.

[7] Commentators, however, remain sceptical as to whether these proposals will actually translate into law. See Cecilia Kang and David McCabe, 'Efforts to Rein In Big Tech May Be Running Out of Time' *New York Times* (Washington, 20 January 2022) <www.nytimes.com/2022/01/20/technology/big-tech-senate-bill.html> accessed 3 February 2022.

[8] European Commission, 'The Digital Services Act Package' <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package/> accessed 18 September 2022; Council of the EU, 'Regulating "Big Tech": Council Agrees on Enhancing Competition in the Digital Sphere' (November 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/regulating-big-tech-council-agrees-on-enhancing-competition-in-the-digital-sphere/> accessed 3 February 2022.

[9] Anshuman Sakle and Pahari Nandini, 'The Interaction between Competition Law & Digital and E-Commerce Markets in India' (2020) 16(2) Indian Journal of Law and Technology 18; Manas Kumar Chaudhuri, Anisha Chand, Tanveer Verma and Armaan Gupta, 'India: Overview' in Asia-Pacific Antitrust Review 2022(Global Competition Review, March 2022) 114.

[10] *Umar Javeed and others v. Google LLC and another*,Case No. 39 of 2018, Order dated 20 October 2022 <https://cci.gov.in/antitrust/orders/details/1070/0> accessed 31 October 2022; *XYZ v. Alphabet Inc and others*, Case No. 7 of 2020, Order dated 25 October 2022 <https://cci.gov.in/antitrust/orders/details/1072/0> accessed 31 October 2022.

broad trends, the paper also notes that despite the general grouping of certain entities as 'big tech', policy actions tend to be subjective and individualised, shaped by the peculiarities of different business models and a range of political, strategic, and pragmatic considerations.

In addition to the regulatory responses aimed at controlling the activities of big tech, India has adopted a novel approach to build alternative technical architectures or networks across different segments of the digital ecosystem. These systems rely on the use of open Application Programming Interfaces ('APIs'), a mechanism that enables technical systems to directly interact with one another.[11] Popular examples of private sector APIs include the use of Google's and Facebook's authentication for logging into other websites and the aggregation and price comparison functions on travel booking sites.[12] In the case of India's public digital systems, the deployment of open APIs is being seen in areas such as digital payments through the Unified Payments Interface ('UPI'), electronic consent management through the Data Empowerment and Protection Architecture ('DEPA'), and, most recently, in the field of digital commerce through the Open Network for Digital Commerce ('ONDC'). The stated goals of these systems include encouraging openness and interoperability in digital ecosystems, empowering users, and, in the process, countering the concentration of power in the hands of dominant tech players.[13]

While policy documents often refer to the novelty and the expected gains of such technical systems,[14] it is equally important to acknowledge the new opportunities of power play that they generate. In this paper, I use the term 'alternative (alt) big tech' to refer to the potential for dominance by these systems and the powers exercised by the entities controlling them. This deliberately provocative term serves a dual purpose. First, it is intended to

[11] Ministry of Communications & Information Technology, 'Policy on Open Application Programming Interfaces (APIs) for Government of India' (May 2015) <www.meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf> accessed 27 May 2022.

[12] Thomas Bush, '5 Examples of APIs We Use in Our Everyday Lives', (*Nordic APIs*, 10 December 2019), <https://nordicapis.com/5-examples-of-apis-we-use-in-our-everyday-lives/>accessed 18 September 2022.

[13] Ministry of Commerce & Industry, 'Shri Piyush Goyal chaired Open Network for Digital Commerce' (*Press Information Bureau*, 13 August 2021) <https://pib.gov.in/PressReleasePage.aspx?PRID=1745611> accessed 20 May 2022; NITI Aayog, *Data Empowerment And Protection Architecture* (August 2020), </www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf> accessed 4 February 2022, 26. The paper was drafted with the support of the Indian Software Product Industry RoundTable (iSPIRT).

[14] NITI Aayog, 'Strategy for National Open Digital Ecosystems: Consultation Paper' (February 2020) <https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf> accessed on 26 May 2022. The paper was drafted with the support of Omidyar Network India and Boston Consulting Group.

capture the positioning of India's new technical systems as an alternative to the present status quo of monopolisation by a few (often foreign-based) firms. Second, it envisages the possibility of the technical systems themselves becoming the new centres of power and control in areas like digital payments, consent management, and e-commerce.

The UPI, the DEPA, and the ONDC represent examples of systems that are being rolled out through a coordinated strategy of public-private collaboration – the solutions are developed and implemented in the private sector but endorsed through state actions. This vests a new form of power in the hands of those involved in developing and implementing India's alt big tech systems. Unlike the economic strength, overt data-centric design, and early mover advantage of traditional big tech, alt big tech systems derive their main firepower from the state's role in asserting their legitimacy and desirability. Their infrastructural status, control over other network participants, and ability to set and monitor technical standards vest additional layers of power in these new systems.

The rest of the paper is organised as follows. Section 2 discusses the main characteristics of big tech as identified in the literature. These are i) market capitalisation and accompanying economic power, ii) size of the user base, iii) data intelligence, iv) infrastructural capabilities, and v) societal impact. Section 3 then presents a conceptual mapping of the different policy contexts in which concerns of 'bigness' are shaping regulatory boundaries in India. This includes areas such as competition law, obligations of 'significant' entities under various laws, and proposals for data governance. This is followed by some illustrations of how various types of strategic and pragmatic considerations, such as pressures from interest groups or the refusal to comply with government demands, also contribute to regulatory outcomes involving big tech. Next, Section 4 discusses India's new technical systems like the UPI, the DEPA, and the ONDC, some of which constitute a new type of response to counter the power of digital monopolies. Section 5 explains the rationale behind referring to these systems as 'alt big tech' and highlights the need to appreciate both the expected benefits as well as the long-term implications of such systems. Section 6 concludes with a summary of the paper's key observations.

II. What are the Characteristics of 'Big Tech'?

Conversations around big tech are often mired in acronyms like GAFA (*Google, Apple, Facebook and Amazon*), FAANG (*Facebook, Amazon, Apple, Netflix and Google*), and, in the case of Chinese companies, BATX

(*Baidu, Alibaba, Tencent and Xiaomi*). But these are merely descriptors of the constituents of big tech. The more pertinent question is: Why is it that certain businesses have attracted this label and what is the basis for these groupings?

In a 2017 piece for Slate, Will Oremus explained that the use of the prefix 'Big' before the name of any industry, such as Big Pharma or Big Tobacco, signifies not just the size of the businesses but an accompanying sense of fear and mistrust.[15] The term is, therefore, used to describe "dominant industries whose power cannot be tamed by politicians or market competition."[16] Oremus observes that the term first entered the mainstream discourse in the US around 2013, corresponding with Edward Snowden's revelations about the National Security Agency's surveillance tactics.[17] In parallel, the growing concerns around anti-competitive practices in the tech sector, the data-extractive practices of the kind illustrated by the Facebook-Cambridge Analytica scandal, and the use of social media for political propaganda and misinformation strengthened the need for a term to capture the power and mistrust that came to be associated with the tech sector. The phrase 'big tech' seemed to fit the bill and gradually became the mainstream expression to describe the world's most powerful technology companies in all the above-mentioned contexts.

The use of the term has become so commonplace that most commentators tend to presume, without explicitly defining, what constitutes big tech. However, there is a body of literature that engages more substantively with the definitional aspects of big tech.[18] Drawing from this work, this Section 2

[15] Will Oremus, 'Big Tobacco. Big Pharma. Big Tech?' (*Slate*, 17 November 2017) <https://slate.com/technology/2017/11/how-silicon-valley-became-big-tech.html> accessed 10 January 2022.

[16] Freddie Hayward, 'What the Term "Big Tech" Tells us About the Future of Silicon Valley Titans' (*The New Statesman*, 16 February 2021) <www.newstatesman.com/science-tech/2021/02/what-term-big-tech-tells-us-about-future-silicon-valley-titans> accessed 10 January 2022.

[17] Oremus (n 15). The Snowden leaks are said to have triggered a phase of resistance-cum-co-operation between large technology companies and government agencies on issues such as encryption and data access. On one hand, tech companies responded to state surveillance with stronger encryption offerings on their products, on the other, metadata was kept easily available for their own business use and for government access. See also Félix Tréguer, 'Seeing like Big Tech', in Didier Bigo, Engin Isin and Evelyn Ruppert (eds), *Data Politics: Words, Subjects, Rights* (1st edn, Routledge 2019) 145.

[18] See Aneja and Chamuah (n 5); Nizan Geslevich Packin, 'Too Big to Fail 2.0? Digital Service Providers as Cyer-social Systems', (2018) 93(4) Indian Law Journal 1211; Reijer Hendrikse, Ilke Adriaans, Tobias J. Klinge and Rodrigo Fernandez, 'The Big Techification of Everything' (2021) 31(1) Science as Culture 59; Jai Vipra, 'Big Tech and the Global Economy' (*Focus on the Global South*, January 2021) <https://focusweb.org/wp-content/uploads/2021/01/Big-Tech-Jan2021.pdf> accessed 29 January 2022; Parminder Jeet Singh,

discusses 5 key markers of the 'bigness' of big tech firms. These are i) market capitalisation and accompanying economic power, ii) size of the user base, iii) data intelligence, iv) infrastructural capabilities, and v) societal impact.

First, market capitalisation, which signifies the total market value of a company's shares, is one of the most widely used parameters for describing big tech.[19] In 2021, seven out of the world's ten largest companies by market cap were technology players – Apple, Microsoft, Amazon, Alphabet, Facebook, Tencent, and Alibaba.[20] To put this in context, Apple alone had a market cap that was higher than the gross domestic product (GDP) of ninety six percent of countries.[21] This economic power comes with the ability to diversify into new markets, to buy out emerging competitors, and to shape research and policy agendas – all of which reinforce the 'bigness' of these firms.

Second, big tech firms are characterised by the size of their user base, which commonly extends beyond international boundaries. For instance, the most popular websites in India, in terms of daily visitors and page views, are largely US-based/ owned businesses.[22] The list includes the usual suspects like Google (Search and YouTube), Facebook and Instagram, Amazon, and Microsoft, in addition to others like Flipkart and Wikipedia. Large user bases combined with data-intensive business models give big tech their big data advantage.[23] This is fuelled by the extractive data policies that Shoshona Zuboff famously termed 'surveillance capitalism.'[24]

Another way to describe this phenomenon is by using the imagery of 'data-based intelligence' as being at the core of the business models of big

'Breaking up Big Tech: Separation of its Data, Cloud and Intelligence Layers' (2020) Data Governance Network Working Paper No. 9 <https://itforchange.net/sites/default/files/add/Regulating_data__cloud_and_intelligence_-_Paper_9-21.pdf> accessed 29 January 2022.

[19] Rodrigo Fernandez, Ilke Adriaans, Reijer Hendrikse and Tobias J. Klinge, *The Financialisation of Big Tech* (Centre for Research of Multinational Corporations December 2020) <www.somo.nl/the-financialisation-of-big-tech/> accessed 10 January 2022; See Vipra (n 18) for a description of leading big tech firms based on this criterion.

[20] Statista Research Department, 'The 100 Largest Companies in the World by Market Capitalization in 2021' (*Statista*, 5 August 2022) <www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/> accessed 18 September 2022.

[21] Omri Wallach, 'The World's Tech Giants, Compared to the Size of Economies' (*Visual Capitalist*, 7 July 2021) <www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/> accessed 18 September 2022.

[22] Top Sites in India (October, 2021). Alexa, <www.alexa.com/topsites/countries/IN>. Australia based Canva.com was the own non-US based business in the top 10 list for India.

[23] Cristian Santesteban and Shayne Longpre, 'How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science' [2020] The Antitrust Bulletin 1.

[24] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).

tech entities.[25] The capability to derive intelligence from the vast data accessible to them, therefore, becomes the third prominent characteristic of big tech firms.

Here it is worth clarifying that features like the assetisation of data, network effects, and increasing returns to scale are not unique characteristics of big tech. Rather, these have become the basic features of most businesses in the digital economy. However, what might distinguish the big tech players is the scale at which they have been able to capitalise on these features, very often due to a first-mover advantage. This first-move advantage has been discussed in contexts like that of Google's search engine, WhatsApp's messaging network and Amazon's cloud computing services.[26] Some, however, question the first-move advantage theory because its relevance is often over-simplified or overstated.[27]

The fourth defining criterion relates to the ability of certain platforms to act as the 'infrastructural core' of the digital ecosystem, creating a constellation of firms that are dependent on them.[28] Proponents of this view would, for instance, count Google's map services and Facebook's identification service as big tech. But they would exclude firms like Airbnb and Uber which essentially ride on top of this core infrastructure.[29] Similarly, Amazon's control over key e-commerce infrastructure and its dominance in cloud services has led to its characterisation as an essential facility.[30] Nizan Geslevich Packin makes an interesting analogy between these key digital service providers and financial institutions that were regarded as 'too big to fail' during the 2008 global financial crisis.[31] He observes that the size, political and financial influence, extent of vertical and horizontal integration, cyber security exposure, and overall social impact of big tech firms merit their designation as critical service providers.

Finally, there is the fifth criterion of the societal impact of big tech firms. One way to understand this is through the lens of 'civic power', stemming

[25] Singh (n 18).

[26] Subcommittee on Antitrust, Commercial, and Administrative Law, 'Investigation of Competition in Digital Markets', (*US House of Representatives*, 2020), <https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519> 79, 143, 316.

[27] Fernando F. Suarez and Gianvito Lanzolla, 'The Half-Truth of First-Mover Advantage' (2005) 83(4) Harvard Business Review 121.

[28] José Van Dijck, Thomas Poell, and Martijn de Waal, *The Platform Society: Public Values in a Connective World* (Oxford University Press, 2018); Also see Hendrikse et al. (n 18).

[29] Van Dijck et al. (n 28), 15.

[30] Lina M. Khan, 'Amazon's Antitrust Paradox' (2017) 26(3) Yale Law Journal 710.

[31] Packin (n 18).

from the role of big tech in the exercise of democratic functions.[32] Prominent examples of this range from the use of social media platforms like Facebook and Twitter for online activism during the Arab Spring and the #MeToo movement.[33] They have also been used as a threat to election integrity across jurisdictions[34] and as a platform for information warfare during the Russian attack on Ukraine.[35] This inquiry can be broadened to examine the impact of big tech on 'societal sustainability'[36] by capturing its impact on different institutions, political systems, and civil society.[37] Furthermore, researchers have also highlighted the role of big tech in shaping research and ethical agendas.[38]

Based on the above, the following emerge as some of the main features of big tech – financial resources and market power, data intelligence, infrastructural capabilities, and societal impact. The relevance of each of these characteristics would vary depending upon the policy context in which the test of bigness is being deployed. Further, as noted by Birch and Cochrane, it would be incorrect to regard big tech as a monolith; each of its constituents

[32] Martin Moore, 'Tech Giants and Civic Power' (Centre for the Study of Media Communication and Power, April 2016) <www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf> accessed 4 February 2019. Martin Moore identifies the following 6 types of civic powers of powerful information intermediaries – (i) The power to command attention, (ii) The power to communicate news, (iii) The power to enable collective action, (iv) The power to give people a voice, (v) The power to influence people's vote, and (vi) The power to hold power to account.

[33] Bani Sapra, 'The Last Decade Showed how Social Media Could Topple Governments and Make Social Change - and it's Only Getting Crazier from Here' (*Business Insider*, 15 January 2020) <www.businessinsider.in/politics/news/the-last-decade-showed-how-social-media-could-topple-governments-and-make-social-change-and-its-only-getting-crazier-from-here/articleshow/73259561.cms> accessed 16 May 2022.

[34] Adrian Shahbaz and Allie Funk, 'Digital Election Interference', (*Freedom House*, 2019) <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference> accessed 16 May 2022.

[35] Collette Snowden, 'Guns, Tanks and Twitter: How Russia and Ukraine are Using Social Media as the War Drags on', (*The Conversation*, 5 April 2022) <https://theconversation.com/guns-tanks-and-twitter-how-russia-and-ukraine-are-using-social-media-as-the-war-drags-on-180131> accessed 16 May 2022.

[36] Bernard Arogyaswamy, 'Big Tech and Societal Sustainability: An Ethical Framework' (2020) 35 AI & Society 829.

[37] Commentators have also documented different facets of big tech's mission creep problem with resulting implications for other key sectors, including labour, health, finance, agriculture, and education. See Michael Kwet, 'Digital Colonialism: The Evolution of US Empire' (*TNI*, March 2021) <https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire> accessed 4 February 2019; '21 Takes on Big Tech from 2021' (*DataSyn*, 16 December 2021) <https://datasyn.substack.com/p/2021-versus-big-tech?r=wx43p&utm_campaign=post&utm_medium=web> accessed 4 February 2022.

[38] Meredith Whittaker, 'The Steep Cost of Capture' (2021) 28(6) ACM Interactions 50; Mohamed Abdalla and Moustafa Abdalla, 'The Grey Hoodie Project: Big Tobacco, Big Tech, and the Threat on Academic Integrity' in 'Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society' (ACM, 2021).

is an independent actor governed by its strategic motivations.[39] By extension, regulatory responses to big tech are also shaped by various strategic and political considerations with seemingly similarly placed actors sometimes being treated differently. I offer some examples of this in the next Section. But before that Section 3 presents a mapping of some of the key policy responses toward big tech in India.

III. Mapping India's policy responses

In the last decade, India has adopted several policy initiatives that appear to be geared towards reigning in the conduct of big tech. The use of the phrase 'appear to be' here is deliberate as the term 'big tech' itself is rarely used in the policy documentation. But based on examples seen in contexts like intermediary regulation, data governance, and e-commerce policies, I note that the regulatory actions broadly mirror the popular understanding of big tech as a set of large American corporations. Policy engagements with Chinese tech entities, on the other hand, lie more clearly in the domain of strategic and security actions. Examples include the banning of a large number of Chinese apps, including the popular social media app TikTok (ByteDance)[40] post the Galwan Valley clash of 2020, and the exclusion of Huawei and ZTE from India's 5G trials.[41]

The mapping exercise that follows relies on cases in which the constituents of big tech (as described earlier) have either been the target of direct regulatory actions or have been mentioned as examples while making a case for regulation. I discuss 4 broad themes or types of regulatory actions in the Indian policy context – i) addressing anti-competitive conduct, ii) enhanced obligations for 'significant' players, iii) data control, and iv) general compliance with laws. This is not an exhaustive list. For instance, policy thinking on the regulation of digital players, which, by implication, includes big tech, is also taking place in many other fields like taxation, consumer protection,

[39] Kean Birch and D. T. Cochrane, 'Big Tech: Four Emerging Forms of Digital Rentiership', (2022) 31(1) Science as Culture 44.

[40] In total about 300 Chinese-origin apps and their proxies have been hit by bans issued by the Indian government since 2020. See Aashish Aryan and Soumyarendra Barik, 'Explained: Why did the govt ban more China-linked apps?' *The Indian Express* (New Delhi, 15 February 2022) <https://indianexpress.com/article/explained/explained-why-govt-ban-more-china-apps-7772982/> accessed 16 May 2022.

[41] Aman Grover and Shivangi Mittal, 'Chinese Firms Left Out of 5G Trials in India but Modi Govt Played Fair. Here's How' (*The Print*, 25 May, 2021) <https://theprint.in/opinion/chinese-firms-left-out-of-5g-trials-in-india-but-modi-govt-played-fair-heres-how/664638/> accessed 2 February 2022.

and regulation of over-the-top services. But all of these are not within the scope of this paper.

A. Addressing anti-competitive conduct

The rise of digital monopolies with accompanying practices of self-preferencing by platforms, the imposition of unfair conditions, and exclusive dealing arrangements have led to several complaints against big tech before the CCI. For instance, the CCI recently found Google to be indulging in the abuse of dominance in cases involving the pre-installation of Google's proprietary apps on its Android platform and for offering a competitive advantage to its own payment services on the Play Store.[42] Apple is also facing a similar investigation in relation to its app store policies.[43]

In the e-commerce space, the CCI is investigating allegations of exclusive arrangements, deep-discounting and preferential listing by Amazon and Flipkart, the two largest online marketplaces in India.[44] It has also initiated an investigation against WhatsApp for the changes announced to its privacy terms in 2020.[45] This case is significant in that it is probably the first occasion where the CCI has taken suo moto action against a digital player (all the other investigations were in response to third-party complaints). Moreover, the issues in the case lie at the intersection of competition policy and data governance issues, an area that the CCI has shied away from traversing in the past.[46]

In all the instances cited above, the CCI has found *prima facie* evidence of anti-competitive conduct and referred the matter to a more detailed investigation by its Director General. This represents a shift from its earlier decisional practice where complaints against tech sector players rarely made it to the stage of detailed investigation.[47] The reasoning given for this included

[42] *Umar Javeed and others v. Google LLC* and another and *XYZ v. Alphabet Inc and others* (n 10).

[43] *Together We Fight Society v Apple Inc*. 2021 SCC OnLine CCI 62.

[44] *Delhi Vyapar Mahasangh v Flipkart Internet (P) Ltd* 2020 SCC OnLine CCI 3.

[45] *Updated Terms of Service and Privacy Policy for WhatsApp Users, In re* 2021 SCC OnLine CCI 19.

[46] *Vinod Kumar Gupta v WhatsApp Inc* 2017 SCC OnLine CCI 32. This case related to the data sharing arrangement between Facebook and WhatsApp.The CCI held WhatsApp to be a dominant player in the market for app-based instant messaging services but did not find it to be indulging in abuse of dominance. *See also*, Smriti Parsheera, 'WhatsApp's Privacy Terms: What Competition Commission Must Note' (*The Quint*, 18 February 2021) <https://www.thequint.com/voices/opinion/whatsapp-change-in-privacy-terms-what-it-means-dominance-abuse-competition-law#read-more> accessed 4 February 2022.

[47] Smriti Parsheera, Ajay Shah and Avirup Bose, 'Competition Issues in India's Online Economy' (2017) NIPFP Working Paper No. 194 <www.nipfp.org.in/media/medialibrary/2017/04/WP_2017_194.pdf> accessed 4 February 2022.

concerns of stifling innovation through premature intervention in nascent technology-driven markets.[48] The order passed by the CCI against Google in 2018 was a notable exception to this trend.[49] The case related to Google's abuse of dominance in its general web search services to limit user choice, the setting of fixed position for Google-owned results, and the imposition of restrictions on search syndication partners. The CCI found Google to violate Indian competition law on several of these counts. While I have previously criticised the order for not going far enough in terms of its rigour and consequences, the case is significant for marking the beginning of the CCI's engagement with big tech.[50] Reportedly, the CCI is now planning to create a 'Digital Markets and Data Unit' for effectively dealing with anti-competitive practices in the tech sector.[51]

In addition to these enforcement actions, there has also been some debate around the legal changes that may be required to better regulate competition in this area. The report of the Competition Law Review Committee (CLRC) constituted by the Ministry of Corporate Affairs included a chapter dedicated to competition issues in 'technology and new age markets.'[52] The CLRC's overall view was that the Competition Act, 2002, already offers sufficient scope to cover several practices seen in online markets, like the use of non-cash considerations, algorithmic collusion, and data and network effects, as factors for determining dominance.

The committee, however, felt that there was a need to look at new parameters like 'size of the transaction' and 'deal value' while considering mergers and acquisitions in the digital sector. This is because the existing asset and turnover-based thresholds are often inadequate to capture the competition concerns that may arise from transactions among digital players. Facebook's acquisition of WhatsApp is a notable case in point.[53] The Competition Law (Amendment) Bill, 2022 now seeks to address this issue through the

[48] *All India Online Vendors Assn v Flipkart India (P) Ltd* 2018 SCC OnLine CCI 97.

[49] *Matrimony.com Ltd v Google LLC* 2018 SCC OnLine CCI 1.

[50] Smriti Parsheera, 'CCI's Order Against Google: Infant Steps or a Coming-of-age Moment?' (*The LEAP Blog*, 22 February 2018) <https://blog.theleapjournal.org/2018/02/ccis-order-against-google-infant-steps.html> accessed 4 February 2022.

[51] Press Trust of India, 'Parliamentary Panel Summons Tech Giants to Discuss Competitive Conduct' *Business Standard* (New Delhi, 29 April 2022) <https://www.business-standard.com/article/current-affairs/parliamentary-panel-summons-tech-giants-to-discuss-competitive-conduct-122042801063_1.html> accessed 24 May 2022.

[52] Ministry of Corporate Affairs, *Report of the Competition Law Review Committee* (2019) <www.mca.gov.in/Ministry/pdf/CLCReport_18112019.pdf> accessed 4 February 2022.

[53] See Rahul Bajaj, 'Towards a Framework for Scrutinizing Combinations in the Digital Market – A Roadmap for Reform' (Vidhi Centre for Legal Policy, 7 January 2022) <https://vidhilegalpolicy.in/research/towards-a-framework-for-scrutinizing-combinations-in-the-digital-market-a-roadmap-for-reform/> accessed 4 February 2022.

introduction of a deal value threshold of Rupees twenty billion involving a party that has substantial business operations in India.[54] Mergers and acquisitions that meet this threshold will have to be notified to the CCI for the assessment of potential anti-competitive effects. In addition to the proposed changes to competition law, the government's proposal to replace the Information Technology Act, 2000 with a new law, being referred to as the 'Digital India Act', may also have a direct bearing on big tech. The proposed law will reportedly contain specific provisions to check the gate keeping role of big tech players.[55]

In another notable development, in 2020, the CCI released a market study on competition in the e-commerce sector.[56] The study was built on information gathered from surveys, deliberations, and written submissions. It focused mainly on the practices of online marketplaces, online travel agents and online food delivery services. The CCI's report did not name any particular entities but it is clear that the dominant players in the markets under study would not only include some of the traditional big tech firms but also players beyond that. For instance, this would include food delivery firms like Zomato and Swiggy and travel booking operators like MakeMyTrip, all of which subsequently became the subject of investigations by the CCI.[57]

Competition law's relevant market-centric approach to examining anti-competitive conduct in the digital sector has to begin with an unpacking of the different layers of the ecosystem and locating the specific market in which competition issues are to be studied. It ensures that any determination of dominance necessarily has to be context-specific, taking into account product/service-specific features as well as geographical aspects.[58] This case-by-case analysis function of competition law is, therefore, neither designed to bring about any kind of sweeping actions against an entire sector nor targeted at big tech in general. Further, competition law remedies are also limited by their primary focus on the economic aspects of big tech's dominance

[54] The Competition Law (Amendment) Bill 2022, s 6.

[55] Deeksha Bhardwaj, 'India considers EU-like laws to check Big Tech dominance´ (*Hindustan Times*, 23 August 2022) <https://www.hindustantimes.com/india-news/india-considers-eu-like-laws-to-check-big-tech-dominance-101661190421041.html> accessed 31 October 2022.

[56] Competition Commission of India, 'Market Study on E-commerce in India: Key Findings and Observations' (8 January 2020) <www.cci.gov.in/images/marketstudie/en/key-findings-and-observations1653299843.pdf> accessed 16 May 2022.

[57] See *Federation of Hotel & Restaurant Associations of India v MakeMyTrip India (P) Ltd* 2021 SCC OnLine CCI 12; *National Restaurant Assn of India v Zomato Ltd 2022 SCC OnLine CCI* 22<https://www.cci.gov.in/antitrust/orders/details/6/0> accessed 16 September 2022.

[58] The Competition Act 2002, ss 2(r), (s), and (t).

while ignoring the broader political and societal implications. But, as elaborated in the previous section, the key features of big tech firms and concerns emanating on account of those features extend beyond the remit of competition enforcement. Competition law remedies for big tech, therefore, need to be accompanied by other types of policy initiatives, some of which are elaborated below.

B. Enhanced Obligations for 'Significant' Players

There are at least 3 examples of ex-ante regulatory proposals/actions in India that seek to impose enhanced obligations on 'significant' firms. The parameters for assessing significance in each context would invariably include big tech.

The first example relates to the obligations for 'significant social media intermediaries' under the new intermediary rules notified under the Information Technology Act, 2000 (IT Act) in 2021.[59] Section 79(1) of the IT Act, exempts intermediaries like telecom service providers, search engines, and social media firms from liability for any third-party information on their platforms as long as the intermediary does not play a role in managing or modifying that information. As per the new rules, a significant intermediary that has more than a specified number of registered users in India[60] (currently set at 5 million)[61] will have to adhere to an additional set of conditions to benefit from this exemption. These additional obligations include the appointment of a nodal contact for law enforcement requests, a resident grievance redressal officer, and ensuring traceability of the originator of a message in case of significant messaging services.

The user base-centric criterion implies that the IT Rules cover all entities that meet this threshold irrespective of whether they are popularly considered as big tech or not. For instance, the list of significant intermediaries includes the Indian social media platform Koo and messaging app ShareChat. Yet, it would appear that the foreign-based big tech intermediaries, which dominate verticals like search, social media, and messaging, might have been on top of the government's mind while framing the new rules. This is illustrated by requirements relating to having locally resident officials in India, which are particularly relevant to multinational firms. In his statement announcing the rules, the then Information Technology Minister, Ravi Shankar

[59] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (IT Rules).

[60] Ministry of Electronics and Information Technology, S.O. 942(E). (Notified on 25 February 2021).

[61] IT Intermediary Rules (n 59) r 2(v).

Prasad, also specifically highlighted the respective user bases of WhatsApp, YouTube, Facebook, Instagram and Twitter while explaining the need for more accountability from significant intermediaries.[62] The big tech link was made more explicit in the amendments brought about by the government to the new IT Rules in June 2022.[63] The changes, which include the strengthening of grievance redress mechanisms by intermediaries, were said to be targeted at removing "some of the infirmities and gaps that exist in the current rule vis-à-vis Big Tech platform[s]."[64]

The next set of developments relate to the proposals around the introduction of a comprehensive data protection law in the country. The legislative proposals in this regard include the Personal Data Protection Bill, 2019 (DP Bill, 2019) which was withdrawn by the government in August, 2022 and has now been replaced with the draft Digital Personal Data Protection Bill, 2022 (DP Bill, 2022).[65] Like its predecessor, the DP Bill, 2022 proposes certain additional obligations on 'significant data fiduciaries' over and above the general requirements for all data controlling entities. Compared to the intermediary rules, the DP Bill allows for greater discretion in the hands of the government in determining who would be treated as a significant player. It lists factors like volume and sensitivity of personal data processed and risk of harm from data processing that are to be taken into account while assessing the 'significance' of any entity or a class of entities.[66] Further, taking into account the recommendations of the Joint Parliamentary Committee that reviewed the DP Bill, 2019,[67] the DP Bill, 2022 also includes criteria like potential impact on India's sovereignty, risk to electoral democracy, security and public order. The obligations that would flow from being classified as a significant entity included requirements such as the appointment of privacy officers, the conduct of data protection impact assessments and privacy audits.

[62] Press Information Bureau, 'Union Ministers Prakash Javadekar and Ravi Shankar Prasad Address a Press Conference' (YouTube, 25 February 2021) <www.youtube.com/watch?v=H0eqWuj84-0> accessed 20 January 2022.

[63] Ministry of Electronics and Information Technology, Government of India, Press note dated June 6 2022, <https://www.meity.gov.in/writereaddata/files/Press%20Note%20dated%206%20June%2022%20and%20Proposed%20draft%20amendment%20to%20IT%20Rules%202021.pdf> accessed 8 September 2022.

[64] ibid.

[65] The Personal Data Protection Bill 2019 (DP Bill 2019); Digital Personal Data Protection Bill, 2022 (DP Bill 2022).

[66] DP Bill 2022 s 11.

[67] Report of the Joint Committee on the Personal Data Protection Bill 2019 (Lok Sabha Secretariat, 16 December 2021) <http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf> accessed 16 May 2022.

Lastly, the proposals for the regulation of Non-Personal Data (NPD) formulated by the Kris Gopalakrishnan Committee also contain specific requirements for designated large data businesses.[68] The recommendations suggest that significant data-controlling entities, demarcated based on factors like gross revenue, number of users, and revenue from consumers, will need to register themselves as data businesses before the proposed Non-Personal Data Protection Authority. This sets the path for mandatory disclosure of the metadata held by these entities and sharing of certain categories of data with the government and others acting in public/community interest.

C. Data Control

Both the data governance initiatives discussed above seek to define the terms on which businesses (and the government) can process data and create a framework for sharing this data with others. The NPD Committee's report, in particular, mentions businesses like Facebook, Google, and Amazon to illustrate the 'imbalance in data and digital industry', which lies at the core of its data sharing recommendations.[69] Claims about the economic value of data and the power and significance enjoyed by a 'handful of companies' controlling it have also been used as a framing device in other contexts. This includes the draft e-commerce policy that was put out by the Department for Promotion of Internal Industry and Trade in 2019.[70] Without naming any specific entities, the draft e-commerce policy spoke of the data controlling and gate keeping functions of large social media platforms and search engines, and used that as a basis for the assertion of data sovereignty.

Yet another dimension of this debate relates to the challenges faced by law enhancement agencies in gaining access to data that is under the control of foreign entities. This is a commonly cited argument for imposing data localisation norms.[71] For instance, the report of the Justice Srikrishna-led Expert Committee on data protection identified the foreign ownership of information intermediaries like Facebook, Google, Amazon, and Uber, its impact on the local data economy, and concerns of foreign surveillance as grounds for

[68] Kris Gopalakrishnan et al., *Draft Report by the Committee of Experts on Non-Personal Data Governance Framework* (16 December 2020) <https://static.mygov.in/rest/s3fs-public/mygov_160975438978977151.pdf> accessed 4 February 2022.

[69] Committee of Experts on Non-Personal Data (n 68) 40.

[70] Department for Promotion of Internal Industry and Trade, 'Draft National e-Commerce Policy: India's Data for India's Development' (February 2019) <https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf>, accessed 20 January 2022.

[71] Rishab Bailey and Smriti Parsheera, 'Data Localization in India: Paradigms and Processes', (2021) 9 CSI Transactions on ICT 137.

data localisation.[72] All these developments point toward a trend of the state seeking greater control over the data that is currently seen as being locked up in the hands of dominant tech players. By extension, attempts to democratise data access through data pooling and sharing initiatives, are being designed with an express intention to exclude big tech players. This has, for instance, been made explicit in the discussions around the data pools to be created under the government's draft National Data Governance Framework, which will not be accessible to big tech.[73]

D. General Compliance with Laws

The large user base of big tech entities and their societal impact often leads to their interactions with courts and policymakers concerning the enforcement of various laws. For instance, intermediaries have been involved in actions before the Indian courts for the implementation of laws relating to hate speech, child pornographic material, non-consensual sexual content, defamatory content, copyright violations, etc.[74] On some occasions, the foreign ownership of large intermediaries and limited local decision-making presence has been noted to be a barrier to securing cooperation for compliance with local laws. The IT Rules and Data Governance proposals discussed earlier are partially geared towards addressing these concerns of limited accountability through requirements of local presence and registration of large operators.

In addition to government agencies and courts, Parliamentary Committees have also been a site for demanding better accountability from big tech. Recently, the Parliamentary Standing Committee on Finance directed that it would be calling companies like Google, Apple, Facebook, Twitter, Amazon, and Microsoft to discuss the competition challenges associated with digital markets.[75] Some of these entities have also been summoned in the past for hearings before the Parliamentary Standing Committee on Information

[72] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 18 September 2022, 92.

[73] Akhil Sur, 'Big Tech Won't be Beneficiary of National Data Governance Framework: MeitY' (*Money Control*, 14 June 2022) <www.moneycontrol.com/news/business/big-tech-wont-be-beneficiary-of-national-data-governance-framework-meity-8686881.html> accessed 8 September 2022.

[74] Varun Sen Bahl, Faiza Rahman and Rishab Bailey, 'Internet Intermediaries and Online Harms: Regulatory Responses in India' (2020) Data Governance Network Working Paper 06<https://www.datagovernance.org/files/research/BahlRahmanBailey_-_Paper_6-2.pdf> accessed 20 January 2022.

[75] Press Trust of India (n 51).

Technology on the issue of misuse of social media platforms.[76] Another Parliamentary panel that made recommendations on the monitoring and take down of child pornographic content on social media had engaged with the representatives of these companies along with those of others like TikTok and ShareChat.[77]

While outlining the general trends in terms of India's policy responses, it is worth noting that actual actions involving big tech are often subjective and individualised in nature. In other words, such actions are shaped not only by general notions of 'bigness' but by a range of other political, strategic, and pragmatic considerations. The use of the terms 'political' or 'strategic' here captures all sorts of external considerations, power equations, and interest groups that may play a part in shaping regulatory enforcement actions or other types of discretionary outcomes. The abovementioned ban of a large number of Chinese apps is a clear example along with the 2 other instances discussed below.[78]

The first example relates to the political-economy forces that resulted in the use of foreign direct investment (FDI) policy as a type of ex-ante competition intervention to reshape the business models of companies like Amazon and Walmart-owned Flipkart.[79] The FDI norms introduced through Press Note No. 2 of 2018 restricted e-commerce marketplaces with foreign investment from owning the inventory to be sold on their platform or influencing sale prices in any manner.[80] Although aimed at creating a level playing field in the e-commerce sector, the choice of FDI rules to introduce these

[76] IANS, 'Parliamentary Committee on IT Summons Google, Facebook on June 29' (*Business Standard*, 28 June 2021) </www.business-standard.com/article/technology/parliamentary-committee-on-it-summons-google-facebook-on-june-29-121062800560_1.html> accessed 20 January 2022.

[77] Jairam Ramesh et al., *Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole* (2020) <https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf> accessed 2 February 2020.

[78] The reasons given for the ban included data security and privacy considerations, which included mining and access of the data by those acting against India's national security and defence interests. See Ministry of Electronics & IT, 'Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order' (*Press Information Bureau*, 29 June 2020) <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206> accessed 26 May 2022.

[79] Ministry of Commerce & Industry, 'E-Commerce Business Model' (*Press Information Bureau*, 11 December 2019) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1595850> accessed 2 February 2022.

[80] Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, 'Press Note 2 of 2018 Review of Policy on Foreign Direct Investment in e-Commerce' (26 December 2018) <www.dpiit.gov.in/sites/default/files/pn2_2018.pdf> accessed 20 September 2022.

conditions has been questioned for creating an uneven playing field between foreign and domestic firms.[81] Notably, these developments come at the back of long-standing political pressures by domestic industry groups like the All India Online Vendors Association, the Confederation of All India Traders, and the Swadeshi Jagran Manch to safeguard small vendors from the exclusionary and predatory practices of big e-commerce tech platforms.[82]

Using the FDI policy as a regulatory tool meant that the treatment was targeted not just at the type of conduct in question but also at the politics of who owned those entities. Recently, the Parliamentary Committee on Promotion and Regulation of E-Commerce in India also took note of this issue and called for a holistic framework to govern anti-competitive practices in the e-marketplace business "irrespective of the marketplace being funded by foreign or domestic entities."[83]

The next example is about the government's selective and aggressive enforcement of the Intermediary Rules against Twitter soon after these rules came into effect. This action, which included police raids at Twitter's office, came about in the context of the government's publicly expressed displeasure against the attachment of a 'manipulated media' tag on tweets put out by members of the ruling political party.[84] Reports revealed that Twitter's interim compliance status on requirements of having designated local employees under the Intermediary Rules was similar to that of others like Google and WhatsApp.[85] Yet there was a stark difference in how the

[81] World Bank, *World Development Report 2021: Data for Better Lives* (March 2021), <www.worldbank.org/en/news/press-release/2021/03/24/stronger-data-systems-needed-to-fight-poverty>, accessed 4 February 2022, 235; Anand Raghuraman, *E-Commerce Policy for a New Digital India*, (*Atlantic Council*, 19 April, 2022) <www.atlanticcouncil.org/in-depth-research-reports/issue-brief/e-commerce-policy-for-a-new-digital-india/>, accessed 16 May 2022.

[82] S. Shanthi, 'Amazon, Flipkart Vs CAIT: A Timeline Of The Row' (*Entrepreneur India*, 20 December 2021) <www.entrepreneur.com/article/403672> accessed 19 May 2022; Press Trust of India, 'MNC E-commerce Giants Violating FDI Norms: CAIT' (*Economic Times Retail*, 15 March 2022) <https://retail.economictimes.indiatimes.com/news/e-commerce/mnc-e-commerce-giants-violating-fdi-norms-cait/90218996> accessed 19 May 2022.

[83] Department related Parliamentary Standing Committee on Commerce, 'Promotion and Regulation of E-Commerce in India (172nd Report)', (June 2022) <https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/13/159/172_2022_6_14.pdf> accessed 8 September 2022, 5.

[84] Yuthika Bhargava, 'Government Asks Twitter to Remove 'Manipulated Media' Tag from Tweets Related to 'Congress Toolkit'' *The Hindu* (New Delhi, 21 May 2021) <www.thehindu.com/news/national/government-asks-twitter-to-remove-manipulated-media-tag-fom-tweets-related-to-congress-toolkit/article34615696.ece> accessed 20 February 2022.

[85] Aditi Agrawal, 'From Google to Whatsapp, and Twitter to Koo, Assessing the Compliance Status of Intermediaries' (*Forbes India*, 17 June 2021) <www.forbesindia.com/article/take-one-big-story-of-the-day/from-google-to-whatsapp-and-twitter-to-koo-assessing-the-compliance-status-of-intermediaries/68531/1> accessed 20 February 2022; Aditi Agrawal,

compliance status of these companies was treated by the government with Twitter seemingly being singled out for reasons that went beyond its immediate acts of delay in compliance with the new rules. The company also attracted political ire for the temporary suspension of the Twitter account of the then Information Technology Minister, Ravi Shankar Prasad, due to a copyright-related issue.[86]

The above discussion reveals that India is seeing a lot of developments aimed at asserting greater regulatory control over the technology sector. While not all of this is explicitly targeted at big tech, the names of big tech firms often come up as examples while discussing the need for, or application of, regulatory interventions. This seems logical given the scale and market power of these firms, which makes them obvious targets of actions aimed at controlling anti-competitive activities and regulating other economic and social consequences in the digital sphere. Further, it is also clear that policy actions tend to be subjective and individualised, shaped by the peculiarities of different business models and a range of political, strategic, and pragmatic considerations. This can sometimes lead to particular entities being treated differently from other similarly placed actors, including other big tech players.

Having discussed the 4 broad types of policy responses influencing the regulation of big tech, I now turn to discuss the fifth type of response that involves the use of technical architectures to counter the status quo of dominance and control in different segments of the digital ecosystem.

IV. Countering Power Through Technical Architectures: Rise of 'Alt Big Tech'

In the last decade, India has seen the emergence of a new model of digital governance that relies on the use of open API-based solutions to implement

'The Woes and Woes of Twitter in India' (*Forbes India*, 30 June 2021) <www.forbesindia.com/article/special/the-woes-and-woes-of-twitter-in-india/68851/1> accessed 20 February 2022.

[86] Vivek Punj, 'Twitter Blocks Ravi Shankar Prasad's Handle over Violation of Copyright Norms; Unblocks Later' (*Live Mint*, 26 July 2021) <www.livemint.com/news/india/twitter-blocks-ravi-shankar-prasad-s-handle-over-violation-of-copyright-norms-11624616188732.html> accessed 18 September 2022; Department Related to parliamentary Standing Committee on Commerce, 'Promotion and Regulation of E-Commerce in India (107th Report)' (Rajya Sabha Secretariat, June 2022) <https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/13/159/172_2022_6_14.pdf> accessed 8 September 2022.

what is often described as India's open digital infrastructure.[87] These digital infrastructure projects can broadly be classified under 2 heads. The first consists of projects that are implemented and controlled directly by the state, as seen in the case of Aadhaar and the Ayushman Bharat Digital Mission in the health sector. The second category, which is the focus of this Section, consists of architectures or networks that are actively backed by the state but are controlled by industry-owned not-for-profit organisations set up for that purpose. I discuss the NPCI's UPI system, the DEPA consent management architecture, and the latest ONDC initiative in the e-commerce sector as examples of this model.

A. An Introduction to the Technical Architectures

The NPCI was established in 2008 as a private not-for-profit company to create enabling infrastructure for the banking and payment systems in India.[88] It is a joint initiative of the Reserve Bank of India ('RBI') and the Indian Banks' Association and is largely owned by banks although some non-bank payment operators have recently been included as smaller shareholders.[89] The UPI platform, which facilitates instant interbank payments, is one of NPCI's key offerings.[90] UPI has seen phenomenal growth in the last few years – it saw a peak of 5.58 billion monthly transactions in April 2022.[91] This progress is often attributed to the convenience, interoperability, and outreach of the platform.[92] Several big tech players like Google, WhatsApp, and Amazon have been authorised to act as third-party application providers in the UPI system. This means that they can connect with the UPI system to facilitate payment transactions between users of their apps and account holders of different banks.

The next system under discussion is a new architecture called DEPA that was created to enable easier sharing of data between entities relying on the user's consent. A 2020 discussion paper published by the NITI Aayog,

[87] NITI Aayog (n 14).

[88] 'An Introduction to NPCI and its Various Products' (*NPCI*) <www.npci.org.in/who-we-are/about-us> accessed 4 February 2022.

[89] 'Equity Shareholding Pattern as on 31st August 2022 (*NPCI*, 2022) <www.npci.org.in/PDF/npci/corporate-governance/shareholding-pattern.pdf> accessed 4 February 2022.

[90] See (n 88) for a full list of the NPCI's product offerings.

[91] Subrata Panda, 'UPI hits record high in April with 5.58 bn transactions worth Rs 9.83 trn' *Business Standard* (Mumbai, 2 May 2022) <www.business-standard.com/article/finance/upi-hits-record-high-in-april-with-5-58-bn-transactions-worth-rs-9-83-trn-122050100480_1.html> accessed 24 May 2022.

[92] Anto T. Joseph, 'How UPI is Making India's Digital Economy Boom' (*Fortune India*, 24 April 2021) <www.fortuneindia.com/enterprise/how-upi-is-making-indias-digital-economy-boom/105433> accessed 4 February 2022.

articulated DEPA's objectives of giving individuals more agency over their data and enabling innovation by breaking down data monopolies.[93] These goals are to be achieved through the operation of a new class of intermediaries called consent managers who will facilitate the sharing of data between businesses relying on an electronic consent management protocol. DEPA has already been deployed in the financial sector through RBI's Account Aggregator's framework and in the digital health sector under the Ayushman Bharat Digital Mission. The API specifications for the Account Aggregators have been put out by the Reserve Bank Information Technology Private Limited (ReBit)[94] and a non-profit industry body called the DigiSahamati Foundation has been set up to develop and enforce the multipartite contractual arrangements between ecosystem participants.[95]

The third, and most recent, example in this list is the ONDC, a project that aims to digitise the entire e-commerce value chain, standardise its operations, and promote the inclusion of more suppliers.[96] The ONDC has been described as a technology-based network that will enable all kinds of e-commerce transactions in goods and services, allowing buyers and sellers across platforms to engage with one another.[97] The roll-out of this initiative is being overseen by the Department for Promotion of Industry and Internal Trade (DPIIT) with the actual implementation being done by a private sector-led non-profit company fashioned along the lines of the NPCI.[98] ONDC's shareholders include some of India's largest banks like HDFC, Kotak Mahindra, Axis Bank, State Bank of India and Punjab National Bank.[99] The system

[93] NITI Aayog (n 14).

[94] 'Account Aggregator Ecosystem API Specifications' (*ReBIT*) <https://api.rebit.org.in/> accessed 24 May 2022.

[95] Sahamati, 'Participation Terms' (*Sahamati*) <https://sahamati.org.in/participation-terms/> accessed 24 May 2022.

[96] Ministry of Commerce & Industry, 'Setting up of Advisory Council for Open Network for Digital Commerce (ONDC)' (*Press Information Bureau*, 5 July 2021) <https://pib.gov.in/PressReleasePage.aspx?PRID=1732949> accessed 20 May 2022.

[97] Quality Council of India, 'Request for Proposal For Onboarding of Consulting Firm(s) for Technology Advisory and Product Management for Open Network for Digital Commerce', Reference No. QCI/PPID/1021/065 <https://qcin.org/public/uploads/ck-docs/1634131716.RFP%20for%20Onboarding%20of%20Consulting%20Firm(s)%20for%20Technology%20Advisory%20&%20Product%20Management%20(1).pdf> accessed 20 May 2022.

[98] Ministry of Commerce & Industry, 'Shri Piyush Goyal reviews Open Network for Digital Commerce' (*Press Information Bureau*, 26 October 2021) <https://dpiit.gov.in/sites/default/files/PressRelease-CIM-26-10-2021-ONDC_27Oct2021.pdf> accessed 20 May 2022

[99] Melissa Cyrill and Naina Bhardwaj, 'What is ONDC? India's Plan to Take on E-Commerce Giants Amazon, Flipkart', (*India Briefing*, 27 May 2022) <www.india-briefing.com/news/what-is-the-open-network-for-digital-commerce-ondc-and-how-will-it-impact-ecommerce-in-india-23463.html/> accessed 20 May 2022.

is currently being piloted in 5 regions – Delhi NCR, Bengaluru, Bhopal, Shillong, and Coimbatore.[100]

All of these initiatives trace their origin to what is referred to as the India Stack framework – a collection of APIs developed by the private think-tank Indian Software Product Industry RoundTable (iSPIRT) and implemented in cooperation with different government and private agencies. India Stack consists of 4 layers of technology-based infrastructure – the presence-less, paperless, cashless, and consent layers – that are meant to facilitate easier digital transactions.[101] UPI and DEPA directly correspond with the cashless and consent layers of India Stack while ONDC represents a sectoral application of the different functionalities of India Stack. Nandan Nikelani, the former Chairperson of the Unique Identification Authority of India, has been a champion of India Stack and has played an advisory role in the development of all the systems being discussed here.[102]

B. Interaction with Big Tech

Unlike the regulatory initiatives discussed in Section 4, which were directly aimed at controlling the behaviour of big tech, the architectures described in this Section focus more on changes to the surrounding ecosystem. This is sought to be done mainly through the introduction of open APIs and standardisation initiatives aimed at facilitating interoperability.

The lack of interoperability is a major contributor to the dominance of big tech. It feeds into strengthening the user base of big tech entities and their resulting ability to gather vast amounts of data intelligence. For instance, messaging platforms are presently designed in a manner that their users cannot interact with the users of other platforms. Similarly, sellers and buyers on e-commerce platforms cannot automatically search and transact across

[100] ibid.

[101] Product Nation/ iSPIRT, *India Stack - Towards Presence-less, Paperless and Cashless Service Delivery. An iSPIRT Initiative* (*Slideshare*, 1 March 2016) <www.slideshare.net/ProductNation/india-stack-towards-presenceless-paperless-and-cashless-service-delivery-an-ispirt-initiative> accessed 8 September 2022; 'Frequently asked questions and their answers' (*India Stack*) <https://indiastack.org/faq.html> accessed 8 September 2022.

[102] TNN, 'Nilekani Advises NPCI on Aadhaar-backed Payments' *The Times of India* (Mumbai, 30 June 2015) <https://timesofindia.indiatimes.com/business/india-business/nilekani-advises-npci-on-aadhaar-backed-payments/articleshow/47873710.cms> accessed 26 May 2021; Nanadan Nilekani, 'How To Empower 1.3 Billion Citizens With Their Data' (*Product Nation Blog*, 6 August 2018) <https://pn.ispirt.in/empowercitizenswiththier-data/> accessed 26 May 2021; Pranav Mukul, 'ONDC: Looking to Open Source E-comm Processes, DPIIT Sets up 9-member Panel with Nilekani, R.S. Sharma' *The Indian Express* (New Delhi, 6 July, 2021) <https://indianexpress.com/article/business/looking-to-open-source-e-comm-processes-dpiit-sets-up-panel-7390607/> accessed 26 May 2021.

different platforms. This generates strong network effects for existing platforms – users find it most efficient to be on a platform that already has a significant user base. Introducing interoperability of the kind that enables information flows on the Internet, emails exchanges across different accounts, and communications between telecommunication networks, can, therefore, be an effective way of countering the dominance of big tech.[103]

The NITI Aayog discussion paper on DEPA gives several examples of large data controlling entities or fiduciaries in the present system that hold user information in 'data silos.' This list includes big tech players like Amazon, Google, and WhatsApp but also others like the State Bank of India and Life Insurance Corporation in the financial sector and Indian technology companies like Paytm, UrbanClap, and Ola.[104] Since much of this discussion relates to the transmission of personal data, the legal and tactical positioning of DEPA has focused on the need for 'empowering' users and granting greater agency to them. But the crux of DEPA lies in creating a market for the exchange of data and, in that process, diluting the effects of the data monopolies that advantage the larger market players. As per DEPA's designers, interoperability is the core advantage being offered by the consent managers framework.[105]

Similarly, in the case of the ONDC, interoperability and unbundling are identified as its main features.[106] In contrast to a system of end-to-end e-commerce management by large platforms, the ONDC proposes to unbundle each step, thereby allowing multiple service providers to compete for services like order and inventory management, payment processing, logistics, etc.[107] It will also allow for cross-platform transactions among entities that choose to join the network. ONDC has been built using the beckn protocol, a set of specifications that enable the creation of decentralised networks.[108] The ONDC is being positioned as an enabler of new e-commerce transactions but also as a means to 'remove monopolistic environments' in the Indian e-commerce sector.[109] News reports have been more explicit in calling it an

[103] Parsheera et. al (n 47)

[104] NITI Aayog (n 14), p. 26.

[105] NITI Aayog (n 14), p. 41.

[106] ONDC, 'Talk by T. Koshy, Chief Executive Officer of ONDC, Future of Digital Commerce with ONDC: Startup Innovation Week' (*YouTube*, 16 January 2022) <www.youtube.com/watch?v=IZSVoG4Pljw> accessed 22 May 2022.

[107] ibid.

[108] 'What is beckn?' <https://becknprotocol.io/> accessed 8 September 2022. The Beckn Foundation set up by Nanadan Nilekani, Promod Varma and Sujith Nair is described as the 'genesis author' and 'angel donor' of the beckn protocol. Beckn Foundation <https://becknfoundation.org/> accessed 8 September 2022.

[109] Ministry of Commerce & Industry (n 13).

initiative that will "erode Amazon and Walmart-owned Flipkart's online domination."[110] Therefore, both the DEPA and the ONDC intend to speak to the challenges posed by the dominance of big tech in the areas of data intelligence and e-commerce.

This has, however, played out differently in the case of the NPCI. As noted earlier, the NPCI was created to strengthen the country's payments infrastructure, a space that has traditionally offered little scope for participation by non-banking entities. In multi-faceted technological ecosystems, each market segment has its own dynamics, constraints, and dominant players. In the case of the digital payments sector, banks have traditionally been and remain, the dominant players. Through the UPI, the NPCI created a platform that allows entities other than banks to participate in one particular segment of the digital payments market. But, as things turned out, big tech players turned out to be among the largest gainers of the UPI system.

The UPI app market is currently dominated by PhonePe (an indirect subsidiary of Walmart) and Google Pay with the Indian company Paytm holding the third position.[111] Commentators have attributed this to the scale and technology benefits enjoyed by these players, the use of cashback, rewards and other incentives, and flaws in the operationalisation of the interoperability requirements.[112] Given what we know about the market power and personal data excesses of big tech, this situation gives rise to a fair number of concerns. In a petition filed before the Supreme Court, Rajya Sabha member Binoy Viswam has questioned the RBI and the NPCI for allowing big tech giants to gain such a dominant position in the payments space.[113] The RBI itself has also articulated concerns around the growing presence of big techs in financial services.[114]

[110] Bhaswar Kumar, 'Can Open Networks for Digital Commerce take on Amazon & Walmart?' *Business Standard* (New Delhi, 2 May 2022) <www.business-standard.com/podcast/technology/can-open-networks-for-digital-commerce-take-on-amazon-walmart-122050200046_1.html> accessed 22 May 2022.

[111] As of January, 2022, PhonePe, GooglePay and Paytm accounted for 46.4%, 34.4% and 15.4%, respectively, of the UPI market in terms of number of transactions. *See* Laxitha Mundhra, 'PhonePe Maintains Lead In UPI With 49% Market Share In Jan 2022, WhatsApp At 0.02%' (*Inc42*, 9 Feb 2022) <https://inc42.com/buzz/phonepe-maintains-lead-in-upi-with-49-market-share-in-jan-2022-whatsapp-at-0-02/> accessed 23 May 2022.

[112] Aaryaman Vir and Rahul Sanghi, 'The Internet Country: How India Created a Digital Blueprint for the Economies of the Future', (*Tiger feathers Substack*, 15 January 2021) <https://tigerfeathers.substack.com/p/the-internet-country?s=r> accessed 23 May 2022.

[113] Legal Correspondent, 'SC Issues Notice to the RBI, NPCI Among Others' *The Hindu* (New Delhi, 16 October 2020) <https://www.thehindu.com/news/national/sc-issues-notice-to-the-rbi-npci-among-others/article32866455.ece> accessed 4 February 2022.

[114] Reserve Bank of India, 'Financial Stability Report Issue No. 23' (July 2021), <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1174> accessed 4

Similar concerns were perhaps behind the NPCI's decision to impose a volume cap of 30% of total transactions on any UPI app.[115] Existing players have been given until the end of 2022 to comply with these requirements.[116] Although the NPCI did not clearly explain its rationale for these actions, its circulars refer to the need to address "risks in the UPI ecosystem" and "provide diverse opportunities to the UPI ecosystem."[117] At the same time, the NPCI also imposed a unique cap of 20 million users on WhatsApp while allowing it to join the UPI platform. The cap, which was subsequently revised to 40 million and recently 100 million, was supposed to ensure that the UPI system would not be overwhelmed by WhatsApp's large user base of approximately 400 million users.[118] While this appears to be a logical concern, the restriction remains at variance with the requirements applicable to other players in the UPI ecosystem that are bound by a general cap of 30% market share but with no individual user limits.

This supplements the earlier point about the discretionary nature of the actions involving big tech, motivated by various strategic and pragmatic considerations. But unlike the previous examples, the authority, in this case, was not exercised by an agency of the state but by a private entity operating with the endorsement of the state. This offers a useful segue into the next segment that examines the NPCI as an example of 'alt big tech' in India.

V. Characterising the New Technical Systems as 'Alt Big Tech'

The survey of the literature in Section 2 highlighted the following key characteristics of big tech – financial resources and market power, data intelligence,

February 2022, 9-10.See also Juan Carlos Crisanto, Johannes Ehrentraud and Marcos Fabian, Big Techs in Finance: Regulatory Approaches and Policy Options (Bank for International Settlements, 2021).

[115] 'Guidelines on volume cap for Third Party App Providers (TPAPs) in UPI' (*NPCI*, 5 November 2020) <www.npci.org.in/PDF/npci/upi/circular/2020/OC-97-Guidelines-for-TPAPs-in-UPI.pdf> accessed 23 May 2022.

[116] 'Standard Operating Procedure (SOP) – Market Share Cap for Third Party Application Providers' (*NPCI*, 25 March 2021) <www.npci.org.in/PDF/npci/upi/circular/2021/standard-operating-procedure-sop%E2%80%93market-share-cap-for-third-party-application-providers-tpap.pdf> accessed 23 May 2022.

[117] NPCI (n 115 and n 116).

[118] Sethu Pradeep, 'National Payments Corporation Of India Allows WhatsApp Pay To Double Users' (*Inc42*, 27 November 2021) <https://inc42.com/buzz/npci-allows-whatsapp-pay-to-double-users-to-40-mn/> accessed 4 February 2022; Shayan Ghosh, 'NPCI Permits WhatsApp to Raise UPI User Base to 100 million' (*LiveMint*, 14 April 2022) <www.livemint.com/industry/banking/npci-permits-whatsapp-to-raise-upi-user-base-to-100-million-11649880595039.html> accessed 19 May 2022.

infrastructural capabilities, and societal impact. The technical systems discussed in the previous Section do not share several of these features, notably, big tech's profit motivations, market capitalization-linked economic power, and cross-border reach. On the contrary, they are said to be propelled by a sense of public-spiritedness that may well be the antithesis of big tech.[119] This vision of having "private companies with a public purpose" was originally articulated by the Nandan Nilekani-led Technology Advisory Group for Unique Projects. The group advocated the creation of National Information Utilities (NIUs) that would implement technology-related infrastructure projects, citing the NPCI as an example of a comparable system.[120]

While systems like the UPI, the DEPA, and the ONDC deviate from the design principle of "making reasonable profits"[121] set out for NIUs, they share the same general model of state-backed, private-sector-led digital infrastructure. The proliferation of this model has attracted several concerns. This includes questions about the privatisation of public data[122] and the true extent of 'openness' in the development and functioning of the systems, particularly on account of the disproportionate control exercised by some private actors in the process.[123]

In this paper, I focus mainly on the competition and accountability implications of these developments, using the term 'alternative (or alt) big tech' to describe the technical systems under study. This is designed to capture their positioning as an alternative to the present status quo of digital monopolisation by a handful of tech firms as well as the ability of these new systems to become the new centres of power and control in different areas of the digital ecosystem. This power emanates from the state's active backing of these projects, their designs of serving as the infrastructural core in the relevant sectors, and the emphasis on population-level deployment strategies. Since these are still early days for the DEPA and the ONDC projects, the observations in

[119] ONDC, 'Talk by Nandan Nilekani, Advisory Board member of ONDC, Future of Digital Commerce with ONDC: Startup Innovation Week' (YouTube, 16 January 2022) < www.youtube.com/watch?v=IZSVoG4Pljw> accessed 22 May 2022.

[120] Nandan Nilekani et al., 'Report of the Technology Advisory Group for Unique Projects' (31 January, 2011) <www.nrcddp.org/file_upload/tagup_report.pdf> accessed 8 September, 2022.

[121] ibid 10.

[122] Usha Ramanathan, 'Aadhaar - From Welfare to Profit' in Reetika Khera (ed), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, 2019) 174.

[123] Bhavani Seetharaman, 'Findings: Large-scale digital public infrastructure' (*HasGeek*, 10 March 2022) <https://hasgeek.com/OpenInnovation/mozilla-open-innovation-project-understanding-innovation-in-the-indian-tech-ecosystem/sub/findings-large-scale-digital-public-infrastructure-MokD4NE9eWVhKrcGikEicd> accessed 22 May 2022.

this part draw mainly on the NPCI's experience.[124] I make 4 broad observations in this context – i) state endorsement as a source of power, ii) scale and data effects, iii) infrastructure lock-in, and iv) accountability limitations.

First, each of the systems under consideration has been promoted by different agencies of the state. The endorsing agencies in the case of the DEPA include the NITI Aayog, which released a discussion paper on the subject, the RBI and other financial regulators, and the National Health Authority all of whom have adopted the architecture. In the case of the ONDC, the project was announced and is directly being overseen by the DPIIT in the Commerce Ministry. In the NPCI's case, the state backing comes from the RBI and, in some ways, the Ministry of Finance.[125] Their control over the organisation has also been illustrated by reports of the RBI's actions to override the NPCI Board of Directors' decision concerning the appointment of its Chief Executive in 2018.[126]

At present, the NPCI is the only entity that has been authorised by the RBI to function as a retail payments organisation in India.[127] In its submissions before the Supreme Court, the RBI noted that the NPCI is solely responsible for allowing an entity to operate on UPI as well as to monitor compliance with the system's rules and procedures.[128] This allows it to unilaterally set the rules of the game, including who gets to participate and on what terms. As a result, the NPCI becomes an essential facility for any non-banking entity that wants to operate in the retail payments space through the UPI. Several commentators have highlighted this to be a problem in terms of the NPCI acting as an infrastructure provider as well as a quasi-regulator of the

[124] The NPCI has been in operation for over a decade and is often invoked as a model for other digital infrastructure projects, particularly in the context of the UPI.

[125] It has been reported that the Ministry actively asked banks to promote NPCI's RuPay card system over Visa and Mastercard leading to allegations of preferential treatment. See Reuters, 'Govt Approves Rs 1,300 Crore Plan To Promote RuPay Debit Cards, Rivaling Visa, Mastercard' (*The Wire*, 16 December 2021) <https://thewire.in/business/govt-approves-rs-1300-crore-plan-to-promote-rupay-debit-cards-rivaling-visa-mastercard> accessed 4 February 2022.

[126] The report indicates that the RBI's actions were influenced by the Government's preference and the recommendations of Nandan Nilekani who acted as an advisor to the NPCI. See Anuj Srivas, 'How the RBI Forced National Payments Body to Hire Government Favourite as CEO', (*The Wire*, 14 February 2018) <https://thewire.in/business/rbi-npci-digital-india> accessed 24 May 2022.

[127] Reserve Bank of India, 'Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India' (3 January 2022) < www.rbi.org.in/scripts/publicationsview.aspx?id=12043> accessed 4 February 2022.

[128] Counter Affidavit on behalf of the Reserve Bank of India in *Binoy Viswam v. RBI*,2021 SCC OnLine SC 273< www.livelaw.in/pdf_upload/wp-1038-of-2020-sc-case-binoy-viswam-vs-rbi-rbi-counter-affidavit-final1-388252.pdf> accessed 2 February 2022, 14-15.

system.[129] Going forward, the DigiSahamati Foundation and the ONDC are likely to play a similarly powerful role in the Account Aggregator and e-commerce spheres but with the additional consideration that, unlike the NPCI, there is no specific regulatory structure to govern them.[130]

Second, the technical systems under study are often described as India's technology-based products designed to achieve 'population scale transformation at start-up speed'.[131] The achievement of significant scale is, therefore, core to each of the projects. In the NPCI's case, its scale advantage spans a range of verticals. The UPI system currently constitutes the single largest retail payment system in the country.[132] In addition to the peer-to-peer transactions and merchant payments offered through the UPI, the NPCI also operates systems for utility bill payments and subscriptions, toll collection, Aadhaar-enabled payments, and the latest payment voucher system called e-RUPI. It sees millions of transactions every month across these verticals, which adds to its scale of coverage and socio-economic impact.[133]

In its capacity as the operator and monitor of all these systems, the NPCI potentially has access to vast amounts of data along with the ability to gather behavioural and transactional intelligence from such data. For instance, as per the rules governing UPI, the NPCI can call for any UPI-related data,

[129] Advait Palepu, 'Deciphering NPCI's Dominance In Digital Payments' (*Medianama*, 28 October 2020) < www.medianama.com/2020/10/223-deciphering-npcis-dominance-in-digital-payments/> accessed 4 February 2022; Amol Kulkarni and Swasti Gupta, 'Submission to the Reserve Bank of India for Managing Concentration Risk and Promoting Competition and Innovation in Retail Payments Sector' (*CUTS International*) <https://cuts-ccier.org/pdf/CUTS_Submission_to_RBI_on_Innovation_and_Competition_in_Retail_Payments.pdf> accessed 4 February 2022; Arundhati Ramanathan, 'NPCI, The God of Many Things' (*The Ken*, 26 February 2018) <https://the-ken.com/story/npci-god-many-things/> accessed 4 February 2022.

[130] The NPCI falls under the supervision of the RBI under the Payments and Settlements Act, 2007.

[131] ONDC, 'Talk by Adil Zainulbhai, Chairman of the Quality Council of India at Future of Digital Commerce with ONDC: Startup Innovation Week' (*YouTube*, 16 January 2022) <www.youtube.com/watch?v=IZSVoG4Pljw> accessed 22 May 2022.

[132] ET Online, 'UPI currently the single largest retail payment platform in the country: Economic Survey' (*The Economic Times,* 31 January 2022) <https://economictimes.indiatimes.com/industry/banking/finance/upi-currently-the-single-largest-retail-payment-platform-in-the-country-economic-survey/articleshow/89242932.cms> accessed 22 May 2022.

[133] For instance, in the month of December 2021 there were 380 million payment transactions on UPI See 'UPI Statistics' (*NPCI*) <www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics> accessed 18 September 2022; 'FASTag Statistics' (*NPCI*) <www.npci.org.in/what-we-do/netc-fastag/netc-ecosystem-statistics), 'AePS Statistics' (*NPCI*) <www.npci.org.in/what-we-do/aeps/product-statistics/2021-22> accessed 18 September 2022 ; 'Bharat BillPay Statistics' (*NPCI*) <www.npci.org.in/what-we-do/bharat-billpay/product-statistics/bbpcu-monthly-product-statistics> accessed 18 September 2022.

information, and records from the system's participants.[134] Concerns about data safety and privacy have also come up specifically in the context of access to data collected by FASTag, the NPCI's electronic toll collection system.[135] However, there is little clarity about what sort of data aggregation and processing is being carried out by the NPCI, which connects with the larger issues of transparency and accountability discussed later.

Third, the resources spent on building and scaling a particular digital infrastructure and the emergence of strong interest groups in that process can create a situation of infrastructure lock-in. Future innovation, therefore, becomes restricted to 'innovation by' the existing entity as opposed to the emergence of radically different systems or models that can compete with it. This is illustrated, to some extent, by the developments surrounding the RBI's proposal to allow new 'umbrella entities' (NUEs) to compete with the NPCI in the provision of payments infrastructure.[136]

In 2019, the RBI acknowledged that the concentration of payment system operations in a single entity can give rise to systemic and operational risks, lack of innovation and upgradation, and monopolistic trends.[137] This led to a proposal to open the payments infrastructure market to other NUEs which saw interest from several consortiums that included banks and other large domestic and multinational corporations.[138] Several commentators responded to these developments with concerns about the risks that big tech's

[134] 'Roles & Responsibilities of NPCI' (*NPCI*) <www.npci.org.in/what-we-do/upi/roles-responsibilities> accessed 18 September 2022; A 2019 audit of NPCI's systems had found several lapses in its data protection systems, such as the storing of personal data like card numbers, names and account numbers in 'plain text'. See Aditya Kalra, 'India Found Cybersecurity Lapses at National Payments Corp in 2019 - Government Document' (*Reuters*, 30 July 2020) <www.reuters.com/article/india-cybersecurity-payments/exclusive-india-found-cybersecurity-lapses-at-national-payments-corp-in-2019-government-document-idINKCN24V0HC?edition-redirect=in> accessed 4 February 2022.

[135] Srikanth Lakshmanan, 'FASTag: Will Datafication of India's Tolls Boost Highway Development?' (*The Wire*, 14 December 2019) <https://thewire.in/political-economy/fastag-will-datafication-of-indias-tolls-boost-highway-development> accessed 2 February 2022.

[136] RBI, 'Framework for authorisation of pan-India Umbrella Entity for Retail Payments' (18 August 2020) <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11954&-Mode=0> accessed 24 May 2022

[137] At the same time, the regulator also pointed to advantages of standardization, economies of scale, and consistency in oversight in such a structure. See Reserve Bank of India, 'Policy Paper on Authorisation of New Retail Payment Systems' (21 January 2019) <https://rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=918> accessed February 2 2022.

[138] Ashwin Manikandan, Sachin Dave and Saloni Shukla, 'Six consortiums apply to RBI for NUE licence for retail payments'(*The Economic Times*, 1 April 2021) <https://economictimes.indiatimes.com/tech/technology/six-consortiums-apply-to-rbi-for-nue-licence-for-retail-payments/articleshow/81791341.cms> accessed 24 May 2022.

role in NUEs posed for India's digital sovereignty, privacy and data safety. It was also claimed to be an unnecessary dilution of the NPCI's powers.[139] In response to such concerns, the RBI seems to have put the NUE process on hold.[140] While the RBI Governor recently noted that the applications were still under consideration,[141] it appears that NPCI's stronghold over the payments sector may keep competition at bay, at least for now.

The setting up of entities like the NPCI and the ONDC as industry-owned, private, not-for-profit entities reflects a deliberate design choice of keeping them out of the purview of slow and cumbersome government processes. But this also means that these entities are able to escape the requirements of accountability, transparency, and due process that would typically be attracted by a public body performing a similar infrastructural function. This situation is what allows the NPCI to set market caps on all UPI apps without any public consultation or impose discretionary user limits on a new player seeking permission to enter the market. While the NPCI is subject to the RBI's supervision, the only available checks for the other not-for-profit systems may be through general rules of corporate governance. Commenting on the not-for-profit character of iSPIRT, M.S. Sriram has noted that this leads to entities being accountable neither to the State nor to the markets (beyond their limited stakeholder community).[142] Similarly, in the case of the technical systems under discussion, their accountability will logically extend only to their members with a mechanism to hold them accountable to end consumers and to the public at large, who are supposed to be the ultimate beneficiaries of these systems.[143]

[139] Venkatesh Hariharan, 'Digital Payments: Do We Really Need New Umbrella Entities?' (*CXO Today*, 9 April2021) <www.cxotoday.com/digital-payments/digital-payments-do-we-really-need-new-umbrella-entities/> accessed 24 May 2022; UNI Global Union, JACAFRE, IT for Change, All India State Bank of India Staff Federation, and UNI Indian Liaison Council, 'Representation Before the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS) Requesting it to Disallow Amazon's Application for the New Umbrella Entity for Retail Payments' (*IT for Change*, 8 June 2021) <https://itforchange.net/sites/default/files/add/Representation-Against-Amazon-Application-NUE-License.pdf> accessed 2 February 2022.

[140] Gopika Gopakumar, 'RBI puts new payment network plan on hold' (*Live Mint*, 25 Aug 2021) <www.livemint.com/industry/banking/rbi-puts-new-payment-network-plan-on-hold-11629830389987.html> accessed 24 May 2022.

[141] Priyanka Iyer, 'New Umbrella Entity applications under evaluation, clarifies RBI Governor Shaktikanta Das' (*Money Control*, 10 April 2022) <www.moneycontrol.com/news/business/new-umbrella-entity-applications-under-evaluation-clarifies-rbi-governor-shaktikanta-das-8072391.html> accessed 24 May 2022.

[142] M.S. Sriram, 'Public Investments and Private Profit' in Reetika Khera (ed), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, 2019), 197.

[143] A 2019 decision by the Central Information Commission rejected a request to treat the NPCI as public authority under the Right to Information Act, 2005 thereby exempting it from the requirement of public scrutiny. See *Neeraj Sharma v. Bank Of Baroda*, Central

In sum, the UPI, the DEPA, and the ONDC are all examples of technical systems that are being rolled out through a coordinated strategy of public-private collaboration – the solutions are developed in the private sector and endorsed through state actions. The entity in question enjoys significant control over the entry of participants into the system and can shape and enforce technical standards and other rules of participation. This represents a new brand of power and control that is different from the kind of power that is enjoyed by big tech yet significant in terms of long-term consequences for competition, innovation, and accountability – all of which will have a bearing on public interest.

VI. Conclusion

This paper engaged with the meaning of big tech, in terms of its popular use as a set of large, predominantly American-owned, corporations and the logic behind clubbing those entities under this umbrella term. A review of the literature on this subject led to the identification of the following defining features of big tech – financial resources and market power, large user base, data intelligence, infrastructural capabilities, and societal impact. The dominating influence of big tech in all of these spheres has generated concerns that cut across issues of fair competition and innovation, digital sovereignty, human rights, and civic and political engagement.

Set against this background, the paper presented a non-exhaustive list of the different policy contexts in which the idea of regulating big tech has come up in the Indian policy space. It highlighted 4 broad motivations or types of regulatory interventions – addressing anti-competitive conduct, enhanced obligations for 'significant' players, data control, and ensuring general compliance with laws.

In all of these situations, the term 'big tech' is rarely, if ever, used in the policy documentation but the examples of its presumed constituents often come up, for instance, in areas such as intermediary liability, non-personal data governance, and e-commerce. This seems logical given the scale and power of these firms which makes them obvious targets of any actions aimed at controlling anti-competitive activities or regulating other economic and social risks in the digital sphere. At the same time, evidence from policy practice suggests that the responses to big tech are often subjective and

Information Commission order dated 10 December 2019 <https://indiankanoon.org/doc/40809441/> accessed 2 February 2022.

individualised, shaped not only by general notions of 'bigness' but also by a range of other political, strategic, and pragmatic considerations.

Alongside this assortment of policy responses, India is seeing a new trend of state-endorsed and industry-owned technical systems aimed at introducing open standards and interoperability in different spheres of the digital ecosystems. The paper discussed the NPCI's UPI system, the DEPA consent management architecture, and the latest ONDC initiative in the e-commerce sector as examples of such 'alt big tech' systems. Their characterisation as such is meant to capture both their positioning as an alternative to the present status quo of digital monopolisation by a handful of tech firms as well as their potential of becoming the new centres of power and control in the digital ecosystem. As elaborated in the paper, these new systems come with their own avenues for power play, the potential for infrastructural lock-in, and accountability concerns that can be detrimental to public interest and competition in the long run.

To summarise, the term big tech offers a helpful and now well-understood label for describing the world's most powerful technology companies. The challenges posed by the dominance and practices of these firms are well recognised, as is the need for imposing more effective checks on them. India is still in the early stages of formulating its governance strategy on big tech, reflected through competition enforcement, domain-specific regulatory actions and new technical systems that aim to alter the underlying dynamics of digital markets. While much has been said about the innovative and inclusive potential of these new systems, the paper highlighted that these developments are accompanied by certain competition and accountability concerns that are not being adequately addressed in the current model.

Future work on this subject could evolve in at least 2 directions. First, to supplement the present mapping exercise with an analysis of the adequacy of India's regulatory responses to big tech and whether a more comprehensive ex-ante regulatory approach may be in order. Second, to understand what sorts of design modifications and checks and balances are necessary to ensure that the claimed benefits of India's new technical systems are not overrun by the risks and challenges identified here.

The Oracle's Foretelling & the Case for Ambiguity: Exploring the Prophesies of Fintech & Financial Surveillance

Shohini Sengupta[*]

Abstract *This article explores the historical, social, and technical underpinnings of the global financial order predicated on massive data collection and surveillance. In particular, the article discusses the instruments of international financial regulation, and challenges the prescience of fintech, contrasting it with alternative narratives. The article does so by examining the history of financial surveillance mediated through biometric identification systems and socio-financial infrastructures, particularly in India and other post-colonial nations. The discourse is facilitated through the study of indigenous banking practices in colonial India, and the role of coloniality and slavery in shaping modern banking and surveillance practices both in India, and the United States. The article argues that understanding this history, both of India and other countries, is key to understanding modern-day biometric identification programmes and the ensuing financial surveillance; and may open pathways to present surveillance architectures that do not encompass sufficient human agency. Lastly, the article hopes to manoeuvre the vocabulary in fintech and financial regulation from prophesies of precision and specificity to one of deliberate ambiguity in the creation of mutable and humane identities.*

Keywords: *Financial surveillance, fintech, identity, identification programmes, biometrics, Aadhaar.*

[*] Associate Professor at the Jindal School of Banking & Finance, O.P. Jindal Global University.

This piece could not have been written without the incredible support of the IJLT editorial team, Uma Krutamana who provided critical support, the kind souls who read my draft paper, Aman, who kept me well-fed and rested, and Idli, who provided plenty of wags and licks. All mistakes are the author's alone.

I. Context and Beginnings

> “The happening of this happening
>
> The earth turns now. In half an hour
>
> I shall go down the shabby stair and meet,
>
> Coming up, those three. Worth
>
> Less than present, past - this future.
>
> Worthless such vision to eyes gone dull
>
> That once descried Troy’s towers fall,
>
> Saw evil break out of the north.”
>
> —Sylvia Plath, ‘On the decline of the oracles’

A. From Ambiguity to Specificity

Cleomenes of Sparta, one of the most important Greek kings once confidently proclaimed that the Oracle of Delphi had clearly prophesied his win over Argos. Of course, the only Argos Cleomenes knew of was the city ‘Argos’ that he wished to conquer until he heard of the hero of the same name.[1] Cleomenes misunderstood the prophecy and in the end went insane and died of suicide.[2]

[1] Julia Kindt, ‘Oracular Ambiguity As a Mediation and Triple’ (2008) 34 CLASSICVM 23, 27.

[2] ‘Cleomenes I’ Encyclopaedia Britannica (2011) <www.britannica.com/biography/Cleomenes-I> accessed 21 September 2022.

The Delphic Oracle is perhaps one of the most inscrutable dramatic personae in Greek mythology. They represented a crucial symbolism of the mortal condition- humans who needed to seek knowledge and insight by seeking the help of the divine, albeit through severely ambiguous prophecies.[3] This ambiguity played with the limits of description and perception and revealed the complexity and the variety of phenomena in the world.[4]

As a direct anti-thesis to the ambiguous prophetic world of Ancient Greece, in 2020, PwC published a report,[5] where it stated that big data analytics and other technologies that make up the Internet of Things will allow insurers to anticipate risks and customer demands with far greater precision than ever before. For rethinking fintech service architectures, they recommended building a system that incorporates a visualisation layer, an application layer, and an analytics layer that does the thinking, using advanced artificial intelligence ('AI') techniques to profile and predict behaviour, detect anomalies and discover hidden relationships. Further, they suggested the inclusion of data lakes that will acquire data from disparate sources and ingest it, so as to use it productively. For certain use cases like algorithmic trading, they propose a trend of AI trading systems that are moving from descriptive (historical data analysis) to predictive (focussed on predicting and understanding the future) to prescriptive analysis (using descriptive and predictive analysis to recommend actions). In fact, it is hoped that regulators will monitor the industry more effectively and predict potential problems instead of regulating after the incident.[6]

B. Identity, Biometrics and the Formation of the State-As-A-Platform

India of course, as an adopter of the largest biometric and digital identification programme in the world – 'Aadhaar', attempts to do all the above, that is, provide an efficient, precise mode of identification, addressing issues of security, transparency, and governance, but also linking it to citizen's socio-financial rights and welfare. In doing so, Aadhaar has enabled the Indian State to be recast in fundamental ways - of 'valorising' the population in a mercantilist sense, using the proverbial 'data is oil' metaphor

[3] Kindt (n 1) 26.

[4] ibid.

[5] 'Financial Services Technology 2020 and Beyond: Embracing Disruption' (PwC) <www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf> accessed 20 September 2022.

[6] ibid.

and forecasting economic growth, and more importantly, moving rapidly towards authorising widespread surveillance.[7]

This idea of Aadhaar has been contested by its architect, Mr Nandan Nilekani, who called it a 'simple' identity verification method,[8] deliberately depoliticising it, and diminishing its impact on society. However, the very act of counting people, governing populations, allocating resources, granting rights and encoding duties has always been deeply political, and identity systems like Aadhaar turn into an actual networked infrastructure, even as the sanctity of such data is fragile and routinely called into question.[9] It is, therefore, through this examination of a digitally moderated identity management system, that the Indian State has been reconfigured as

> a platform to coordinate citizens, market players and state agencies, guided by the logistics of Aadhaar as the waist that holds together an hour-glass: below it are multiple private services that facilitate the enrolment of people into the Aadhaar network and the management of the identity number; above are numerous private and public services that use the identity infrastructure to organise their own activities.[10]

The focus on legal identities is also dictated by the fact that almost all of the modern financial services are premised on it, through millions of data points accumulating to form an amorphous self-capable of telling banks and financial institutions specific, precise things, with clarity. For instance, the banks can receive information regarding the person applying for a loan including her true identity, her credit history, her spending habits, etc. These official identities, often static and immutable, commonly include personal details such as name, place and date of birth, sex, current address, nationality, familial relationships or other information needed to determine individuals' rights and responsibilities vis-à-vis financial institutions, regulators, and/or any other benefactor.[11] In India, this has resulted in a plethora of documents over the years - PAN card, passport, driver's license, election card/voter ID, ration card, and most importantly, Aadhaar.

[7] Nicolas Belorgey and Christophe Jaffrelot, 'Identifying 1.3 Billion Indians Biometrically: Corporate World, State and Civil Society' [2021] Heidelberg Papers in South Asian and Comparative Politics 1.

[8] 'Aadhaar just an ID, says Nandan Nilekani' The Economic Times (22 April 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-just-an-id-says-nandan-nilekani/articleshow/68992875.cms> accessed 21 September 2022.

[9] Ursula Rao, 'Biometric IDs and the Remaking of the Indian (Welfare) State' (2019) 21(1) Economic Sociology. Perspectives and Conversations_<https://econsoc.mpifg.de/38379/03_Rao_Econsoc-NL_21-1_Nov2019.pdf> accessed 20 September 2022.

[10] ibid 11.

[11] ibid.

The desire for specificity and precision then is central to understanding the intent of surveillance and the tools employed on its behalf. Noted scholars have looked at the surveillance assemblage in different forms. Orwell, for instance, associated surveillance with the means to maintain a form of hierarchical social control, whereas Foucault proposed that 'panoptic surveillance' was a form of population management strategy.[12] Karl Marx, on the other hand, viewed surveillance as a means of producing 'surplus value', which today would mean surplus information that can be commodified.[13] The most important aspect of modern surveillance assemblages, however, is their ability to transcend institutional boundaries so that systems intended to serve one purpose find other uses.[14] This is because surveillance is a key feature of modern capitalism that is premised on deriving monetary values from a range of transactions and interaction points by both firms and Governments. It is also a result of the increased commodification of the self, propelled by technologies that aid and expand people's abilities to do so.[15] This function and scope are explored later in this article in particular with reference to financial policies and Aadhaar in India.

In this regard, while identity and identity management are not synonymous with biometrics, biometrics does offer to strengthen core identity systems like civil registries and national ID cards, which legitimize and facilitate interactions between states and formerly '"invisible" citizens– those with physical or learning disabilities, the elderly, those with mental health issues, certain races, religions, genders, the homeless.[16] Apart from several legitimate reasons for exclusion from the system, these technologies have also been documented to cause discrimination. This is because they emerge from efficiency-orientated technology design, which presupposes certain generalisations about the population based on the imagination of a standardized normative body.[17]

The key research agenda of this paper will focus on these challenges, exclusions, and vulnerabilities, to understand the concerns arising from technology determinism and specificity that underlines India's modern biometric

[12] Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51 The British Journal of Sociology 605, 615.

[13] ibid.

[14] ibid 616.

[15] ibid 615-616.

[16] Hartej Singh Hundal and Bidisha Chaudhuri, 'Digital Identity and Exclusion in Welfare: Notes from the Public Distribution System in Andhra Pradesh and Karnataka' (International Conference on Information and Communication Technologies and Development, New York, June 2020) <https://dl.acm.org/doi/abs/10.1145/3392561.3397583> accessed 21 September 2022.

[17] ibid.

digital ID system and fintech. It uses the site of financial legal policies, both international and Indian, and relies on specific historical case studies and the political economy of financial laws to pose alternate questions about present digital identity management systems. To do so, it discusses the various modes of 'financial surveillance' in the use of technologies, and practices associated with monitoring the financial sphere for legal and/or regulatory purposes.[18] The paper also presupposes that 'identity' and 'identification' are subjective and highly context-specific, composed of various attributes, personal and psychological traits, preferences, physical as well as digital, self-made and imposed without consent. However, it chooses to focus specifically on legal or official identity and the supposed 'identity gap' that precludes development in countries like India.[19]

C. Chapterisation

To this effect, the paper discusses the issue in the following manner -

Part A has set out the context for surveillance generally, its specific infusions into the socio-financial infrastructure in India through biometric identification systems, and the expectations of what this piece sets out to do.

Part B expands on this foundation to discuss the history of the international financial order - the anti-money laundering and financing of terrorism outfits, global standards of disclosures, and the complex role of private actors, regulation, and the State in advancing financial surveillance.

Part C ties in the larger global discourse to India, exploring the anchoring of this particular public-private partnership through Aadhaar, which serves both as a basis for the digital identification program in India and has since rapidly been enmeshed in the larger digital-financial infrastructure.

Part D presents a historical view of the Indian financial order by discussing specific indigenous banking practices in colonial and pre-colonial India and traces the particular role of coloniality in establishing modern banking and financial practices rooted in identities and surveillance.

[18] James W Williams, 'Law, Surveillance, and Financial Markets' (2015) 13 Surveillance & Society <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law_finance/law> accessed 20 September 2022.

[19] Alan Gelb and Julia Clark, 'Identification for Development: The Biometrics Revolution' (2013) Center for Global Development Working Paper 315, 5 <www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315> accessed 20 September 2022.

Part E serves as the concluding piece, articulating what historical practices have taught us and where this leads us in the future, with the hope that the ideas of dismantling surveillance architectures divorced from human agency will begin with an understanding of what lay before us.

II. Tracing the Roots of the International Financial Surveillance Economy: 'Exceptionalism within the Governmentality of Everydayness'

> There is no whole self. He who defines personal identity as the private possession of some depository of memories is mistaken. Whoever affirms such a thing is abusing the symbol that solidifies memory in the form of an enduring and tangible granary or warehouse, when memory is no more than the noun by which we imply that among the innumerable possible states of consciousness, many occur again in an imprecise way
>
> —Jorge Luis Borges, 'The Nothingness of Personality'

The governance of the Internet is filled with surveillance technologies. Information intermediaries, critical Internet resources, surveillance, and security devices play crucial governance roles alongside political, national, and supra-national institutions and civil society organizations.[20] This is also true of the governance of finance, which is aided by digital surveillance technologies and infrastructures.[21] This section traces this history of financial policy in more detail.

A. Contribution to Economic Intelligence

Financial surveillance is conducted through a range of information-gathering methods and practices, including the freezing of assets, differential risk assessments and exclusion of illegitimate flows of money by banks.[22] These methods, certified and made ubiquitous with the help of instruments such as the Anti-Money Laundering/Countering Terrorist Financing ('AML/CTF') policies and the Financial Action Task Force ('FATF') create, an 'exceptionalism within the governmentality of everydayness'.[23] This creates a permanent state of exception, leading to an expansion of the rules of emergencies. For instance, in the wake of the 9/11 terrorist attacks in the US, the focus on the fight against terrorist financing led to a new impetus to blacklists.[24]

[20] Malcolm Campbell-Verduyn Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance (Routledge 2018) 136.

[21] Anthony Amicelle and Gilles Favarel-Garrigues, 'Financial Surveillance' (2012) 5 Journal of Cultural Economy 105, 105.

[22] ibid 106; Anthony and Favarel-Garrigues describe 'economic intelligence' as the technological instruments that process information that could be used against clients and used as a bargaining chip in the expanding interactions between the bank personnel in charge of the anti-money-laundering activity and the relevant police and intelligence services, 111.

[23] ibid.

[24] See RBI's FATF press releases from last year- 'Financial Action Task Force (FATF) High Risk and other Monitored Jurisdictions' (Reserve Bank of India, 28 June 2021) <www.

These attacks and the 2008 financial crisis deserve special mention for their contribution to the expansion of the AML-CTF regimes and for having an impact on the developing world as well. This expansion of the AML-CTF regime has been seen as a way to counter therise in global terrorist events. As a result, U.S. banks, for instance, have reduced lending and processing of payments to and from banks in small foreign economies.[25] This has had adverse effects on financial inclusion because of the increasing compliance requirements by the international financial order, particularly those set by the US.[26] This has led to, as per some studies, an increased money transfer operation ('MTO') account closures in countries like Australia as well, where stricter financial regulation has resulted in lower risk tolerance and higher compliance costs. It also posed a serious threat to financial inclusion in the Pacific Island Countries ('PIC'). This has happened due to the closure of MTOs, with people being forced to receive remittances through bank accounts which many people in the PICs do not have, or to rely on informal means that lack adequate consumer protection standards and defeat the purpose of AML-CTF regimes.[27]

To this effect, the Bank Secrecy Act, 1970 in the US which mandated that financial institutions maintain customer identity records and report illicit activity to government agencies, paved the way to an ever-expanding system of international surveillance that has arguably become a cornerstone of U.S. economic power.[28]

Financial surveillance tools, therefore, directed by a larger public security interest, now consist of routinized use of specialized data processing tools, with banks, in particular, having to develop tools for regulatory compliance. For instance, in India, the Reserve Bank of India's ('RBI') Department of Supervision has developed a 'Risk Based Approach' ('RBA') for 'Know Your Customer' ('KYC') and AML where as part of their internal governance structure, banks are required to institute risk management strategies. The regulator has the mandate of preparing models for the generation of risk scores and conducting specialised on-site assessments of select banks

rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=51803>; 'Investment in NBFCs from FATF Non-compliant Jurisdictions' (Reserve Bank of India, 12 February 2021) <www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12027&Mode=0> accessed 20 September 2022

[25] Michael J Casey, 'A Reckoning Looms for America's 50-Year Financial Surveillance System'" (2021) 41 Cato Journal 367.

[26] Rebecca L Stanley and Ross P Buckley, 'Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses' (2016) 17(1) Melb J Int'l L 83, 85.

[27] ibid 106.

[28] ibid.

based on their risk scores. Consequently, one of RBI's goals last year was to strengthen the process of collecting supervisory data relating to KYC/AML and streamline such data collection.[29] This was preceded in 2020 by the Master Direction on KYC that was updated regarding internal risk assessment by regulated entities ('Res') relating to money laundering and terrorist financing to further align RBI's instructions with the provisions of FATF.[30] This kind of routinized information processing and dissemination rather than simple information collection, explicitly constitutes 'economic intelligence' and demonstrates expanding interactions between bank personnel in charge of anti-money laundering activity and the relevant police and intelligence services.[31]

B. Screening and Profiling

These concerns are also supplemented by fears of data theft, security, and associated fraud, India being one of the top three countries that is most prone to breakdown or hacking of banking software systems.[32] Along with data security threats, another concern is also screening and profiling as part of bank regulation. In India, the roots of this can be traced back to 2008 when the RBI issued KYC/AML/CFT norms. An essential requirement of banks as part of the 'Customer Acceptance Policy' was to prepare 'profiles' for each new customer of a bank with information relating to a customer's identity, social/financial status, nature of business activity, information about their clients' business and location etc; with customers ultimately categorised as 'low-risk' and 'high-risk'.[33] Illustrations of low-risk customers were given as salaried employees whose salary structures were well defined, people belonging to lower economic strata of the society whose accounts showed small balances and low turnover, Government Departments and Government-owned companies, regulators and statutory bodies. On the other end, examples of high-risk customers included non-resident customers, high net worth individuals, trusts, charities, NGOs and organizations

[29] 'Annual Report' (Reserve Bank of India, 27 May 2021) <https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1319> accessed 20 September 2022.

[30] See 'Annual Report of the RBI' (Reserve Bank of India, 27 May 2020) <https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1326> accessed 20 September 2022.

[31] Stanley and Buckley (n 26) 111.

[32] CP Chandrasekhar and Jayati Ghosh, 'The Financialization of Finance? Demonetization and the Dubious Push to Cashlessness in India' (2017) 49 Development and Change 420.

[33] See 'Master Circulars-Know Your Customer Norms/Anti-Money Laundering Standards/Combating of Financing of Terrorism/Obligation of Banks under PMLA, 2002' (Reserve Bank of India, 2022) <https://m.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?Id=4354&Mode=0#cust> accessed 21 September 2022.>.

receiving donations, politically exposed persons (PEPs) of foreign origin, and non-face-to-face customers amongst others.

The reasons for these categorisations were unclear, and no evidence was adduced for these fictions of policy. The possibility of shifting identities between these categories was also left unimagined, for the idea of these categories seemed fixed and immutable. Even those identities described explicitly as 'financially or socially disadvantaged', for whom banks were instructed not to deny banking services, were not expounded upon.[34] Completely negating the experiences of socially disadvantaged groups - women, Dalits, transgenders, pensioners dependent on State welfare, amongst others. The possibility therefore of multiple, mutable identities, lying at the intersection of several disadvantages stacked on top of one another was completely missing.

C. Financial Stability and Security with a Side of Surveillance

Another challenge of financial surveillance based on vague risk categorisation is its intermingling with other goals of AML and macro stability. This can be witnessed for instance in the policies of the IMF[35]

The IMF even advanced the idea of 'financial abuse', to include not only illegal activities that may harm financial systems but also other activities that exploit the tax and regulatory frameworks with undesirable results. Financial abuse is therefore linked to financial integrity and stability, underscored also in the Basel 'Core Principles for Effective Supervision' and in the 'Code of Good Practices on Transparency in Monetary and Financial Policies'. It is ironic that the paper itself admits to a distinct lack of statistical data and appropriate methodology, and states that "an adequate measure of financial system abuse remains illusive."[36]

Subsequently in India, in 2002, a technical report made a detailed assessment of India's position with respect to G-7 principles on market integrity, anti-money laundering, and terrorist financing. The Report drew significant impetus from the Financial Stability Forum ('FSF'), promoted by members of G-7 in 1999, which was crucial in ideating the mandate of financial stability

[34] 'Know Your Customer Guidelines- Anti-Money Laundering Standards' (Reserve Bank of India, 23 August 2022) <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/65481.PDF> accessed 21 September 2022.

[35] 'Financial System Abuse, Financial Crime and Money Laundering—Background Paper' (International Monetary Fund, 2001) 13 <www.imf.org/en/Publications/Policy-Papers/Issues/2016/12/31/Financial-System-Abuse-Financial-Crime-and-Money-Laundering-Background-Paper-PP128> accessed 21 September 2022.

[36] ibid 40.

and reducing systemic risk through information exchange and international cooperation in the supervision and surveillance of financial markets.[37] It tends to combine various forms of bilateral and multilateral surveillance to solve multiple challenges in digital technology, climate change, inequality, demographics, and geopolitics.[38] These goals, now coupled with others demonstrated above like climate change, demographics and technology have laid ambivalent foundations for interventionist policies and led to the production of "complex new spaces of governing in which public and private authorities, knowledges and datasets cooperate closely, and sometimes become practically indistinguishable".[39] including money laundering and financing of terrorism.[40]

As such, suspicious activity reporting relies on the dynamic interplay of surveillance with the construction of risk and (ab)normality, where risk-scoring acts both as the frequency modulator of surveillance, and aids in the production of suspicion which determines normal and abnormal conduct.[41] It is interesting, that while the definitions of 'identity information', 'KYC identifier' and 'officially valid document' in the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 are all strictly defined, the language of 'suspicious activities' and 'suspicious transactions' incorporate a level of interpretive flexibility, making it impossible to mark out the exact contours of suspicion and the intrinsic value of the information supplied. As such, 'suspicion' becomes not a question of discovery but a question of interpretation, and an argumentative battle between State security-oriented institutions and their designated 'eyes and ears'.[42]

The second insight is that this vocabulary of surveillance, bank resilience, risk management and futurity, is predicated solely on data collection and analysis. A prominent example of this can be seen in a recent Bank for International Settlements (BIS) paper.[43] This then blurs the distinction between regulators and regulated actors in relation to risk-based regulation and creates new 'public– private' arrangements in the field of financial

[37] 'IMF Policy Advice' (International Monetary Fund, 2022) <www.imf.org/en/About/Factsheets/IMF-Surveillance> accessed 21 September 2022.

[38] Anthony Amicelle, 'Towards A "New" Political Anatomy of Financial Surveillance' (2011) 42 Security Dialogue 161, 162.

[39] 'Suspicious transactions' is defined in clause (h) of sub-rule (1) of Rule 2 of Prevention of Money-Laundering (Maintenance of Records) Rules 2005.

[40] 'STR (Suspicious Transaction Reports)' (Department of Revenue, 2022) <https://dor.gov.in/preventionofmoneylaundering/str-suspicious-transaction-reports> accessed 21 September 2022.

[41] ibid.

[42] Amicelle 'Towards A 'New' Political Anatomy of Financial Surveillance' (n 43) 165.

[43] Amicelle 'Towards A 'New' Political Anatomy of Financial Surveillance' (n 43) 167.

intelligence – that is, new forms of cooperation between professionals of security and professionals of finance to manage the 'risk' of terrorist financing, as discussed before.[44]

In India, these insights, prompted by the international financial order, are incorporated within the functioning of the Banking Regulation Act, 1949 (the 'BR Act'). For instance, the BR Act empowers the RBI to inspect and supervise commercial banks, both through on-site inspection and off-site surveillance.[45] Its primary objective is to monitor the financial health of domestic banks in between on-site inspections, essentially acting as an ex-ante trigger warning system for provoking remedial action.[46] Admittedly, this was done with a view to secure a macro analysis for evolving monetary and credit policy, to assess the quality of assets of the financial system and to improve co-ordination between banks and financial institutions (FIs).[47]

However, the fundamental role of digital identification and surveillance and the matter of public-private partnership in supporting and advancing this infrastructure in India is anchored most implicitly in Aadhaar, which is discussed in the next part of the article.

III. Aadhaar and the 'Deserving Poor'

"Definitions belong to the definers, not the defined."

—Toni Morrison, 'Beloved'

A. Categorisation and who deserves to be poor

The marriage of surveillance, bank regulation, and fintech in India is rooted in digital identity. Legal identity documents themselves are complex "creatures of the everyday sociality that marks the processes of claiming welfare governance in India" through which people from well-marked and not-so-properly marked territorial spaces become citizens.[48] identity to over a billion people. Over the years, it has come to be the fulcrum of several innovative

[44] ibid 167.

[45] 'Core Principles of Effective Banking Supervision' (Reserve Bank of India, 1999) <www.rbi.org.in/upload/publications/pdfs/10115.pdf> accessed 21 September 2022.

[46] ibid.

[47] ibid.

[48] 'Biometrics' has been defined in Rule 2(1)(b) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 as "the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', voice patterns', facial patterns', 'hand measurements' and 'DNA' for authentication purposes".

digital platforms built in and around this identity 'rail'. Built on top of each other, this created the now famous 'India Stack' applications architecture, including on top of the identity rail – the payment rail, and data sharing rail amongst others.[49] particularly noted for its ability to create a vast network that has changed the dynamic between regulators and innovators, and enabled collaborations between the public and private sectors.[50] These 'rails' are therefore often termed as 'public goods', allowing multiple and competing solutions to emerge for 'technological problems', all capable of scaling up, including new services, from lending to insurance and wealth management.[51] amongst scores of gender, caste and other socio-cultural and legal barriers that people regularly face.[52] The focus of Aadhaar and its analysis[53] Most criticisms cited through the years, have been reduced to a mere challenge of consent and poor data literacy, solved easily through provisions of additional cyber-security, and an omniscient and omnipotent data privacy legislation.[54] This is also expressed as an idea of 'coded citizenship', which transforms citizens into a set of data points.[55]

A corollary of the idea of 'deserving poor' can be found in the now infamous Moynihan Report of 1965 in the United States that argued that

'Biometric information' has been defined in section 2(g) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 as "photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations".

[49] Derryl D'Silva et al, 'The design of digital financial infrastructure: lessons from India' [2019] BIS Papers Series 106, 8.

[50] ibid 4.

[51] Ria Singh Sawhney, Raman Jit Singh Chima and Naman M Aggarwal, 'Busting the Dangerous Myths of Big Id Programs: Cautionary Lessons from India' (Access Now, October 2021) 29 <www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf> accessed 7 October 2022.

[52] Ashok Kotwal, and Bharat Ramaswami, 'Aadhaar that Doesn't Exclude' The Indian Express (2018). The issue of Aadhaar exclusion has also been noted by several academics and activists; see Amiya Bhatia & Jacqueline Bhabha, 'India's Aadhaar Scheme and the Promise of Inclusive Social Protection' (2017) Oxford Development Studies, 45:1, 64-79, Drèze, J., & Khera, R 'Recent Social Security Initiatives in India' (2017) World Development, 555–572, Muralidharan, K, Niehaus, P, & Sukhtankar, S 'Identity Verification Standards in Welfare Programs: Experimental Evidence from India' (2020) NBER Working Paper 26744, Grace Carswell & Geert De Neve, 'Transparency, Exclusion and Mediation: How Digital and Biometric Technologies are Transforming Social Protection in Tamil Nadu, India' (2022) India, Oxford Development Studies, 50:2, 126-141

[53] Shweta Banerjee 'Aadhaar: Digital Inclusion and Public Services in India'(World Bank, December 2015) <https://thedocs.worldbank.org/en/doc/655801461250682317-0050022016/original/WDR16BPAadhaarPaperBanerjee.pdf> accessed 6 October 2022.

[54] Usha Ramanathan, 'Biometrics use for Social Protection Programmes in India Risk Violating Human Rights of the Poor' (UNRISD, 2004) <https://www.unrisd.org/en/library/blog-posts/biometrics-use-for-social-protection-programmes-in-india-risk-violating-human-rights-of-the-poor> accessed 7 October 2022.

[55] ibid 84.

because many black families deviated from the cultural norm of the male head-of-household or breadwinner, these families were destined to be long-term dependents on state assistance program. Therefore, it constructed the myth of 'welfare queens' - single, black women, producing multiple children and dependent on financial support from the State.[56] privacy, work, and reproductive freedom.[57] Aadhaar creates a compelling incentive for the State to focus on the empowerment of only the deserving poor, leaving aside those considered not worthy of the benevolence.

B. Aadhaar and its Expanding Universe

A key challenge of Aadhaar, therefore, is the exclusion of people, whether for various socio-political or technical reasons. This has grave consequences for the excluded, because of the wealth of services and entitlements that Aadhaar connects to in India. This is despite the fact that, when it started, the UIDAI claimed that it would only guarantee identity and not rights, benefits, or entitlements.[58] takes one far away from the early assurances, and puts the idea of the deserving poor in even sharper focus.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 illustrates this point through several provisions. Section 6 of the Act requires Aadhaar number holders to update their demographic information and biometric information from time to time to ensure the continued accuracy of their information in the Central Identities Data Repository. An example of this continuous burden of proof is the 'Jeevan Pramaan' or digital (biometrical enabled) life certificate /DLC for pensioners of the Central Government, State government or any other Government organization. To generate the certificate, pensioners must provide their Aadhaar number, name, mobile number, and self-declared pension-related information - PPO Number, Pension Account number, Bank details, Name of Pension Sanctioning Authority, Pension Disbursing Authority, etc. Pensioners also have to provide their biometrics - either iris or fingerprint. A special note declares that "incorrect information may lead to rejection of the DLC by the authorities." To even download the Jeevan Pramaan mobile app from the Google Play Store, an 'Aadhaar Face RD' service is required.[59]

[56] ibid 278.

[57] Rao (n 9) 15.

[58] K.S. Puttaswamy v Union of India (2018) 1 SCC 809.

[59] 'Submission of Life Certificate/Non-Remarriage Certificate by Pensioners under EPS, 1995 – Regarding' (Employees' Provident Fund Organisation, 9 April 2018) <www.epfindia.gov.in/site_docs/PDFs/Circulars/Y2018-2019/Pension_JeevanPramaan_913.pdf> accessed 5 October 2022

Further, the Aadhaar legislative ecosystem itself is expanding, given its wide and open-ended definition in section 2 (aa) as per the Aadhaar and Other Laws (Amendment) Act, 2019, and the amended section 4, which allows the 'voluntary' use of Aadhaar, subject to a number of specifications provided in regulations in addition to changes made to section 4 of the Telegraph Act, 1885 and insertion of section 11A to the Prevention of Money-laundering Act, 2002. This also contributes to a growing chain of exclusion, and even though the Act provides civil penalties for infractions, no data on actual offenders and penalties is available on the UIDAI's website.

When we look at recent endeavours of the Government in India, we find this digitally mediated service provision even further entrenched. A good example from the past year is a "digital payment solution" called 'e-RUPI',[60] E-RUPI, is basically a pre-paid redeemable voucher issuable only by RBI banks (participating as 'Payment Service Providers' or PSPs), that provides certain benefits to consumers that are not available with other payment options including UPI. For example, redemption is an easy 2-step process under e-RUPI, and beneficiaries do not need to share personal details during redemption.[61] The scheme has been widely popularised, with the RUPI, is NPCI website mentioning 16 "live banks"[62] To ensure that e-RUPI is used to affect DBTs and technology-enabled digital governance in the country, it is linked to Aadhaar, enmeshing it in this vast, ever-expanding universe. Since receiving any benefits from the Government relies on the framework of the Aadhaar-bank account-phone number or the Jan Dhan - Aadhaar - Mobile (JAM) trinity, it implicitly implies that even though at the point of redemption there is no transfer of personal details from the beneficiary to the merchant, the aforementioned scheme of e-RUPI ties in to the existing biometric Aadhaar assemblage, including with it, the privacy and financial surveillance concerns as pointed out by experts.[63] through KYC registrations linked to Aadhaar, or direct Aadhaar linkage. As such, e-RUPI, the latest venture in

[60] ibid.

[61] ibid.

[62] 'PPV Hospital' (National Payment Corporation of India, 2021) <www.npci.org.in/PDF/npci/e-rupi/PPV-Hospital-02nd-September2021.pdf> accessed 7 October 2022.

[63] This includes, but is not limited to the Retail Direct Scheme, Payments Infrastructure Development Fund integrated into the PM SEVA Nidhi Scheme beneficiaries, Sovereign Gold Bond Scheme 2021-22, Interest Subvention Scheme for MSMEs – Co-operative Banks, Banking Facility for Senior Citizens and Differently abled Persons, Deendayal Antyodaya Yojana – National Rural Livelihoods Mission (DAY-NRLM), Interest Subvention Scheme (ISS) and Prompt Repayment Incentive (PRI), Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems, Deendayal Antyodaya Yojana – National Rural Livelihoods Mission (DAY-NRLM), Direct Benefit Transfer (DBT) Scheme – Implementation and Deendayal Antyodaya Yojana – National Urban Livelihoods Mission (DAY-NULM).

a line of increasing socio-financial programs and fintech endeavours by the Government, links back to Aadhaar, as a central focus of identification of people, connected to a host of privileges and services (including cash and credit).

It is important to highlight that even though all DBTs in India are linked to Aadhaar, the banking ecosystem was specifically included within its net with the launch of the Pradhan Mantri Jan Dhan Yojana (PMJDY) in 2014, when the Government's goal was to provide access to banking services to all unbanked households in India together with access to a savings account through debit card and mobile banking, yielding almost 42.55 crore beneficiaries.[64] Before the judgement in K.S. Puttaswamy v Union of India[65] This creates a financial information system that consists of heterogenous classes of data that areshared between regulators, fintech providers and other third parties. The honeypot of heterogenous yet connected data also creates a critical public infrastructure that when breached, may be a cybersecurity concern and, as has been witnessed in India, a contested legal subject.

C. Myth-making and Aadhaar

Financial information systems predicated on a fixed digital legal identity, are replicated in financial inclusion efforts across the globe. For instance, UNESCO's Sustainable Development Goal, 16.9 articulates the goal of providing legal identity for all, including birth registration, by the year 2030.[66] This is drawn from a colonial idea of subjugating populations to explicit state aims of legibility, of monitoring 'criminal' populations, refugee infusion, state-imposed emergency, fingerprints and other biometrics, as well as documents, such as birth certificates, passports, ration cards, and national ID cards.[67] The British government frequently used technologies developed in colonial India and South Africa, such as indexable codes and fingerprinting, allowing for a vast, searchable biometric database that could

[64] 'Scheme Details' (Pradhan Mantri Jan-Dhan Yojana) <https://pmjdy.gov.in/scheme> accessed 5 October 2022.

[65] Kathryn Henne, 'Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India' in Blayne Haggart, Kathryn Henne and Natasha Tusikov (eds) Information, Technology and Control in a Changing World (Palgrave Macmillan 2019) 225.

[66] Janaki Srinivasan and Elisa Oreglia, 'The Myths and Moral Economies of Digital ID and Mobile Money in India and Myanmar', (2020) 6 Engaging Science, Technology, and Society 215, 217.

[67] Keren Weitzberg, 'Biometrics, Race Making, and White Exceptionalism: The Controversy over Universal Fingerprinting in Kenya'" (2020) 61(1) The Journal of African History 23, 24.

be cross-referenced against criminal records.[68] This is especially true of the Global South where digital biometric technologies although no longer as explicitly racialized, are far more ubiquitous in postcolonial countries, where they are governed by significantly less scrutiny, transparency, and consent than is the norm in the Global North.[69] The Court found, in spite of the Inter-American Development Bank sanctioning $68 million to the Jamaican Government, similarities with the Aadhaar Act in India, and particularly found Justice DY Chandrachud's dissenting opinion in the Indian Supreme Court's judgment in Puttaswamy persuasive.[70] This has resulted in massive exclusions, exploitation of individuals' data and identity, and the seeding of a surveillance state[71]

Biometric governance in particular, contrary to claims of precision, extends these illusions of transparency, incorruptibility and social inclusion.[72] Finally, the myth of financial inclusion through 'financial data collection' (exhibited most recently in RBI's national strategy for financial inclusion 2019-2024), specifically in the context of forced financial inclusion, has not been necessarily shown to result in greater welfare of unbanked populations[73]

Since the vast production of financial knowledge comes to us from the Global North, and more particularly from the erstwhile colonial powers of the world - the British, Portuguese, Dutch, and the French, it is indubitably the case that current techno-financial infrastructures are marked by the methods and practices of these colonial states, and the other institutions born out of their patronage - the colonial brokerage firms, banking companies, trading houses, currency exchanges and the like.

In fact, the banking, financial and generally commercial environment in India, in general, underwent massive changes directly as a result of the British colonial rule. This is true as much of India, as of Jamaica, the US, and many other post-colonial states across the world. This part of the article argues

[68] Supra 97 pg. 220.

[69] Tony Bitzionis, 'Jamaican Government Aims to Fast-Track National Identification System to Help with COVID-19 Aid', (Find Biometrics, 31 March 2020) <https://findbiometrics.com/jamaican-government-aims-fast-track-national-identification-system-help-covid-19-aid-033103/> accessed 5 October 2022.

[70] Sawhney, Chima and Aggarwal (n 69) 9.

[71] Supra 97 p 231.

[72] Shrimoyee Nandini Ghosh, 'Documented Lives: Aadhar and the Identity Effect in Kashmir' (Kafila, 23 January 2014) <https://kafila.online/2014/01/23/documented-lives-aadhar-and-the-identity-effect-in-kashmir-shrimoyee-nandini-ghosh/> accessed 7 October 2022.

[73] Amitav Ghosh, The Nutmeg's Curse: Parables for a Planet in Crisis (University of Chicago Press 2021) 152.

that understanding of this history, both of India and other countries is key to understanding modern-day obsession with identification programmes and the ensuing financial surveillance; and may open the passages to dismantling these structures in the future.

i. Legal Stereotypes and Historical Myopia[74]

The Nakarattars were unique because they relied on familial and caste connections to succeed rather than the capitalist system which was denied to them because of colonialism and the caste system.[75] Even with respect to deposits, the Nakarattars dealt with different kinds of deposits with different terms to maturity based on a variety of caste-based principles for social cooperation. Therefore, their understanding of 'risk' corresponded closely with 'trust'.[76] This also led to the creation of a standard legal practice and commercial vocabulary, outlawing of indigenous banking and financial practices (such as the legal challenges to financial instruments like the 'Hundi'[77] This assimilation and slow decimation of the indigenous and often termed 'informal' economy is symptomatic of modern rule-based standardised processes of financial information collection, risk identification, and establishing identities for the goals of financial regulation.

ii. Etymology of Data Practices

Along with the subversion of indigenous banking practices and forced legal standardisation attempts in India, the expansion of the banking, insurance and financial services industry in Britain continued on the back of an expansive slave-based economy.[78] and had links to slave plantations (particularly Rose Hall Estate) in Jamaica.[79] Along with this, there is empirical support for the claim that the slave economy played an active role in the development of almost all financial markets in Britain.[80]

[74] ibid.

[75] Supra 114 p 232

[76] Vere A. da Silva, 'Commercial Law in India' (1964) 8 International and Comparative Law Quarterly Supplementary Publication 51, 55.

[77] Rajat Kanta Ray, 'The Bazaar: Changing Structural Characteristics of the Indigenous Section of the Indian Economy Before and after the Great Depression' (1988) 25(3) The Indian Economic & Social History Review 263, 268, 317.

[78] 'Robert Cooper Lee' (Centre for the Study of the Legacies of British Slavery) <www.ucl.ac.uk/lbs/person/view/2146645287> accessed 5 October 2022.

[79] Sissoko and Ishizu (n 122) 3.

[80] 'Statement in Relation to the Bank's Historical Links to the Slave Trade', (Bank of England, 19 June 2020) <www.bankofengland.co.uk/news/2020/june/statement-in-relation-to-the-banks-historical-links-to-the-slave-trade> accessed 5 October 2022.

Similarly, in the United States, there is emerging evidence demonstrating that commercial banks, particularly in the South were both willing to accept slaves as collateral for loans and as a part of loans assigned to them from a third party.[81]

This history is supplemented by growing evidence of modern banking, financial surveillance and accounting practices deriving much of their roots from the American plantations in the 1800s. Caitlin Rosenthal documents that the planters or slave owners in the American South paid close attention to data management practices by measuring how efficiently enslaved people worked, frequently experimenting with new methods for maximizing output. Thus, these plantations were distinguished not by their sheer size, but by their 'data practices' (including collection and recording of data, and analysing of data year after year).[82]

As Rosenthal states, 'control', which is at the heart of modern accounting practices, has its etymological roots in "verification", and later by the 16th century, the direction, management, and surveillance that verification required.[83]

IV. Conclusion

This article started with oracular ambiguity and why it became so important in the Greek mythological narrative. Much like the essence of this piece, it denotes that prophecies of precision and specificity, in something as mutable and dynamic as human identity, especially in countries like India, which links it to basic public goods of finance, food, nutrition, social security and health is a deeply limiting and dehumanising concept.

Oracular prophesies were never meant to be precise, and simply allowed a reflective discourse on the world and the human place within it.[84] In this backdrop of Ancient Greece and the testimony of oracular ambiguity, this article lists the many ways in which the codification of identities in numbers, much like their accounting counterparts in the colonies, and standardisation of the vocabulary of financial regulation predicated on fixed identities and surveillance; is rooted in rhetoric and a myth of infallible technologies. More concerning is the historical myopia of the oppressive pasts from which modern data and financial practices emerge. Ultimately, the perception rests

[81] ibid 27.
[82] ibid 41.
[83] ibid 120.
[84] ibid.

either on the fallacy that as one scales up, one must trade identity for inclusion, or on the idea of neatly categorising certain bodies and citizens worthy of the benevolence of the State, excluding the very subjects that these programs were intended to include, rendering these 'exclusion errors' as unreadable bodies.[85] The article, by presenting a connected history of international financial policies, and the impact of coloniality in India, has sought to provoke current examination and development of alternative methodologies and systems that may help achieve the same goals of financial regulation and inclusion. As has been demonstrated in this paper, history is rife with stories of indigenous banking and financial systems that were erased to accommodate colonial agendas. Therefore, the myths of modern surveillance technologies, particularly in furtherance of the myths of specificity and efficiency, in the face of evidence suggesting otherwise is both untrue and dangerous. To this extent, even though we may not have the Delphic Oracles to guide us today, understanding the histories and fallacies of infallible technologies that claim to make predictions of an ambiguous future, will hopefully lead us to question ideas of identities and how we must manage them through more humane and inclusive systems.

[85] Weitzberg (n 101) 43.

Guidelines to Build Robust Security Standards for the Financial Technology Sector in India

Vipul Kharbanda and Cheshta Arora[*]

Abstract *Given the rapid growth of the fintech sector in India and the lack of any national data protection framework, there is an urgent need to arrive at stop-gap measures to ensure robust information security standards for the sector. Owing to threats such as financial data leakages, malware attacks etc., information security standards are central to ensuring business and operational sanctity. We present a set of minimum guidelines, which privilege a co-regulatory framework for the fintech sector, that should be considered when building a regulatory framework for the fintech entities to ensure adequate data protection as well as the growth of the industry.*

Introduction

Standards provide a mechanism for institutional coordination to ensure that products and services are safe, sustainable and conform to a basic minimum. While standards are crucial for governance, they may not necessarily

[*] Vipul is a non-resident fellow and Cheshta is a Researcher at the Centre for Internet and Society. Parts of this essay are adapted from the Information Technology (Fintech Security Standards) Rules ("Fintech Rules"), 2019 previously published by the Centre for Internet and Society and authored by Vipul Kharbanda and Prem Sylvester.

be legislated top-down by state actors but be negotiated through a diffused system of industry actors, governments, and civil society, for example, the ISO/IEC standards.[1] Although standards can be classified in varied ways, in the context of this paper, it is important to distinguish between network/technical standards and enforceable standards.[2]

The former refer to those standards that incentivize coordination among actors and their enforcement is generally self-incentivized as the actors using the standards benefit from participation in a certain network. The latter i.e., 'Enforced standards',[3] which are perhaps more relevant for our discussion, refers to standards which are used by parties, not due to their self-interest but rather owing to incentives or demands placed on them via a legal requirement or external pressure.

Regulatory policies often cite multiple information security standards as a baseline that is to be complied with in order to ensure the adequate protection of information systems as well as associated architecture.[4] In the context of the financial industry, information security standards provide consideration to the specific risks and threats that financial institutions may face either owing to their inherent data integrity risks, data leakages or malware attacks or due to collaborations between traditional financial actors and new fintech firms,[5] making information security standards an integral part of the process of ensuring business and operational sanctity.

This interest is amplified considerably due to the policy push towards a 'cashless society'.[6] This recent policy push has in part led to the ubiquitous adoption of technology-centric financial services such as *PayTM, PhonePe, Mobikwik* and others. Thus, there is also an urgent economic interest in ensuring robust security of the financial technology sector within the

[1] Wang Ping, 'A Brief History of Standards and Standardization Organizations: A Chinese Perspective' [2011] East-West Center Working Papers <https://www.files.ethz.ch/isn/134857/econwp117.pdf> accessed 7 October 2022.

[2] Peter Cihon, 'Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development' (University of Oxford 2019) <https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf> accessed 18 October 2022.

[3] ibid.

[4] Karin Höne and JHP Eloff, 'Information Security Policy — What Do International Information Security Standards Say?' (2002) 21 Computers & Security 402 <https://linkinghub.elsevier.com/retrieve/pii/S0167404802005047> accessed 7 October 2022

[5] Khakan Najaf, Md Imtiaz Mostafiz and Rabia Najaf, 'Fintech Firms and Banks Sustainability: Why Cybersecurity Risk Matters?' (2021) 08 International Journal of Financial Engineering 2150019 <https://www.worldscientific.com/doi/abs/10.1142/S2424786321500195> accessed 7 October 2022.

[6] RBI, 'Payments Vision 2025' <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53886> accessed 7 October 2022.

country.[7] In the following essay, we present the guidelines and principles upon which rules pertaining to information security standards for the fintech entities could be based. In the first section, we present an overview of the current information security standards in India and their inadequacy at addressing the needs of different fintech entities constituting the present fintech ecosystem. In the second section, we present a minimum guidelines framework,privileging a co-regulatory approach, upon which such rules pertaining to information security standards could be based.

I. Information Security Standards in India: An Overview

The current landscape with respect to security standards for financial institutions in India is multi-pronged with multiple standards in place for companies to implement depending upon the sector in which they operate.[8] There may be an assumption amongst some that all fintech entities are governed by the Reserve Bank of India which has a number of detailed guidelines regarding security standards.[9] However, not all fintech entities come under the jurisdiction of the Reserve Bank of India, which can exercise supervisory jurisdiction only as delineated under various legislations, such as the Reserve Bank of India Act, 1934, Banking Regulation Act, 1949, Payment and Settlement Systems Act, 2007, etc. Similarly, the Securities and Exchange Board of India and the Insurance and Regulatory Development Authority only have powers to regulate entities specific to their sectors as specified by various statutory provisions.

The burden of regulating the security standards of fintech entities which do not fall under the regulations issued by the abovementioned authorities falls on the Information Technology Act, 2000, ("IT Act") and more specifically on the rules issued pursuant to section 43-A of the IT Act, *viz.* the

[7] 'At $29 Bn, Indian Fintech Sector now has 14% Global Funding Share: Report' *The Economic Times* (22 August 2022) <https://economictimes.indiatimes.com/industry/banking/finance/at-29-bn-indian-fintech-sector-now-has-14-global-funding-share-report/articleshow/93715347.cms?from=mdr> accessed 7 October 2022; Ashish Rathi, 'Why Cybersecurity is a Priority for Fintech Firms Today - ETCIO' (*ETCIO.com*, 2022) <https://cio.economictimes.indiatimes.com/news/corporate-news/why-apis-are-so-important-for-fintechs/88747660> accessed 7 October 2022.

[8] Aadya Misra and Mathew Chacko, 'Square Pegs, Round Holes, and Indian Cybersecurity Laws' (2021) 2 International Cybersecurity Law Review 57 <https://doi.org/10.1365/s43439-021-00026-7> accessed 18 October 2022.

[9] Cyber Security Framework in Banks, dated June 2, 2016; Reserve Bank of India (Digital Payment Security Controls) Directions, 2021; Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach, dated December 31, 2019, etc.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ("SPDI Rules"). Section 43-A of the IT Act requires body corporates to comply with 'reasonable security practices and procedures' in order to avoid liability for negligence in dealing with data causing wrongful loss or gain.[10] *The explanation to section 43-A states that in the absence of a contract specifying the security practices adopted by the body corporate, reasonable security practices and procedures will be those as specified in the SPDI Rules. Unfortunately, even the SPDI Rules do not lay down any specific security standards or protocols but say that entities would be assumed to have implemented reasonable security practices and procedures if they have undertaken measures that are commensurate with the information assets being protected with the nature of business.*[11]

The only specific standards that the SPDI Rules prescribe or refer to are the ISO27001 (or any other standards developed by an industry body which have been duly notified by the Central government).[12] This means that if a body corporate has implemented the ISO27001 standard it shall be deemed to have complied with reasonable security practices and procedures as long as such standards have been certified or audited on a regular basis.

Need to develop specific information security standards for the fintech sector

The financial sector in India has to date not developed any sectoral security standards that have been approved by the Central government (as required by the SPDI Rules). Meanwhile, the experience of the industry and more

[10] S 43-A provides as under:

"43-A. *Compensation for failure to protect data.*— Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation ....

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

......"

[11] R 8(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[12] R 8(2) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

specifically fund strapped fintech start-ups, has been that ISO 27001 is an expensive standard for small businesses to implement.[13] Therefore, there appears to be a need for a set of security standards or guidelines that fintech entities can look to implement which are specific and detailed enough to perhaps form a checklist but easier and more economical to implement than the ISO27001 standard.

The crucial need to have information security standards specified primarily for the fintech industry and not for other entities which deal with sensitive and personal data or information is rooted in the structure of section 43A of the IT Act, which provides for monetary damages due to negligence in dealing with sensitive and personal data.[14] It is assumed that losses due to negligence in dealing with financial data would be easier to quantify in monetary terms, and perhaps would affect users in a more direct manner than other forms of data.[15]

Thus, there is a need to create regulations that can specify a set of security standards for the fintech industry. This will guarantee that user data is handled securely and safely, and that smaller companies in the fintech sector have a specific standard to consider in order to minimize their exposure to any potential breaches. Such regulations could be introduced in the form of delegated legislation under the IT Act similar to how the SPDI Rules were implemented. This approach can help bypass the cumbersome and sluggish process of parliamentary legislation. It is crucial that we introduce regulations specifying the security standards as soon as possible, even if just as a stop-gap measure until the goal of a more comprehensive data protection legislation is finally realized – which could take significant time as the new Digital Personal Data Protection Bill, 2022 issued for public consultation is being perceived in certain sections as being too weak.[16] Concerns have been raised over a number of issues such as increased grounds for collection and processing of data under the concept of deemed consent,[17] non-application

[13] Yazan Alshboul and Kevin Streff, 'Analyzing Information Security Model for Small-Medium Sized Businesses' [2015] AMCIS 2015 Proceedings <https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/26>.

[14] (n 11).

[15] Elisabeth Rhyne, 'Consumer Harm from Data Breaches is a Black Box' (Centre for Financial Inclusion, 18 January 2019) <https://www.centerforfinancialinclusion.org/consumer-harm-from-data-breaches-is-a-black-box> accessed 19 October 2022.

[16] Internet Freedom Foundation, 'IFF's First Read of the Draft Digital Personal Data Protection Bill, 2022' (Internet Freedom Foundation, 18 November 2022) <https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2022/> accessed 21 November 2022.

[17] S 8, Digital Personal Data Protection Bill 2022.

to offline data,[18] as well as non-automated processing,[19] absence of the principles of purpose limitation and data minimisation,[20] increased powers to exempt State agencies,[21] etc.

This would suggest that there is a possibility of a long-drawn-out process before a more widely acceptable draft of the Bill is agreed upon and before it passes through the various Committees and debates in Parliament, a process which was fatal for its predecessor, the Personal Data Protection Bill, 2019.[22]

Defining fintech entities

One of the major stumbling blocks when dealing with the fintech sector is the lack of a universally accepted definition of the term. Fintech is generally understood as an amalgamation of "finance" and "technology," but there is divergence on whether the centre of gravity is the former or the latter.

Those that focus on the financial services offered by fintech entities describe technology as an enabler,[23] with the goal to develop "novel, technology-enabled financial services" with the aim to "transform current financial practices".[24] Others describe fintech in terms of the technological innovations that interact with financial services in a variety of ways — specifically, digital innovations and technology-enabled business model innovations[25] and novel technologies adopted by financial institutions to provide more effective financial products and services that bring the sector into the digital age[26] or to enhance the efficiency of the financial system".[27] Fintech, therefore, has

[18] S 3(b), Digital Personal Data Protection Bill 2022.

[19] S 3(a), Digital Personal Data Protection Bill 2022.

[20] Gautam Bhatia, 'Why the New Draft Bill must be Reconsidered', (*Hindustan Times*, 29 November 2022) <https://www.hindustantimes.com/opinion/why-the-new-draft-data-bill-must-be-reconsidered-101669731526700.html> accessed 5 January, 2023.

[21] S 18(2), Digital Personal Data Protection Bill 2022.

[22] 'Govt Withdraws Personal Data Protection Bill 2019, to Present New Bill' (Money control) <https://www.moneycontrol.com/news/india/govt-to-withdraw-personal-data-protection-bill-2021-8946661.html> accessed January 5, 2023.

[23] Douglas W Arner, Janos Nathan Barberis and Ross P Buckley, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' [2015] SSRN Electronic Journal <http://www.ssrn.com/abstract=2676553> accessed 20 October 2022.

[24] Dávid Varga, 'Fintech, the New Era of Financial Services' (2017) 48 Budapest Management Review 22 <http://unipub.lib.uni-corvinus.hu/3170/> accessed 20 October 2022.

[25] Thomas Philippon, 'The FinTech Opportunity' (National Bureau of Economic Research 2016) <http://www.nber.org/papers/w22476.pdf> accessed 20 October 2022.

[26] Benedict J Drasch, André Schweizer and Nils Urbach, 'Integrating the "Troublemakers": A Taxonomy for Cooperation between Banks and Fintechs' (2018) 100 Journal of Economics and Business 26 <https://linkinghub.elsevier.com/retrieve/pii/S0148619517301431> accessed 20 October 2022.

[27] Daniel McAuley, 'What is FinTech?' (Wharton FinTech, 2 November 2015) <https://medium.com/wharton-fintech/what-is-fintech-77d3d5a3e677> accessed 20 October 2022.

three dimensions: an input (namely the combination of technology, organization and money flow), mechanisms (create or improve or change, disrupt, apply technology to finance, create competition on the market) and an output (creation of new services or products or processes or business models).[28]

While the breadth of approaches in the literature to define fintech offer us a broad range of factors to consider, it also makes it difficult to arrive at a comprehensive definition of the same. We agree with Dorfleitner et al. who note that it is not possible to construct a restrictive definition of "fintech" that applies to all of the entities traditionally associated with the term.[29]

However, for the purpose of laying a foundation for understanding its functions and regulatory responses, we define fintech as a broad range of individuals or entities that develop technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks & non-banking financial companies).

We do not incorporate in this definition the form such enhancements may take or the motivations for such enhancements as our objective is to present a minimum set of guidelines that all fintech entities would be required to follow. In the case of fintech entities which have an extremely large number of users, or large turnover, or are extremely data reliant, etc., for whom the generic standards may be considered insufficient, a classification may be made, and larger entities could be mandated to comply with stricter prescribed standards or could be required to comply with ISO27001 or other similar standards.

II. Minimum guidelines framework: Towards a Co-regulatory approach

Legislative mandates may not always be necessary to regulate certain industries or sectors and in some cases, the goals of the legal mandate may be better achieved through self-regulation rather than state regulation, as has been the case for the countries in the Global North.[30] Self-regulation can take many different forms, but at its most fundamental level, it entails a private organization taking responsibility for its own rules and procedures

[28] Liudmila Zavolokina Mateusz and Gerhard Schwabe, 'FinTech – What's in a Name?' (2016).

[29] Gregor Dorfleitner and others, 'Definition of FinTech and Description of the FinTech Industry' in Gregor Dorfleitner and others, *FinTech in Germany* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-54666-7_2> accessed 20 October 2022.

[30] Ping (n 1).

and overseeing their implementation as opposed to a government regulator doing the same under the law. This can be accomplished by each organization tailoring its own code of conduct or by any industry body (such as a trade association) developing a common code or set of principles, and by each individual firm modelling its policies for adopting such a code. Such a model of governance, however, has been criticized due to an overall lack of accountability and transparency, the incomplete realization of the principles promulgated in common codes, and weak oversight and enforcement.[31] Nonetheless, reverting back to a command-and-control regulatory model may not be the most efficient approach for many fledgling industries operating with new technologies as 1) the law would not be able to keep up with the latest developments and 2) excessive regulation could stifle the growth of such industries.

A co-regulatory framework, which involves the government and the industry working together to share the responsibility of drafting and enforcing regulatory standards can offer a middle path between self-regulation and government regulation.[32] This allows the government and the industry body to negotiate proper regulatory goals, collaborate on the drafting of standards, and work in a cooperative manner to enforce the standards against firms which violate them. Furthermore, this approach may be better than the traditional regulatory regimes as it tends to 1) draw on industry knowledge and expertise; 2) yield rules that are more cost-effective, workable, and innovative; 3) create a stronger sense of industry's ownership over rules which can lead to better compliance; 4) lead to rules that are politically viable and efficient.[33] Although the SPDI Rules also provide for a co-regulatory mechanism, there are as yet no standards developed by any industry body which have been notified under the Rules.

A co-regulatory model for information security standards may not depend on a licensing requirement, i.e., fintech entities should not have to comply with the rules as a pre-condition to starting operations. In this regard, they could be like the SPDI Rules, i.e., as a measure to be implemented for fintech entities to absolve themselves of any liability against claims of negligence. This means that there could be no legal obligation on fintech entities

[31] Dennis Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439 <https://digitalcommons.law.seattleu.edu/sulr/vol34/iss2/3>.

[32] Hans-Bredaw-Institut, 'Final Report Study on Co-Regulation Measures in the Media Sector' (University of Hamburg 2006) <https://hans-bredow-institut.de/uploads/media/default/cms/media/cd368d1fee0e0cee4d50061f335e562918461245.pdf> accessed 19 October 2022.

[33] Hirsch (n 31).

to comply with these rules, instead, there would be a commercial rationale to do so given the negative cost of data breaches.[34] Moreover, if a fintech entity adopts and implements the standards prescribed in these guidelines then it can legally absolve itself from liability for damages on the grounds of negligence as specified under section 43A of the IT Act. If not, then the entity leaves itself vulnerable to monetary claims for damages.

Thus, there would be an economic case for fintech entities to implement the standards rather than a legal obligation— which allows us to argue for a co-regulatory approach; this approach should ensure that the data of users is well protected while at the same time ensuring that there is no unnecessary burden on smaller players in the fast-evolving fintech industry. If a fintech entity believes that it is too small or deals with extremely small amounts of data, it can take a commercial decision (risk) on whether to comply with the standards at all or follow its own policies. If it chooses the latter, then in case of a data breach, it will have the obligation to prove in court that its policies comprise reasonable security practices and procedures.

Any regulations prescribing standards for information security would have to take into consideration a number of issues, some of the more significant of which are discussed below:

A. To include fintech entities not located in India

Due to the very nature of the internet, it has become very easy for entities to offer services to consumers across borders. While the capital controls imposed by the RBI do pose certain restrictions in the Indian context,[35] the advent of Web3.0 and decentralised finance (DeFi) poses fresh challenges to the *status quo*. This was most popularly witnessed in the crypto sector where certain exchanges continued to function despite the (now repealed) restrictions imposed by the RBI in April 2018.[36][37] It is therefore important for any regulation dealing with fintech to include within the ambit not only entities established or located within the territorial borders of India but also those which are not located within India but are offering services within India. However, some filtration mechanisms would have to be used to exclude entities that have a minuscule presence or whose activities are not geared towards

[34] Manas Tripathi and Arunabha Mukhopadhyay, 'Financial Loss Due to a Data Privacy Breach: An Empirical Analysis' (2020) 30 Journal of Organizational Computing and Electronic Commerce 381 <https://doi.org/10.1080/10919392.2020.1818521> accessed 19 October 2022.

[35] See generally the Foreign Exchange Management Act, 1999.

[36] WazirX being the most prominent among them.

[37] RBI Circular No. DBR.No.BP.BC.104 /08.13.102/2017-18 dated April 6, 2018.

India to ensure that compliance does not become a burden to commercial activity. The mechanism used in the EU General Data Protection Regulation and followed to some extent in the Consumer Protection (E-commerce) Rules, 2020 could offer useful guidance in this regard.[38]

B. Definition of Personal Data

The definition of personal data needs to ensure that all aspects of a person's identity whereby the person could be directly or indirectly identifiable should be covered. Although it may not be possible for the definition to be entirely future-proof, it should at the very least take into account existing technology to ensure its own resilience. To illustrate, a few years ago, anonymization of data was considered an acceptable standard of data protection, however, with the decreasing costs of computing power and increased pervasiveness of big data it is now possible to re-identify individuals from different sets of anonymised data and anonymisation by itself may not be considered an acceptable tool for data protection anymore.[39]

C. An adequate classification of fintech Entities

While strict standards for privacy and data protection would be laudable aims in themselves when dealing with industry and especially a sunrise sector such as fintech, one must be pragmatic and ensure that we do not throw out the baby with the bathwater. Painting all fintech entities with the same brush and imposing onerous obligations on smaller bootstrapped start-ups just because they are offering services to a few clients in the fintech sector and perhaps not even dealing with very sensitive financial data, would not be beneficial to the growth of the fintech sector. In this context, it may be beneficial to classify entities based on various factors such as the amount of money at risk, the type of data being collected, the number of customers, etc. to calibrate the extent of data protection measures that would need to be implemented by the different fintech entities. The regulation could impose different data protection obligations on fintech entities with the security standards to be implemented getting increasingly stricter and stronger with the increase in the number of customers served, value at risk, the sensitivity of the data, etc. The stricter standards could also include obligations such as periodic security audits and updating of the security practices pursuant

[38] Art 3, read with Recital 23 of the Regulation; r 2(2) of the Consumer Protection (E-Commerce) Rules 2020.

[39] Imperial College London., 'Anonymizing Personal Data "not Enough to Protect Privacy," Shows New Study' (*Science Daily*, 23 July 2019) <https://www.sciencedaily.com/releases/2019/07/190723110523.htm> accessed 19 October 2022.

thereto. Such an approach would ensure that the regulatory requirements do not act as an entry barrier for further innovation in the fintech sector. A similar approach was used in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[40]

D. Minimum Data Protection Requirements

While it's important to distinguish between various fintech entities to find appropriate regulatory standards, there ought to be some fundamental data security and confidentiality rules that would have to be observed by all fintech businesses. These basic requirements should broadly adhere to the privacy principles suggested in the Justice A.P. Shah Committee Report.[41] In brief, these principles are:

Notice: Fintech entities should give a simple-to-understand notice of their information practices to all individuals before collecting any personal information.

Choice and Consent: Fintech entities should give individuals opt-in and opt-out choices with regard to providing their personal information and take their informed consent for collection of the same.

Collection Limitation: Fintech entities should only collect such amount of personal information from consumers as necessary to provide the service.

Purpose Limitation: Personal data collected and processed by the fintech entities should be adequate and relevant to the purposes for which it is collected. If there is a change of purpose for usage of the data, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures.

Access and Correction: Customers should not only have access to the personal information about them held by the fintech entity, but should also be allowed to seek correction, amendments, or deletion of such information where it is inaccurate.

Disclosure of Information: Fintech entities should not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure.

[40] R 2(1)(w) of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 which uses the concept of a significant social media intermediary.

[41] *Report of Group of Experts on Privacy* (Planning Commission, Government of India 2021) <http://planningcommission. nic.in/reports/genrep/rep_privacy.pdf>.

Security: Fintech entities shall employ reasonable security safeguards to secure users' personal information against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, and unauthorized disclosure either accidental or incidental or other reasonably foreseeable risks.

Accountability: Fintech entities should be accountable for complying with measures that uphold privacy principles. Such measures may include mechanisms to implement privacy policies including tools, training, and education as well as external and internal audits, etc.

Openness: Information regarding the steps taken in order to ensure compliance with the privacy principles shall be made available to all consumers in an intelligible form, using clear and plain language.

E. Option for Co-regulation

A parallel model that could be considered is the development and certification of industry-led data protection standards. As discussed above, such a model could be especially useful as it enables the fintech entities to take into account the peculiarities and specific context of their business operations, whether in relation to a particular product or service category.[42] Simply put, the fintech industry should have the option to develop its own standards of best practices for data protection. The Central Government may introduce a process of getting such industry-developed standards certified by a competent authority to ensure their adequacy in terms of strictness and resilience. Once such a standard is notified for a particular part of the fintech sector, all entities in that sector would have the option to either follow such industry-developed and notified standards or the standards prescribed in the Rules.

F. Designation of Data Protection Officers

Fintech entities should be required to designate a specific data protection officer to inform and advise the entity and its employees on data protection issues, monitor the implementation and compliance with data protection standards, supervise updates to the data protection policies as well as act as the nodal person for all data protection issues. To ensure that this obligation does not impose too heavy a cost, smaller fintech entities could allow

[42] Maximilian Grafenstein, 'Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the "State of the Art" of Data Protection-by-Design' (18 February 2019) <https://papers.ssrn.com/abstract=3336990> accessed 19 October 2022.

the data protection officer to take up tasks and duties other than merely data protection. A similar approach has also been envisaged under the EU General Data Protection Regulations.[43]

G. No delay in breach notification to customers

In order to maintain complete transparency with regard to the safety of customer data, there should be an obligation on fintech entities to not only report any breaches to the CERT-In as is required by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 but also inform the customers in case of any breach of customer data without undue delay.

On a final note, while, there are various sectoral privacy and security regulations e.g., RBI's 2018 data localisation circular, RBI's Master Direction on Digital Payment Security Controls, SEBI's Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants, IRDAI guidelines on Information and Cyber Security, these sectoral legislations are limited to the sectors that they govern. They do not cover other important sectors such as e-commerce, crypto assets, etc. This is why a data protection regulation that transcends sectoral limits is needed.

Conclusion

With the fast-paced growth of the fintech sector coupled with the Government's push towards a cashless and digital economy, there is an urgent need to strengthen the data protection regime for this critical sector. The withdrawal of the Data Protection Bill, 2019 and criticism of the newly issued Digital Personal Data Protection Bill, 2022 means that the enforcement of a comprehensive data protection regime could still be some time away. In this context, it is imperative to bring about regulations to establish a data protection regime for the growing fintech sector before the lack of strong regulations leads to major consumer disasters. As we have argued, such stop-gap regulations would nonetheless have to take into consideration certain basic aspects of data protection such as the privacy principles, the definition of personal data, the inclusion of non-residential actors, co-regulation, proper classification of entities, etc. in order to strike an ideal balance between providing adequate data protection and ensuring the growth of the industry.

[43] Art 38(6) of the EU-GDPR.

FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy

*Vidushi Marda and Amber Sinha**

Abstract *In the last five years, the Fintech sector has thrived in India, with Machine Learning (ML) driven credit scoring based on alternative data, emerging as a growing segment. The credit scoring industry in India needs to be viewed in light of a careful examination of rights, inclusion, appropriate safeguards and discrimination, currently missing from the discourse and practices. In this paper, we explain how ML-based credit scoring works, and the regulatory and commercial factors that have enabled and impeded its growth in India. Through legal and technological analysis, richened by insights from qualitative interviews with entrepreneurs and practitioners, we provide a detailed picture of the credit scoring sector, and highlight its spillover privacy and predatory impacts in India.*

I. Introduction

Financial Technology ("FinTech") is defined as the intersection of the financial services and technology sectors, where technology-focused start-ups and new market entrants innovate the products and services traditionally provided by the financial services industry.[1] There are over seven thousand

[*] Vidushi is a Lawyer and Senior Programme Officer at Article 19. Amber is a Lawyer and Trustworthy AI-Senior Fellow at Mozilla Foundation.

FinTech companies in India, next only to the US and China.[2] In 2021, there were investments of over USD 8 million in this segment in India.[3] This includes a wide range of financial services, from lending and payments, to alternate credit scoring and insurance. There are several factors that led to the rise of the FinTech industry in India. The Indian government's investment in a digital ecosystem, its focus on increasing bank accounts accessible through Aadhaar-based verification, and the decision to demonetise about 85% of currency in circulation in 2016 have all contributed to a boost in the Fintech sector. The sector promises nimbler and cost-effective financial services, and can enable financial inclusion through a range of services including new methods of risk assessment and mobile wallets. The potential for India's FinTech sector to attract global investment and incentivise economic growth has also attracted attention from start-ups, investors,[4] and regulators.[5] Further, these services have evolved in the context of the narrative of financial inclusion—over 95% of the Indian population has no credit history as they lack the financial truncation history to generate CIBIL scores.[6] The Government's push towards a digitally empowered society is visible through its Digital India initiative.[7] The Reserve Bank of India has played a key role in enabling FinTech companies to emerge and operate in India by encouraging innovation and providing the regulatory and infrastructural capabilities to

[1] 'Blurred Lines: How FinTech is Shaping Financial Services' (*PwC,* March 2016) <https://www.pwc.de/de/newsletter/finanzdienstleistung/assets/insurance-inside-ausgabe-4-maerz-2016.pdf> accessed 23 April 2023.

[2] 'At $29 bn, Indian Fintech Sector Now has 14% Global Funding Share: Report' *Business Standard* (New Delhi, 22 August 2022) <https://www.business-standard.com/article/companies/at-29-bn-indian-fintech-sector-now-has-14-global-funding-share-report-122082201014_1.html> accessed 23 April 2023.

[3] Naina Bhardwaj, 'India Briefing, What Trends are Driving the Fintech Revolution in India?' (*India Briefing*, 9 June 2022) <https://www.india-briefing.com/news/what-trends-are-driving-the-fintech-revolution-in-india-23809.html/> accessed 23 April 2023.

[4] Arti Singh, 'Fintech VC Report Card— Part III: Omidyar vs. Kalaari vs. Blume vs. Prime vs. Ribbit' *The Economic Times* (29 January 2019) <https://prime.economictimes.indiatimes.com/news/67733067/fintech-and-bfsi/fintech-vc-report-card-part-iii-omidyar-vs-kalaari-vs-blume-vs-prime-vs-ribbit> accessed 23 April 2023.

[5] 'Initiatives by India's Government to Boost FinTech' (*FinTech Futures*, 2 January 2019) <https://www.fintechfutures.com/2019/01/initiatives-by-indias-government-to-boost-fintech/> accessed 23 April 2023.

[6] Tarunima Prabhakar, CLTC White Paper Series, A New Era for Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending (*Centre for Long-Term Cybersecurity, University of California Berkeley,* June 2020). <https://cltc.berkeley.edu/wp-content/uploads/2020/06/A_New_Era_for_Credit_Scoring.pdf> accessed 23 April 2023.

[7] 'Digital India - A Programme to Transform India into Digital Empowered Society and Knowledge Economy' (*Press Information Bureau- Government of India,* 20 August 2014) <http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926> accessed 23 April 2023.

do so.[8] Further, the Artificial Intelligence Task Force set up by the Ministry of Commerce and Industry identifies FinTech as a domain of relevance and priority for the Government of India.[9]

The digital lending industry in India has benefited from government and regulatory support and grew rapidly chiefly due to two reasons.[10] First, Aadhaar, the biometric identity scheme in India, meant that companies could verify and onboard potential lendees at virtually no cost in terms of time and money. Second, the ability to scrape intimate details about a person's life from social media, text messages, call records etc. using sophisticated algorithmic and statistical models meant that analysis of profiles could be much more granular at a negligible cost.

In 2018, there were two significant changes in the ability of FinTech companies to take advantage of these options. First, following the Supreme Court's verdict on Aadhaar, the ability to use Aadhaar numbers for onboarding customers has been significantly curtailed. Second, the Personal Data Protection Bill was introduced, revised several times and finally withdrawn. The draft of a new Digital Data Protection Bill has been released by MeitY and 2022, is yetto be passed, with significant implications for the use and processing of data. Therefore, despite the Supreme Court's decisions on right to privacy and restrictions on private use of Aadhaar, the Fintech industry has grown in India, with little, if any regulation of the data ecosystem that it relies on. This recent development in the absence of data governance provisions had direct and clear implications for the privacy and autonomy of individuals who are the primary customers of this industry.

Against this background, this paper will study the impact of these changes on the FinTech lending sector in India and subsequent developments, with specific reference to implications for privacy and autonomy. It aims to do so to bridge some gaps between academic analysis and industry insights in the context of alternate lending. Section I provides background and an introduction to this report. Section II will offer a primer on the privacy and security opportunities, limitations, and vulnerabilities offered by the two

[8] Report of the Working Group on FinTech and Digital Banking (*Reserve Bank of India*, 2017) <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF> accessed 23 April 2023.

[9] Report of the Artificial Intelligence Task Force (*Department for Promotion of Industry and Internal Trade*, 20 March 2018) <https://dipp.gov.in/whats-new/report-task-force-artificial-intelligence> accessed 23 April 2023.

[10] Gopal Sathe 'After Beta-Testing on a Billion Indians, The Tech behind Aadhaar is Going Global: Modi Bats for India Stack at Singapore Summit' (*HuffPost India*, 12 June 2018) <https://www.huffingtonpost.in/2018/06/06/after-beta-testing-on-a-billion-indians-the-tech-behind-aadhaar-is-going-global_a_23452248/> accessed 23 April 2023.

technologies that form this report's focus: Aadhaar-based authentication, and machine-learning based lending in the FinTech sector. Section III will analyze the policy developments that have had an impact on FinTech companies' ability to conduct business, and lay out the current state of affairs. Section IV will contextualize analysis with perspectives from practitioners in the FinTech sector, gathered through a series of qualitative interviews. Section V will conclude with findings and recommendations.

II. Evaluating underlying technologies

A. Aadhaar-based authentication

Aadhaar, the largest biometric identity project in the world, was introduced in 2009 by the Government of India. It intends to provide unique identification for Indian residents that can be used for the efficient delivery of services. The Unique Identification Authority of India (UIDAI) is the authority in charge of Aadhaar enrollment and authentication, created to issue unique identification numbers that are *"(a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way."*[11] At the time of enrollment of individuals into the Aadhaar system, both biometric and demographic details such as name, date of birth, and address are collected. This includes fingerprints, iris scans, and photographs of each individual being enrolled. This data is stored in the Central Identities Data Repository ("CIDR").

A key component of FinTech lending is the process of Know Your Customer ("KYC") - the due-diligence that lenders need to carry out at the time of verifying and assessing potential customers by obtaining appropriate information about them.[12] Following the Aadhaar Act of 2016, private companies were allowed to use Aadhaar - which meant that lenders could lower compliance costs to carry out KYC and customer onboarding, essentially completing the process in a matter of minutes as opposed to a few days.[13]

[11] 'About UIDAI' (UIDAI - Government of India) <https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html#:~:text=The%20Unique%20Identification%20Authority%20of,the%20Ministry%20of%20Electronics%20and> accessed 23 April 2023.

[12] Reserve Bank of India, 'Guidelines on Digital Lending' (*Reserve Bank of India*, 2 September 2022) <Lending. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF> accessed 23 April 2023.

[13] KYC Solutions, 'Problems and Challenges in Traditional KYC Systems' (*Records Keeper,* December 2016) <https://www.recordskeeper.com/blog/kyc-solutions/problems-challenges-traditional-kyc-systems/> accessed 23 April 2023.

This linkage with Aadhaar was facilitated through India Stack, *"a set of APIs*[14] *that allows governments, businesses, startups and developers to utilise a unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery."*[15] This Stack, the first of several other emerging stacks in India leveraging digital identity has a cashless, paperless, presence less and consent layer, intended to enable APIs for Aadhaar Authentication and eKYC developed by the UIDAI, eSign meant for digital signature developed by the Controller for Certifying Authorities, UPI developed by National Payments Corporation of India, among others. The Open API policy forms the basis of both India Stack and National Health Stack services. Open APIs, in their existing form in government applications, allow interoperability between different e-Governance applications. Despite these initiatives, the source code of such applications has not been made available under the open-source license, thus not making it possible to be tested and audited openly. Parts of this centralised digital infrastructure remain proprietary. It is still prescriptive of what kind of solutions can be built upon it. Hence, while the India Stack and the National Health Stack are built on open APIs, they offer limited opportunity opportunities for other stakeholders to build different kinds of services. Further, the infrastructural requirements assumed currently for such an ecosystem to function effectively, do not match the infrastructural availability on the ground. Thus, services such as UPI, e-Sign, and e-KYC would still be inaccessible to a large section of the population, as they require access to a mobile phone and network connectivity. For the purposes of FinTech lending, there are two APIs within India Stack that were particularly relevant; the first is e-KYC[16] which embraces India Stack's paperless goal, by verifying the identity and address of a person through Aadhaar authentication. The second is e-Sign, which *"allows an Aadhaar holder to electronically sign a form/document anytime, anywhere, and on any device legally in India."*[17]

[14] API stands for Application Programming Interface, which is essentially a set of clearly defined methods of communication between various software components. For further reading, please see 'What is an API? In English, Please' (*freeCodeCamp*, 19 December 2019) <https://medium.freecodecamp.org/what-is-an-api-in-english-please-b880a3214a82> accessed 23 April 2023.

[15] 'About India Stack', <https://indiastack.org/about/> accessed 23 April 2023, 'Whats is the India Stack?; All You Need to Know' *Times Now* (13 February 2023) <https://www.timesnownews.com/technology-science/whats-is-the-india-stack-all-you-need-to-know-article-97860756#:~:text=According%20to%20the%20official%20website,%2C%20and%20cashless%20service%20delivery.%22> accessed 23 April 2023.

[16] 'India Stack's explanation on E-KYC' <https://indiastack.org/ekyc/> accessed 23 April 2023.

[17] 'India Stack's Explanation on E-SIGN'<https://indiastack.org/esign/> accessed 23 April 2023.

The use of Aadhaar-based authentication in the FinTech sector brought down the cost of onboarding substantially, making smaller loans economically viable for lenders, and opening up the market to "*previously underserved communities*."[18] The emergence of India Stack allowed apps to authenticate new customers via Aadhaar's eKYC, an online authentication mechanism linked to people's unique Aadhaar IDs, and also leverage UPI a real-time money transfer protocol.[19] Together, they dramatically reduced the costs of both onboarding customers and transfer of funds for online businesses.

Even so, the Aadhaar system has been a controversial topic of public debate since its inception for multiple reasons. It has worrying implications for the enjoyment of fundamental rights enshrined in the Indian Constitution, particularly the right to privacy.[20] Aadhaar has also come under focus for having major security flaws,[21] with multiple leaks being revealed over the years.[22] There are also privacy implications of India Stack, as services such as eKYC and UPI collect sensitive data of residents during transactions. The financial data allows more power to banks and other financial institutions, as it can be used for creating credit profiles of residents.[23] The ability of the project to meet its goals of unique identification through biometric authentication has also been strongly critiqued over the years following costly errors sometimes leading to loss of life, insecure software and multiple hacks.[24]

[18] PP Thimayya, 'India Stack to Serve the Underserved', *The Financial Express* (August 2017) <https://www.financialexpress.com/industry/technology/india-stack-to-serve-the-underserved/821926/> accessed 23 April 2023.

[19] RohinDharmakumar,'AadhaarandtheGradualCollapseofIndiaStackLivebyAadhaar,Dieby Aadhaar', <https://the-ken.com/story/aadhaar-and-the-gradual-collapse-of-india-stack/>.

[20] Amber Sinha and Pranesh Prakash, 'Privacy Concerns Overshadow Monetary Benefits of Aadhaar Scheme' *The Hindustan Times* (New Delhi, 12 March 2017) <https://www.hindustantimes.com/india/privacy-concerns-overshadow-monetary-benefits-of-aadhaar-scheme/story-E3o0HRwc6XOdlgjqgmmyAM.html> accessed 23 April 2023.

[21] Usha Ramanathan, 'All is not well with Aadhaar' *The Indian Express* (7 January 2018) <https://indianexpress.com/article/opinion/columns/all-is-not-well-with-aadhaar-leak-aadhaar-details-5013305/> accessed 23 April 2023.

[22] Amber Sinha and Srinivas Kodali, 'Information Security Practices of Aadhaar (or lack thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information' (*The Centre for Internet and Society,* 16 May 2017) <http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1> accessed 23 April 2023.

[23] Shashidhar KJ, 'Privacy International Raises Concerns over IndiaStack & UPI for Establishing Financial Identity' (*Medianama*, 4 December 2017) <https://www.medianama.com/2017/12/223-privacy-international-upi-indiastack/> accessed 23 April 2023.

[24] Reetika Khera, 'Aadhaar Failures: A Tragedy of Errors', Economic & Political Weekly (2019) 54 (16) <https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare> accessed 23 April 2023.

In the case of FinTech companies using Aadhaar for onboarding customers - each case of authentication *and authorisation creates a digital trail*, providing the government, and (in the absence of adequate safeguards in the law) potentially private parties with access to granular information about intimate details of individual's lives. While the central repository of the Aadhaar ecosystem maintained by the UIDAI may be more secure, the project has also led to the creation of an ecosystem built around the digital identity framework where other public and private actors also interact with the identity program leading to exponentially increased generation of data. The API-based system means that various actors are involved in building services on top of the Aadhaar identity layer. Further, the seeding of other public databases with Aadhaar numbers also meant that personal and sensitive data held by other government operations was now integrated with Aadhaar data. Even if we assume that the CIDR, the central repository which houses the enrolment data including biometrics is secure, the nodal points which engage with Aadhaar data, and often involve collection, storage, access to and processing of Aadhaar numbers, biometrics and connected profiling data often lack similar technological or process protections. These include cybersecurity protections, strict processes such as access control and severe penal provisions.

Particularly in the context of e-KYC, the privacy implications of Aadhaar authentication became a cause of grave concern following the passage of the Aadhaar Act in 2016.[25] Before 2016, the CIDR was only meant to provide a "yes" or "no" answer for the purpose of authentication. This was also explicitly provided for in the National Identification Authority of India Bill 2010 (NIAI) which contemplated only these two responses from the CIDR, *"The Authority shall respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic information and biometric information."*[26] While this Bill did not become law, the Aadhaar Act that was passed in 2016 removes the safeguards contemplated in the NIAI Bill 2010. Under the Aadhaar Act, the CIDR is now permitted to respond with, *"a positive, negative or any other appropriate response sharing such identity information excluding any core biometric information."*[27] What is particularly worrying in light of this change is that the term "appropriate response" is not defined, leaving it susceptible to wide interpretation, which could *prima facie* include

[25] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, s 57.

[26] The National Identification Authority of India Bill ('NIAI') 2010, s 5(2).

[27] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act 2016, s 8(4).

demographic information. Therefore, from a pure authentication system which would ensure a degree of data minimisation, the possibility that requesting entities could access more identity information without user consent is built into this process. This added provision also belies the claim that Aadhaar is intended only for correct authentication, and demonstrates that there may be a clear intent for mission creep to use the authenticating system for greater sharing of personal data.

B. Machine learning based lending

One of the promises that FinTech lending brings to the fore is that of financial inclusion. The fact that individuals who were earlier invisible to traditional financial services and formal credit systems, are now potential customers, can be owed to the fact that FinTech companies access data about individuals that did not traditionally factor into credit decisions.[28] The ability to factor in non-traditional types of data, and look at 20,000 - 30,000 data points[29] that signal various aspects of a person's life for the purpose of assessing creditworthiness brings the promise of banking to those who previously thought they were ineligible. This is because of increasing reliance on machine learning systems that improve the performance of a task over time, at speeds and scales that are far beyond the reach of humans. To glean intimate details about a person's life from their behaviour online, and factor in these data points into building a cohesive map of an individual's life is essentially what ML systems offer in the FinTech lending sector.[30] ML-based lending, thus introduces the promise of efficiency at scale in assessing the credit-worthiness of potential customers.

The ability of ML systems to learn from examples, make inferences and spot patterns at great speeds and enormous scale contribute to the excitement surrounding the use of these systems in the financial services sector.[31] The use of ML systems for making decisions about credit, for example,

[28] M.A. Bruckner, 'The Promise and Perils of Algorithmic Lenders' Use of Big Data' Chicago-Kent Law Review (2018) 93(1) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137259> accessed 23 April 2023.

[29] Raktim Nag, 'How Matrix Backed FinTech Startup Finomenais Disrupting the $8 Bn Youth Loan Market'(*Inc 42*, 10 June 2016) <https://inc42.com/startups/finomena/> accessed 23 April 2023.

[30] Dirk A. Zetzsche and others, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) University of Hong Kong Faculty of Law Research Paper No. 2017/007 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959925> accessed 23 April 2023.

[31] Peter Martey Addo, Dominique Guegan, and Bertrand Hassani, 'Credit Risk Analysis using Machine and Deep Learning Models' (2018) University Ca' Foscari of Venice, Dept. of Economics Research Paper Series No. 08/WP/2018 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155047> accessed 23 April 2023.

significantly changes the manner in which traditional lending takes place.[32] FinTech startups can now use new sources of data, such as social media data, or call data, to make decisions about the credit-worthiness of individuals.[33] These non-traditional types of data are often termed "alternative data". Some FinTech companies factor in up to 22,000 data points to assess credit-worthiness of individuals.[34] The impact of such technology on the overall landscape of financial services, particularly on financial inclusion is well understood.[35] However, the implications of these systems on privacy, identity, and inclusion are less thoroughly considered.

While thinking through the implications of ML systems, it is essential to understand the process through which these systems are built and deployed. In an academic paper published in 2018, Marda offers a framework for this by dividing the ML process into three distinct steps: Data, Model, and Application.[36] ML algorithms are trained on datasets often referred to as *"training data"*. For the purposes of FinTech lending, this could be datasets that contain information about people's behaviour online, their spending patterns, their living conditions, geolocation, and so on. As mentioned above, some FinTech companies in India have publicly acknowledged that the number of data points is often around 20,000.[37]

III. Data

ML-enabled credit scoring works by collecting, identifying and analysing data that can be used as proxies for information that helps answer the three key questions in any credit scoring model— a) identity, b) ability to replay and c) willingness to repay. With the advent of Big Data and greater digitization

[32] Matthew A. Bruckner, 'Regulating FinTech Lending'(2018) 37(6) 1 Banking & Financial Services Policy Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3207365> accessed 23 April 2023.

[33] Vivina Vishwanathan, 'SMS, Social Media may Reveal Credit Strength' (*Livemint*, 17 November 2015) <https://www.livemint.com/Money/9LdV0ttbYT2BgVFbLwN6UM/SMS-social-media-may-reveal-credit-strength.html> accessed 23 April 2023.

[34] Aparajita Choudhury, 'How Finomena is Making it Possible for Borrowers without Credit Scores to get a Loan', (*YourStory*, 18 February 2017) <https://yourstory.com/2017/02/finomena-2/> accessed 23 April 2023.

[35] Shekhar Lele, 'Fintech 2.0: A New Era of Financial Inclusion' (*PwC*, November 2018) <https://www.pwc.in/consulting/financial-services/fintech/fintech-insights/fintech-2-0-a-new-era-of-financial-inclusion.html> accessed 23 April 2023.

[36] Vidushi Marda, 'Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making' [2018] Philosophical Transactions A: Mathematical, Physical and Engineering Sciences <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240384> accessed 23 April 2023.

[37] Nag (n 29).

and datafication of information, new data sources such as telecom data, utilities data, retailers and wholesale data and government data, are available. Examples of telecom data include prepaid data and recharge patterns that are said to provide insights about a person's cash flows. The daily call patterns and location data can indicate whether a person is working a steady job or not. One of the key sources of proxy data about income and spending is the texts about payments, and the credit and debit texts received on the consumer's mobile phone. Payment of bills, purchases made, regular remittances and made or received are all deemed very useful in predicting a consumer's ability and intent to repay.

The digitisation of records and the use of digital payment mechanisms to pay utilities bills make this data available for analysis. This data not only shows the consumption patterns of an individual but also how timely the person is in making payments. The payments cycles for utilities bills are usually periodic, like monthly repayment cycles and therefore considered highly indicative of how the person handles their monthly financial obligations. In India, electricity bills, which indicates the usage of household appliances, are widely seen as good indicators of socio-economic status and income.[38] Retailers' data can be used to evaluate the individual's expendable income, their family structure, other relevant characteristics, for instance, purchase of certain goods can suggest health consciousness while others may indicate risk taking abilities.

The metadata collected by the mobile apps used by small lending firms are analysed to derive insights about the consumer. The mobile apps typically seek various permissions to access other data on the person's mobile phone and their logon identities like Facebook and Google. Further, psychometric analysis of the manner in which the consumer fills the online form on the app, such as time taken on each question, the number of times an answer was changed etc. are also seen as indicative of the individual's character.[39]

IV. Model

As algorithms train, what emerges from the training process is called a *"model"* which is a decision matrix that can then be refined and tested till

[38] Shivam Shankar Singh, *How to Win an Indian Election: What Political Parties Don't Want You to Know* (Penguin Ebury Press 2019).

[39] Amber Sinha, 'Big Data in Credit Scoring', in Elonnai Hickok, Sumandro Chattapadhyay and Sunil Abraham (eds), *Big Data in Governance in India: Case Studies* (The Centre for Internet and Society 2017) <https://cis-india.org/internet-governance/files/big-data-compilation.pdf> accessed 23 April 2023.

it is considered appropriate for deployment. As models continue to be built and trained, they are deployed when they get comfortably close to a definition of "success" as laid out by the engineers who build these systems. Once this is achieved, models can be deployed for the purposes of credit scoring, underwriting, etc. This means that the definition of success, the choice of data used to train algorithms, and the criteria used to assess the performance and appropriateness of machine learning models are all extremely subjective, human decisions. This stands in strong contrast to the generally held belief that algorithmic models are all-knowing, neutral and objective.

Traditionally, credit scoring algorithms would consider set categories of data such as an individual's payment history, debt-to-credit ratio, length of credit history, new credit, and types of credit in use.[40] Machine learning algorithms as envisioned by the FinTech sector use thousands of alternate data points such as the number of contacts in one's phone, call logs, and social media behavior to discern an individual's creditworthiness.[41] The first implication of this type of model is that it is not always possible to explain why a certain decision was made, as models that use complex techniques like neural networks are inscrutable even to those individuals who build them. Given the vast amount of data analyzed and complex structures within neural nets it may not even be possible for lenders to understand why certain loan applications are approved while others are rejected. Second, creditworthiness is not easy to predict, particularly given that historical data on access to credit, payment and default is imbued with a number of societal realities along the axes of gender, class, caste, religion, and so on — complexities that datasets do not reflect. For instance, if a model is trained with data only about men receiving and repaying loans, and does not 'learn' from any examples of women being good credit prospects, this could risk women's access to credit in the future.[42]

With the introduction of new forms of data, the richness of data may theoretically increase the predictive power of the algorithm. However, narratives on greater accuracy presume both the suitability of input data towards

[40] See National Consumer Law Center, *Fair Credit Reporting* § 16.4.5.2, at 720 (9th edn 2017).

[41] Pierre Biscaye and others, 'Review of Digital Credit Products in India, Kenya, Nigeria, Tanzania and Uganda' (2017) EPAR Technical Report #351a <https://epar.evans.uw.edu/sites/default/files/EPAR_UW_351a_Review%20of%20Digital%20Credit%20Products_4.12.17_0.pdf> accessed 23 April 2023.

[42] In a non-lending context, Amazon's hiring algorithm made a similar mistake; See Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool that Showed Bias against Women' (*Reuters,* 11 October 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> accessed 23 April 2023.

the desired output, as well as faith that past attributes or activities that are used as training data do not lead to unintended outcomes. The use of alternative data and assumptions about proxy factors that influence ability and willingness to pay are both largely untested. Therefore, there is a risk of creating a financial market which is dependent on unproven assumptions.

V. Application

The overarching narratives around the use of machine learning in the FinTech sector are that of efficiency, and providing credit to those who were not included in traditional financial systems. Individuals with thin credit files and limited interaction with financial services were stuck in a vicious circle that denied them credit, but with the use of alternate data, this can change. This narrative also promises quicker access to credit due to the sheer speed and agility of ML systems.[43] However, the limitations of these systems are significant in the context of FinTech lending and require thoughtful deliberation.

First, ML systems that are trained for the purpose of financial services need to carefully consider the data used to train systems. Financial disparity in India is large, and thus, the choice of datasets has an impact on how these systems will function. An ML system trained on the financial behavior of predominantly affluent people, for example, will systematically underperform or exclude less affluent people because of embedded assumptions about the “ideal” case in datasets. For instance, affluent people may, on average, have a significant portion of money being transferred to equity and debt investments, which can in turn become a proxy for the “ideal” individual. This is not a luxury that individuals from less affluent sections of society necessarily have, particularly not in a country like India, thus making them immediately at odds with the “ideal” loan applicant. Similarly, communities that have been systematically excluded by social and political norms will have distinct financial footprints and behaviors. Thus, an uncritical adoption of data can lead to a situation where people continue to be discriminated against and excluded simply because historical bias is being encoded in formal and opaque ways into ML systems.

[43] Arjuna Costa, Anamitra Deb, and Michael Kubzansky, Big Data, Small Credit: The Digital Revolution and its Impact on Emerging Market Consumers (2015) 10 (3-4) ‘Innovations: Technology, Governance Globalization’ 49 <https://ideas.repec.org/a/tpr/inntgg/v10y2015i3-4p49-80.html> accessed 23 April 2023.

A preliminary survey of the emerging companies in the Fintech sector in India done in 2017 and the profiles of their management teams show a preponderance of those with 44 technology and sales background and a lack of individuals trained in banking and finance.[44] This suggests an over-reliance on data and technology, and a tendency to ignore other kinds of expertise which have been integral to the credit scoring industry. This is reflective of the narrative that data is exhaustive and comprehensive enough to provide inferences that negate the need for domain expertise, theoretical models and interpretivism. However, this assumption has been greatly critiqued and various authors have pointed out the perils of the over-reliance on data.[45] However, this ignores the need for professionals with prior domain knowledge who can critically look at the predictions or inferences made by machine learning algorithms.[46]

Second, ML systems today often lack the Indian context: A classic credit underwriting ML system is built using practices imported from developed economies, which impacts their efficacy and accuracy in the Indian context. For example, people's geolocation and their call data records are thought to reveal a lot about their personalities and lifestyle. However, this assumption is lost in the context of loan applicants who are women from traditional families in some parts of India —a cellphone is not a personal possession, but rather a household one, often in the name of the head of the family who is invariably a man. This means that perfectly good candidates who deviate from the norm of what is considered "normal" behaviour in the West run the risk of being systematically excluded by these systems. Contextual development of models is key, failing which these systems could end up excluding vulnerable communities as the norm.

Finally, ML systems have profound implications for **privacy and autonomy.** From inferring intimate details about an individual's life, to potentially enabling surveillance, even well-intentioned ML systems can be detrimental to privacy. Further, the volumes at which these systems are trained mean that multiple correlations can emerge, some of which may pertain to sensitive

[44] Sinha (n 39).

[45] S. Leonelli, 'What Difference does Quantity Make? On the Epistemology of Big Data in Biology' (2014) 1(1) Big Data & Society <https://journals.sagepub.com/doi/epub/10.1177/2053951714534395> accessed 23 April 2023. ; Fulvio Mazzocchi, 'Could Big Data be the End of Theory in Science? A few Remarks on the Epistemology of Data-Driven Science (2015) 16(10) EMBO Reports1250 <https://doi.org/10.15252/embr.201541001> accessed 23 April 2023.

[46] Mireille Hildebrandt, 'Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning' (2019) 20(1)83 <https://doi.org/10.1515/til-2019-0004> accessed 23 April 2023.

attributes. Even if the correlation is only very slight, this is enough to build systems that factor in sensitive attributes. It is also unclear whether the use of ML has helped with access to credit in a sustainable way, and if financial inclusion is meaningfully achieved at all. The models, datasets, and applications that are currently in play are not subject to audits, with no transparency or accountability mechanisms.

The FinTech sector has grown substantially in the last few years because of these two factors, i.e. the option of Aadhaar-based authentication, and the growth in popularity of machine learning techniques and applications. As this Section demonstrates, however, the adoption of these technical 'solutions' cannot and should not be treated as straightforward or simplistic - particularly in a country like India, where the layers of complexity and disparity merit a close, deliberate and careful approach to critical services such as access to credit.

VI. Recent Regulatory Developments

Having discussed the promises and limitations of these two underlying technologies in the FinTech sector, we will now turn to a brief analysis of a few developments from the last few years that had an impact on companies' ability to use these technologies - the Aadhaar judgment and the Personal Data Protection Bill.

A. Aadhaar judgment

In September 2018, the Supreme Court of India upheld the constitutional validity of Aadhaar with a 4:1 majority, following the second longest hearing in the Supreme Court's history.[47] While the judgment covers a range of important and intricate issues from proportionality to surveillance, for the purposes of this paper, we will discuss the extent to which private parties' use of Aadhaar was curtailed, what questions remain, and what the status quo is.

In discussing the use of Aadhaar by private companies, Section 57 of the Aadhaar Act came into focus and was found to be unconstitutional by all three opinions that made up the judgment. This section allowed for the use

[47] Moneylife Digital Team, 'Historic Aadhaar Hearing, Second-longest in SC history, Concludes' (*Money life,*10 May 2018) <https://www.moneylife.in/article/historic-aadhaar-hearing-second-longest-in-sc-history-concludes/53992.html> accessed 23 April 2023.

of Aadhaar in establishing the identity of a person for **any** purpose, by a state or a body corporate or person.

While discussing this section of the Act, the majority found[48] that it was susceptible to misuse as:

> "(a) *It can be used for establishing the identity of an individual 'for any purpose'. We read down this provision to mean that such a purpose has to be backed by law. Further, whenever any such "law" is made, it would be subject to judicial scrutiny.*
>
> (b) *Such purpose is not limited pursuant to any law alone but can be done pursuant to 'any contract to this effect' as well. This is clearly impermissible as a contractual provision is not backed by a law and, therefore, first requirement of proportionality test is not met.*
>
> (c) *Apart from authorising the State, even 'any body corporate or person' is authorised to avail authentication services which can be on the basis of purported agreement between an individual and such body corporate or person. Even if we presume that legislature did not intend so, the impact of the aforesaid features would be to enable commercial exploitation of an individual biometric and demographic information by the private entities. Thus, this part of the provision which enables body corporate and individuals also to seek authentication, that too on the basis of a contract between the individual and such body corporate or person, would impinge upon the right to privacy of such individuals. This part of the section, thus, is declared unconstitutional."*

While discussing Section 57, Justice Bhushan found, "*When any law permits user of Aadhaar, its validity is to be tested on the anvil of threefold test as laid down in Puttaswamy case, but permitting use of Aadhaar on any contract to this effect, is clearly in violation of Right of Privacy. A contract entered between two parties, even if one party is a State, cannot be said to be a law. We thus, are of the view that Section 57 in so far as it permits use of Aadhaar on "any contract to this effect" is clearly unconstitutional and deserves to be struck down."*[49]

Finally, the dissenting opinion from Justice Chandrachud found "*Section 57 indicates that the legislature has travelled far beyond its stated object of ensuring targeted delivery of social welfare benefits. Allowing the Aadhaar*

[48] K.S. Puttaswamy v Union of India (2017) 10 SCC 1. A.K. Sikri, J. p 561.

[49] K.S. Puttaswamy v Union of India (2017) 10 SCC 1. Ashok Bhushan, J. Para 282, p 264.

platform for use by private entities overreaches the purpose of enacting the law. It leaves bare the commercial exploitation of citizens data even in purported exercise of contractual clauses. This will result in a violation of privacy and profiling of citizens." He further stated, "*Section 57 does not pass constitutional muster. It is manifestly arbitrary, suffers from overbreadth and violates Article 14.*"[50]

Following the judgment, FinTech firms had to grapple with alternatives to e-KYC that can offer similar ease of execution and .cost-effectiveness. At the time of the judgment being pronounced, there was a sense of doom within the FinTech industry.[51] Following this, the UIDAI offered two alternatives to continue using Aadhaar without sharing biometric information or the Aadhaar number - by either using a QR code[52] or a digitally signed XML file.[53] A few months down the line, it was clear that some types of lenders are hit more than others.[54] Lenders focusing on short-term, small ticket loans of less than one lakh, simply have not found economically viable options as traditional KYC costs are too high, and in the meanwhile are moving towards video-KYC,[55] and other methods through dialogue with regulators. On the other hand, lenders who are more diversified in the market seem to be embracing alternatives, such as more traditional banking KYC methods which rely on paper documents such as PAN and Driver's License. This form of authentication usually employs the Original Seen and Verified ("OSV") method where the original copy of the document should be seen and verified by the case officer. UIDAI also introduced its offline verification tools like XML databases and QR code-based solutions.

[50] K.S. Puttaswamy v Union of India (2017) 10 SCC 1. Dr Dhananjaya Y Chandrachud, J. Para 245, p 338.

[51] Vanita D'Souza, 'Here is Why the Aadhaar Verdict Left Fintech Companies in Ripples' (*Entrepreneur*, 23 December 2018) <https://www.entrepreneur.com/article/325288> accessed 23 April 2023.

[52] Mayur Shetty, 'Banks may Use Aadhaar QR Code for Paperless KYC' *The Times of India* (New Delhi, 26 October 2018) <https://timesofindia.indiatimes.com/business/india-business/banks-may-use-aadhaar-qr-code-for-paperless-kyc/articleshow/66370303.cms> accessed 23 April 2023.

[53] UIDAI, 'Offline Aadhaar Data Verification Service' (*UIDAI*, 23 August 2018) <https://uidai.gov.in/images/Offline-Aadhaar-Data-Verification-Service_v1-23082018.pdf> accessed 23 April 2023.

[54] Pratik Bhakta, 'India's FinTech Companies Struggle for an Alternative to Aadhaar' *The Economic Times*(21 December 2018) <https://economictimes.indiatimes.com/small-biz/startups/features/indias-fintech-companies-struggle-for-an-alternative-to-aadhaar/articleshow/67186586.cms> accessed 23 April 2023.

[55] Shreya Ganguli, 'RBI Mulls Live Video Authentication as Aadhaar eKYC Alternative' (*Inc42*, 10 December 2018) <https://inc42.com/buzz/rbi-mulls-live-video-authentication-as-aadhaar-ekyc-alternative/> accessed 23 April 2023.

While the judgment clearly finds Section 57 to be unconstitutional, there has been some speculation on the extent to which private players can use Aadhaar for e-KYC going forward. Shortly after the verdict was pronounced, Finance Minister Arun Jaitley stated that if the use of Aadhaar for private players *"is backed by a law, it is not unconstitutional."*[56] There have been legislative efforts to revive Aadhaar-based e-KYC for private parties through the Aadhaar and Other Laws (Amendment) Bill 2018.[57] This contemplates making furnishing Aadhaar "voluntary", and proposes amendments to the Prevention of Money Laundering Act and the Telecom Act, by allowing Aadhaar access to banks and telecom operators. Elsewhere, FinTech companies sought clarification on whether the use of e-KYC by them would be permitted if it was done on a voluntary basis.[58] There have been two views about the extent of the application of reading Section 57 down by the court. The first view posited that this meant that "private actors were not permitted to use the Aadhaar infrastructure even as requesting entities, even under a voluntary contract."[59] On the other hand, the second view argues that the wide definition of the term 'requesting entity' in the Aadhaar Act and the UIDAI's power to authenticate the request of any requesting entity also includes private sector parties.[60]

In July 2019, the Rajya Sabha passed the Aadhaar (and other laws) Amendment Bill.[61] In line with the Aadhaar judgment, Section 57 was omitted, however Section 4(4), Aadhaar Act was introduced to permit "an entity" to perform authentication, as long as (i) it was compliant with certain specified standards of privacy and security (which are yet to be specified) and (ii) it was permitted to offer authentication services by law or it was seeking

[56] Karan Dhar, 'Arun Jaitley Hints at New Law after Supreme Court Bars Private Companies from Using Aadhaar Data' (*Business Today*, 26 September 2018) <https://www.businesstoday.in/current/economy-politics/arun-jaitley-aadhaar-supreme-court-private-companies-banks-law/story/282886.html> accessed 23 April 2023.

[57] The Aadhaar and other Laws (Amendment) Bill 2019 <https://prsindia.org/files/bills_acts/bills_parliament/2019/Aadhaar%20and%20Other%20Laws%20(Amendment)%20Bill,%202019.pdf> accessed 23 April 2023.

[58] Yuthika Bhargava, 'FinTech Companies Seek Clarity on Using Aadhaar for e-KYC' *The Hindu* (New Delhi, 14 December 2018) <https://www.thehindu.com/business/fintech-companies-seek-clarity-on-using-aadhaar-for-ekyc/article25746312.ece> accessed 23 April 2023.

[59] Vrinda Bhandari, 'Governing ID: India's Unique Identity Programme' (*Digital Identities and Uses*, 6 February 2023) <https://digitalid.design/evaluation-framework-case-studies/india.html>accessed 23 April 2023.

[60] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, s 8(1).

[61] Aadhaar (and other Laws) Amendment Act 2019 (*PRS Legislative Research*) <https://www.prsindia.org/billtrack/aadhaar-and-other-laws-amendment-bill-2019> accessed 23 April 2023.

authentication for certain prescribed purposes. Through this legislation, the private sector use of Aadhaar was effectively restored. The Telegraph Act and the PMLA Act were also amended to allow various private entities to use Aadhaar for authentication.

In light of the Supreme Court's verdict discussed above, and consequent efforts to revive Aadhaar authentication for private companies, the use of Aadhaar for e-KYC going forward, in our view, will be impermissible even through a new law, given that the crux of such access involves: 1) commercial exploitation of an individual's sensitive personal information, including biometric and demographic information; and 2) through (voluntary)[62] contracts - the very basis on which the court struck down Section 57 in the first place. The legal rationale behind striking down the use of Aadhaar under Section 57 relies on the age-old dictum that what is prohibited by law, cannot be facilitated by way of contract. Section 57 played the role of carving out an entire ecosystem of contractual transactions, outside the purview of protections and governance in the Act. It is this carve out that the Supreme Court struck down, and has been reinstated contrary to the spirit of the Aadhaar judgment through the 2018 rules.

VII. Personal Data Protection Bill

The first version of the Personal Data Protection Bill[63] was published in July 2018, along with the final report[64] of the Justice Srikrishna Committee on Data Protection. Over the last four years, two subsequent versions of the bill, one from MeitY[65] and another from the Joint Parliamentary Committee haveemerged.[66] In each of these draft legislations, informed consent remains the primary ground for the processing of personal data. Although it must be noted that the scope of non-consensual grounds has only increased in each subsequent draft.

[62] Prasanna S, 'Section 57: Why Aadhaar can't be Used as Authentication by Private Companies' (*Medianama,* 27 September 2018) <https://www.medianama.com/2018/09/223-section-57-why-aadhaar-cant-be-used-as-authentication-by-private-companies/> accessed 23 April 2023.

[63] The Personal Data Protection Bill 2018 <http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf> accessed 23 April 2023.

[64] BN. Srikrishna and others, 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians: Committee of Experts under the Chairmanship of Justice B.N. Srikrishna' (*Ministry of Electronics and Information Technology*, 27 July 2018) <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 23 April 2023.

[65] Personal Data Protection Bill 2019 <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 23 April 2023.

[66] Report of Joint Committee on the Personal Data Protection Bill 2019.

For FinTech lending companies, the notion of informed consent is one that needs to be studied more closely. Most lenders obtain explicit consent from customers, by obtaining signatures and multiple consent forms as part of the onboarding process. The extent to which this consent is informed, free and specific is limited. For consent to be informed, when given in response to written declaration which also concerns other matters, requires the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. For consent to be free, we need to consider whether the performance of a contract or provisions of service is conditional on consent being provided to a non-negotiable, one-sided contract. This is particularly relevant in the context of alternative data given that lenders who factor in multiple data points from all aspects of an individual's life are, it can be argued, essentially carrying out a business model that is at odds with the purpose of data minimization and collection limitation. Another aspect to consider is the limitations on the storage of personal data, with the law contemplating that data fiduciaries *"shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed."*

While there are undoubtedly significant improvements made to the data protection landscape through the various versions of the Personal Data Protection Bills, a pessimistic reading of the draft legislations leads to the conclusion that it may not go too far in protecting consumers' data in the context of FinTech lending for two reasons:

First, while there is a requirement for informed and explicit consent, the latter is slowly becoming a surrogate for the former, particularly in the absence of existing mechanisms that explain how to operationalize informed consent in the context of FinTech lending. Second, the Bill does not talk about privacy considerations at the level of machine learning models, unlike the rights on automated processing and explanation provided in the EU's GDPR. This effectively means that models can continue to be opaque even once the Bill comes into force, and be built and deployed in a manner that is detrimental to the right to privacy of individuals.

Practices such as checking credit scores during background verification for employment, health insurance etc. have been criticized for a long time. However, big data-enabled credit scoring provides a far more granular profile involving different behavioral aspects of a person and the big data ecosystem provides more opportunities for credit data to be used for non-credit purposes. In light of the lack of regulation in the Fintech sector, there is a risk of such practices emerging as a business model to generate additional revenue for the companies.

VIII. Digital Lending Regulations

On September 2, 2022, the Reserve Bank of India (RBI) released a set of guidelines to regulate digital lending in India.[67] This followed a framework released by RBI in August 2022.[68] The regulations introduce some regulatory restrictions on digital lending apps. First, it introduces privacy protections for data collection carried by service providers. It requires that processing should be need-based with clear audit trails, and should be only done with the prior explicit consent of the borrower. In order to address, blanket app permission taken by such services, it imposes restrictions on access to mobile phone resources such as files and media, contact lists, call logs, and telephony functions. Further prescriptive provisions require that one-time access can be taken for the camera, microphone, location or any other facility necessary for the purpose of onboarding or KYC requirements only with the explicit consent of the borrower. Other obligations include the need for a privacy policy, data localisation, data security, transparency around data storage etc.

The second set of rules relevant for our discussion here is the obligation to ensure that the algorithm used for underwriting is based on extensive, accurate and diverse data to rule out any prejudices. RBI also imposes auditability requirements for the algorithm up to minimum underwriting standards and potential discrimination factors used in determining credit availability and pricing. In the same vein, the regulations encourage ethical AI which focuses on protecting customer interest and promotes transparency, inclusion, impartiality, responsibility, reliability, security and privacy. These are early attempts towards regulating predatory practices in the lending industry and will require significant fine-tuning and evolution. The first impressions of the industry have been largely negative towards the rules, with concerns around the prescriptive nature of the provisions.[69] One technology lawyer

[67] Reserve Bank of India, 'Guidelines on Digital Lending' (*RBI*, 2 September 2022) <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0> accessed 23 April 2023.

[68] Reserve Bank of India, 'Recommendations of the Working Group on Digital Lending - Implementation' (*Reserve Bank of India*, 10 August 2022) <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54187> accessed 23 April 2023.

[69] Reuters, 'India's Digital Lending Rules Spark Disruption, Firms Plan Pushback' *The Economic Times* (26 August 2022) <https://economictimes.indiatimes.com/tech/technology/indias-digital-lending-rules-spark-disruption-firms-plan-pushback/articleshow/93798112.cms> accessed 23 April 2023.

that the authors spoke to indicated that the Fintech industry was likely to ramp up lobbying efforts in response to the new rules, and advocated a lighter set of laws based on first principles. It remains to be seen how these political economic factors lead to the crystallization of financial regulation of digital lending. However, it must be noted that the RBI guidelines are only a threadbare first step towards regulation of the algorithmic lending regulations with very attention paid to anti-discrimination provisions. We will look at comparative regulations below.

Beyond analyzing recent regulatory developments, it is also important to briefly touch upon the absence of legal safeguards in the context of lending. In countries like the United States, for instance, the Equal Credit Opportunity Act, 1974 (ECOA Act) prohibits discrimination on the basis of certain protected characteristics like gender, race or marital status.[70] The ECOA also protects against policies that have a disproportionate impact on protected groups (also known as protecting against disparate impact).[71] It also institutes notice requirements which compel lenders to explain why they take 'adverse action' which includes refusal to grant credit, or refusal to increase the amount of credit available to an applicant.[72] In India, the Reserve Bank of India's Guidelines on Fair Practices Code for Lenders, 2003 suggests that lenders should not discriminate on the basis of caste, sex or religion, and also requires lenders to convey in writing *"the main reason/reasons which, in the opinion of the bank after due consideration, have led to rejection of the loan applications within stipulated time."*[73] However, these are merely recommendary guidelines, as recent research has found that FinTech companies in India do not readily disclose the reasons for the rejection of a loan.[74] The absence of binding regulation in India means that there are little to no safeguards in place for borrowers.

[70] Brian Kreiswirth and Anna-Marie Tabor,'What you need to know about the Equal Credit Opportunity Act and How it can Help you: Why it was Passed and What it is' (*Consumer Financial Protection Bureau*, 31 October 2016) <https://www.consumerfinance.gov/about-us/blog/what-you-need-know-about-equal-credit-opportunity-act-and-how-it-can-help-you-why-it-was-passed-and-what-it/> accessed 23 April 2023.

[71] Tarunima Prabhakar and Steve Weber, 'Financial Inclusion as a Fairness Criterion in Credit Risk Assessment' (*SSRN,* 25 June 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3579695> accessed 23 April 2023.

[72] 'Interactive Bureau Regulations: 12 CFR Part 1002 (Regulation B)' (Consumer Financial Protection Bureau) <https://www.consumerfinance.gov/rules-policy/regulations/1002/9/> accessed 23 April 2023.

[73] Reserve Bank of India, 'Guidelines on Fair Practices Code for Lenders' (*RBI*, 5 May 2003) <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=1172&Mode=0> accessed 23 April 2023.

[74] Tarunima Prabhakar and Steve Weber, 'Alternative Lending in a Digital Age: A Comparative Case Study in Regulation Across India and the United States' (*SSRN*, 19 May 2020) 22 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3956623> accessed 23 April 2023.

IX. How the industry coped

In order to bridge the gap between legal analysis and policy implications on one end, and practitioner perspectives on the other, this section will synthesize findings from six in-depth qualitative interviews[75] with entrepreneurs from the FinTech industry. Interviewees were founders and/or CEOs of leading FinTech lending companies in terms of market size in India that focus on easy and quick disbursal of loans, some entirely online, based on alternate data. These interviews were conducted to understand how FinTech players view policy changes in re: Aadhaar and data protection in context of their businesses, and how they have adapted to them. Interviews were semi-structure, but broadly, questions centered around *inter alia* understanding how alternate data featured in their business models, how FinTech companies view regulatory developments and whether there were certain bright lines for what definitely does or doesn't work for them, and how they coped with meaningful alternatives to Aadhaar onboarding.

The threads that emerged from interviews are discussed below:

1. **Viable alternatives to Aadhaar are possible and also feasible**: All interviewees acknowledged that the inability to use Aadhaar for onboarding customers, while inconvenient and most certainly a setback, was not fatal for most lending firms as several viable alternatives could be developed. This is for two main reasons. The first is that e-KYC was only allowed for loans up to Rs. 60,000 and some interviewees' firms only began lending at 1,00,000. For those interviewees who focus on smaller, shorter personal loans, methods of digital lending that don't require Aadhaar are currently being built and tested by the sector. Some interviewees mentioned working towards driver license or voter ID based verification, which one interviewee claimed would be "just as robust" as Aadhaar. Other lenders are moving towards video-KYC which is recognized by SEBI,[76] or an email-based KYC which works with some Non-Banking Finance Companies (NBFCs). For loans above a lakh, the KYC requirement of Original Seen and Verified (OSV) continues as it did before.

[75] The interviews have been completely anonymized in the interest of uniformity for this section.

[76] 'SEBI Comes Out with Revised KYC Norms for FPIs', *The Economic Times* (21 September 2018) <https://economictimes.indiatimes.com/markets/stocks/news/sebi-comes-out-with-revised-kyc-norms-for-fpis/articleshow/65902690.cms> accessed 23 April 2023.

However, after the new Aadhaar regulation circumvented the Aadhaar judgment, Aadhaar-based authentication again became the default for digital lending companies.

2. **UIDAI's offline verification tools do not inspire confidence:** The solutions offered by the UIDAI following the Supreme Court verdict, like the Offline Aadhaar XML file, or the QR code route do not seem like practical options for any of the interviewees. In case of the XML file, interviewees mentioned that it puts the onus on end customers to be digitally savvy. As one interviewee remarked, *"It may work for some, but it is not a solution for the masses"*. The QR code route has also failed to garner much excitement as lenders believe that if they are made to go to a potential lendee's house anyway, they'd much rather see a PAN card or driver's license for the purpose of KYC. Simply put, if these are the only two alternatives to eKYC, one interviewee succinctly stated, *"the economics of lending don't make sense for the small loan segment anymore"*.

3. **Overall positive response to the letter, but not necessarily the spirit of the Personal Data Protection Bill:** Most FinTech firms seem unperturbed by the standards on collection, processing, consent, and sharing introduced by the different versions of the data protection bills. One interviewee, in particular, welcomed the Bill as the *"right direction for India to move in, because the way data is handled in India today is shocking"*. He also stated that the requirements under the Bill, as far as they require specificity and security, should ideally be routine hygiene for FinTech companies. He added that another positive aspect of the bill is that it does away with 'fly-by-night operators' who collect vast quantities of data for no clear purpose. Another interviewee welcomed the fact that the bill signals the *"ecosystem is evolving to bring clarity into what can/can't happen"*. A fourth interviewee was agnostic to what the bill entails as the bill would apply to all FinTech companies equally, with no significant repercussions for competitiveness within the sector.

On the question of how requirements of consent, data minimization, purpose limitation, and collection limitation affect the sector, 5 out of 6 interviewees believed that it would change how they conducted their business. Most interviewees (save one) explained that there is explicit consent secured at the time of onboarding. One interviewee even told us that at the time of onboarding a new customer, there are approximately 40 consent forms that must be signed for the purposes of receiving credit, effectively covering all bases on what data would be collected and processed. Another interviewee clarified that customers are free to revoke consent with ease at any given time. It is clear that these companies are focused on *explicit*consent, however, the understanding of what constitutes *informed consent*leaves much to be desired. This tension was succinctly captured by one interviewee who asked me, *"How is this new requirement of explicit consent different from a simple tick box?"*.

4. **Significantly diverging views on what constitutes alternative data:** Three of six interviewees expressed scepticism about the extent to which alternative data is used in the sector today, while two other interviewees' business model is predicated on it. However, it also appears that the definition of alternative data as understood in the industry is changing quite rapidly. One interviewee said, *"As we move away from manual underwriting, nothing is really alternative anymore. In a sense, we are using traditional data in non-traditional ways: we assess loan applications in alternative ways when you compare us to traditional financial institutions. In order to do this, we look at signals from your life and your business as a means to understand your ability and intent to pay."* This was echoed by another interviewee, who stated that *"much of what is thought of as alternative data is really mainstream data"*, and he further added, *"When people talk about alt data, they often mean traditional data through alternative means"* while referring to the use of SMS data to understand financial transactions. These interviewees look at SMS data as a proxy to official bank statements for those individuals who aren't embedded in the formal banking system. This sentiment is in sharp contrast to responses from other interviewees who use alternative data and view it as a central factor in their business model for the purpose of underwriting and lending.

5. **Significantly diverging views on the potential value of alternative data**: As mentioned above, two interviewees view alternative data as their bread and butter. The role that alternative data plays, according to one interviewee, is enabling the building of accurate prediction-based risk models and other decision engines that can inform complex decisions. Another interviewee explained that alternative data plays a crucial role in his business as the market that the company hopes to serve includes those who are not embedded in formal financial systems. On the other hand, other interviewees held a very different view - that *"social media data was a hype a few years ago, but there has been no value found from using it thus far.."* Additionally, Facebook's

move to cut off access to social media data[77] means that this is also logistically difficult to do at this time. The same interviewee added, *"The thesis for using many data points was that this could be used to include the large unbanked population of our country. But people are finding very little correlation between social media data and credit behavior. There is hard to prove incremental value, if any, of using alternatives."*Two of the six interviewees also expressed caution against the use of alternative data because they believe that losing access to alternative data is only a matter of time.

6. **Restriction on Android apps on data scraping changes very little for lenders:** At the time of Google's decision to limit third-party apps' access to user data, there was a flurry around its significant impact on lender's ability to carry out business. Less than six months after that announcement, interviewees are not worried about this shift, since Google continues to allow scraping "relevant" data for lending. One interview remarked, *"Currently, you need to justify why you need certain permissions - in this way self-regulation is making sure that data is used by the right parties in the right manner - this is both progressive and positive"*. The deficiencies of this case-by-case assessment, however, don't fix the wider issue of problematic business models that have implications for privacy. As another interviewee stated, *"This doesn't have much of an effect on how privacy is violated because some FinTech companies require contact details to call your friends and relatives at the time of collection if you are a defaulter - that will still be allowed under the justification model."* Another glaring shortcoming of this justification model was brought up by an interviewee who said, *"If you can continue using alternate methods to access traditional information… this leaves the question of other sensitive information like income tax messages being read by FinTech apps"*.

7. **Paradox of machine learning** - At the time of commencing interviews, we took the use of machine learning to be a given in this sector, but interviews indicated otherwise. One interviewee expressed scepticism around the actual use of machine learning systems in the FinTech sector in India, stating, *"From my conversation with many leaders in this space, my understanding is that there are very few use cases where ML is being used. Basic data modeling has always happened*

[77] Johnny Lieu, 'Facebook Cuts Off Access to User Data for 'Hundreds of Thousands' of Apps' (*Mashable India*, 31 July 2018) <https://mashable.com/article/facebook-user-data-apps/> accessed 23 April 2023.

> *- but no one seems to be using alternative data points to underwrite consumers. This is far from being the norm."* At the same time, another interviewee explained how machine learning is a central consideration in his company's business model, and shared the three main challenges that the company faces while implementing machine learning systems. The first is that feedback cycles for machine learning models are somewhere between 9 - 12 months, which means that it takes a long time to build good credit-scoring models. Second, building models require large amounts of data, and FinTech companies in India can't build deep learning models as there isn't access to the kind of volume required for it. Finally, he mentioned that ML research and talent is funded by big tech companies that focus on certain types of problems, as a result of which *"there hasn't been an improvement in algorithms catering to the need of Indian problems and Indian consumers. There is no funding for home grown tech that takes Indian problems seriously."*

X. Conclusion

Through this report, we have attempted to examine the current state of FinTech lending companies in India, in the context of developments in law and policy since 2018. By offering an explanation of how Aadhaar authentication and machine learning are relevant to the sector, explaining legal developments in the context of these technologies, and informing these findings through industry interviews, we hope to have bridged the gap between legal analysis and practitioner insights.

The credit scoring industry in India needs a careful examination of rights, inclusion, appropriate safeguards and discrimination through current services. Currently, there is a lack of non-discrimination regulations that apply to the industry to safeguard against unintentional disparate impact of data-driven decision-making. There are no laws which prevent firms from collecting data on religion, caste and other sensitive attributes, which can be used toward disparate treatment. Even in other jurisdictions, there is a call for Fintech firms to be exempt from equal credit opportunity and fair credit regulations. However, regulations which prevent discriminatory practices are essential for any financial products introduced in the market.

People who lack the education, information, and other economic, cultural, and social capital that would allow them to take advantage of—and shield themselves against—the free market are most vulnerable and need greater protection. The consequences of bad decisions are far more dire for those disadvantaged and lacking the resources—financial, psychological, social, and political—to compensate for their errors. A review of big data-enabled loan products by the National Consumer Law Centre in the US showed that they were very poor payday loan alternatives. Most of these products involved annual percentage rates three times higher than considered non-predatory. Most importantly, most products require electronic access to the applicant's bank account or some other arrangement of automatically deducting the owed amount from the borrower's account.[78]

As big data scoring uses closed and proprietary algorithm-based technologies, it is impossible to analyze them for potential discriminatory impact. There are no regulations that may be used to address discrimination on the basis of the disparate impacts of data-driven decision-making in India. The promise of Fintech lending business models to empower the unbanked and reduce timelines for approvals needs closer scrutiny. The focus of financial regulation has been on reducing financial fraud, but due to the absence of a data protection law, and non-discrimination regulations, the spillover privacy and predatory effects that are magnified by the use of machine learning algorithms are largely unregulated.

[78] Persis Yu, Jillian Mclaughlin, and Marina Levy, 'Big Data: A Big Disappointment for Scoring Consumer Credit Risk' (*National Consumer Law Centre*, 14 March 2014) <http://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf> accessed 23 April 2023.

The Present and Future of AI Usage in the Banking and Financial Decision-Making Processes within the Developing Indian Economy

Dr. Shouvik Kumar Guha, Bash Savage-Mansaray and Dr. Navajyoti Samanta[*]

Abstract *In course of this paper, the authors have soght to examine the extent to which technology based on artificial intelligence (AI) have made inroads into the banking and financial sectors of a developing economy like India. The paper begins with providing a contextual background to the adoption of such technology in the global financial arena. It then proceeds to identify and categorise the forms of AI currently being used in the Indian financial sector and also considers the different channels of operation where such technology is in vogue. The advantages of using such technology and the future goals for integrating the same in the concerned sector have also been discussed. The paper then proceeds to refer to the various regulatory norms already or potentially applicable to the areas where the technology is currently being used to explore solutions. Finally, it concludes with a series of concerns voiced in regard to the adaptability and sustainability of such technology within the financial sector of a developing Indian economy, and also recommendations for the road ahead.*

[*] Dr. Guha is an Associate Professor at The West Bengal National University of Juridical Sciences. Mr Savage-Mansaray is a Ph.D. Researcher, University of Warwick. Dr. Samanta is an Associate Professor at Leicester University.

I. Introduction

The introduction of newdigital technologies particularly Artificial Intelligence (AI) into financial services has transformed different sphere of financial decision-making processes, and perhaps, is on the cusp of replacing the more conventional forms of human-centred decision making to a computer-based financial service.[1]Arguably, AI programmes are said to have surpassed human performances in certain tasks such as, computational and predictive financial modelling.[2]In the financial service eco-system, AI decision-making process is now pivotal for a myriad of reasons, yet it constitutes considerable challenges to global financial institutions and regulatory frameworks- not least because of the difficulties around data and privacy, and financial fraud and cybersecurity.

Challenges like data management and cybersecurity are especially acute for developing economics, who are waking up to the reality of integrating AI technology into their financial systems,[3] and governments will now have to create policies and regulations to keep up with AI technology. Similarly, building regulatory frameworks would require legislators and policymakers in developing countries to work with industry leaders and technology experts to understand and manage the risks presented by the AI in a digital age.[4]With AI policy deliberation still looming in India and other developing countries, this paper for the first time seeks a cross-jurisdiction and cross-sectors discussion on the issues of AI in financial decision-making in the Indian context.

This paper therefore argues that notwithstanding the potential risks, that the AI technology might pose to the financial industry, its emergence would have a profound effect in financial decision-making process and India should take a proactive regulatory stance in integrating AI technology into the financial systems.

The paper first conceptually defines the role of AI in the financial services in the global context to analyse how it has enmeshed itself in the wider financial sector, then it explores the contours of the adoption of AI in the Indian financial and banking sectors, followed by an analysis of the contemporary

[1] R.M. Lacasse et al., 'A Digital Tsunami: FinTech and Crowdfunding', (2016) ISCDI, available at <http://fintechlab.ca/wp-content/uploads/2016/11/Digital-Tsunami-Site-Web.pdf> accessed March 31, 2020.

[2] K. Grace, et al., 'When will AI Exceed Human Performance? Evidence from AI Experts', arXiv, May 3, 2018 <https:// arxiv.org/pdf/1705.08807.pdf> accessed March 31, 2020.

[3] Jon Truby et al., 'Banking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector', 14(2) Law and Financial Markets Review 110 (2020).

[4] *Ibid.*

regulation in the area in India. The paper finally concludes with recommendations on adapting the regulations in the area.

II. Conceptual Definition and Backdrop in the Global Context

Within the financial services sphere, AI is amongst sophisticated new technology that is capable of processing large quantity of data faster and more efficiently than even seen before- thereby supplementing humans who had previously had autonomy over data processing.[5] Globally, financial institutions like banks and investment firms are using AI in a plethora of areas- like to help make lending decisions and to test the credit worthiness of potential borrowers,[6] future market position[7] and online security trading.[8] In Financial Technology for instance, start-up FinTech companies are using AI to leverage advances made by technology for a competitive edge.[9] However, currently, it appears as though the discussion around AI, policy and law is largely framed within a Western context,[10] and the emerging standards may not be useful or adequate for developing economies like India. In India for instance, the regulators are unsure about foundational aspects like data protection, anti-competitive practices, consumer rights etc.[11] There is a propensity to act with fiat in a reactive manner rather than focusing on evidence based proactive policies. This part of the paper briefly highlights the major initiatives to set up a policy to regulate usage of AI especially in the consumer financial-banking context.

Whilst Western jurisdictions have somewhat leaped forward in terms of creating a framework to harness AI technology by putting the necessary safeguards within their financial systems to protect individual freedoms, it remains in the policy phase with practical and philosophical questions

[5] Malali and Gopalakrishnan, Application of Artificial Intelligence and its Powered Technologies in the Indian Banking and Financial Industry: An Overview, 25 (4) IOSR Journal of Humanities and Social Science 55 (2020).

[6] Raghav Bharadwaj, 'AI for Cybersecurity in Finance – Current Applications', Emerj (2019), available at <https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/> accessed March 31, 2020.

[7] *Ibid.*

[8] Narcisa Roxana Mosteanu, Artificial Intelligence and Cyber Security– Face to Face with Cyber Attack– A Maltese Case of Risk Management Approach, 9(2) Ecoforum Journal 4 (2020).

[9] Malali and Gopalakrishnan, (n 5).

[10] Vidushi Marda, 'Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-driven Decision-Making', 376 (2133) Philosophical Transactions of the Royal Society (2018), <https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0087>.

[11] *Ibid.*

which still to be addressed.[12] Organisation for Economic Co-operation and Development (OECD) have published proposed principles that could be applied to AI regulatory framework for its members.[13] Similarly, in the US, in 2019, President Trump signed an Executive Order that required National Institute of Standards and Technology (NIST) to create standards for the AI focusing on security, interoperability, reliability etc.[14] In addition, the European Commission High-Level Expert Group for AI (AI HLEG) also produced its own guidelines to inform the European Union (EU) legal framework on AI matters.[15]

The EU have perhaps gone further than any other jurisdiction to inculcate AI governance into financial service system through the introduction of Article 22 of the General Data Protection Regulation (GDPR).[16] In so doing, the EU has not only created the parameters for "Automated individual decision-making"[17] through the use of AI technology, but it has also created the safeguards needed to protect basic freedoms and interests as AI continues to evolve and innovate financial industries. Section (1) Article 22 allows citizens the right to not be subjected to decisions made solely on the basis of automated processing and profiling of data, although section (2) allows certain exceptions.[18]

A quick review of the global regulatory approach shows that the majority of the rules revolve around data protection, consumer confidence, reliability and interoperability. While the US, OECD and EU have taken a lead in these aspects, there is still someway before a global standard or consensus may appear in this area.

[12] Jon Truby, (n 3).

[13] 'Ratification of the Convention of OECD' <https://www.oecd.org/about/document/ratification-oecd-convention.htm> accessed 31 March 2022

[14] Jon Truby, (n 3). See also <https://trumpwhitehouse.archives.gov/ai/executive-order-ai/>; Johannes Ehrentraud, Denise Garcia Ocampo, Lorena Garzoni, and Mateo Piccolo 'Policy Responses to Fintech: a Cross-Country Overview' <https://www.bis.org/fsi/publ/insights23.pdf> accessed 31 March 2023.

[15] European Commission, 'Artificial Intelligence: Commission Takes Forward its Work on Ethics Guideline', available at <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1893> accessed March 31, 2022.

[16] 'Art 22 of the General Data Protection Regulation', available at <https://gdpr-info.eu/art-22-gdpr/> accessed March 31, 2022.

[17] *Ibid.*

[18] *Ibid.*

III. Potential Use of AI in the Indian Financial and Banking Sectors

Any analysis of the use of AI in decision-making in the financial and banking sectors of a country like India ought to be conducted in the context of certain recent developments over the past few years. Such developments include government policies like demonetisation and schemes like the DigiDhan Mission.[19] Some of these schemes recognise the need for financial inclusion and seeks to bring it about through a fillip in digital payments and banking in India.[20] Being a middle income economy, India does display some limitations like restricted network infrastructure, lack of sufficient point of sales machine and the difficulties faced by a large section of the population in adapting to the technological changes brought about by the multitude of apps and platforms involved in e-commerce, financial transactions and retail banking in particular.[21] Yet the volume of digital financial transactions have witnessed a steady rise over recent years, leading to a sizable amount of data created by such transactions[22] –such data may in turn be mined and processed in order to keep a close watch on consumer behaviour, predict future behaviour and customise responses to the same, and also chart new ways of including consumers hitherto excluded from the ambit of digital banking and finance. In addition, the proliferation of mobile technology across the country, reduced cost of Internet connectivity, breakthroughs in terms of computational power and storage of data, greater reliability on energy, and advanced analytical techniques are some of the factors to have also encouraged the growth of FinTech, as well as regulators' openness to enter into partnerships with developers of technology so as to better serve the regulatory cause.[23] In this section of the paper we shall mainly focus on discussing the potential utilities of using AI in the Indian banking and financial sector. This would allow us to critically analyse the failure of adopting appropriate regulations in the Indian context.

[19] Digital Economy & Digital Payment Division, DigiDhan Mission Logo has been unveiled by Hon'ble Minister Electronics & IT on 5th December 21, available at <https://www.meity.gov.in/digidhan> accessed on March 2, 2022.

[20] Kamalika Ghosh, 'Demonetisation Catalysed Digital Payments, but Nobody Knows its Impact on Black Money, available at <https://www.outlookindia.com/website/story/business-news-demonetisation-led-to-increased-digital-adoption-that-helped-in-dealing-with-covid-19-but-still-no-data-on-black-mon/400179> accessed on March 3, 2022.

[21] Rajat Kathuria et al., 'Implications of AI on the Indian Economy, 2020', available at <http://icrier.org/pdf/Implications_of_AI_on_the_Indian_Economy.pdf> accessed on March 2, 2022.

[22] JermyPrenio and Jeffery Yong, 'Humans Keeping AI in Check – Emerging Regulatory Expectations in the Financial Sector', 2021, available at <https://www.bis.org/fsi/publ/insights35.htm> accessed on March 3, 2022.

[23] Vidushi Marda, (n 10).

One of the forms of technology that are currently being deployed in the banking and financial sector in India in a slow yet steady manner is that of a combination of blockchain and AI –such deployment is in vogue both in the domain of direct consumer service as well as back-office activities, all the more so since instances of successful proof of concept exercises have revealed the competitive advantage that such technologies may bring to a market player.[24] This trend is significant even from the perspective of financial inclusion, because when one considers the major reasons why a large chunk of the population of a developing nation are traditionally underserved by the banking and finance sector[25], viz. lack of formal identification, ascertainable credit history and acceptable collateral, it may be possible to find alternatives to at least the first two by using AI to get relevant information about such potential customers based on their regular interfaces with data in course of their daily lives.

Some of the AI-based technology that are already in vogue in the banking and finance sector outside India include natural language generation (NLG) and processing (NLP), computer vision (CV), and machine learning (ML) and deep learning (DL) via the use of neural networks (NN).[26] If one carefully considers the different domains within the aforesaid sector where such technology is being used, one may be able to broadly categorise those into two different sub-domains, viz. *operations that are related to finance* and *operations that are related to business and management.*

In the first category, we have examples of algorithms being utilised for collecting information about individuals based on mobile usage, banking transactions, family history and other relevant factors, so as to build credit and risk profiles and scores for them, which in turn facilitate and expedite lending decisions.[27] At the same time, data about spending and transactional habits of such individuals obtained in similar manner can also help the companies and regulators to identify potential fraud and malpractice in terms of banking transactions as well as trading in secondary markets.[28] AI can also be used to track spread of financial rumours which create false market

[24] Saman Goudarzi et al., 'AI in Banking and Finance, Report by the Centre for Internet and Society', 2018, available at <https://cis-india.org/internet-governance/files/ai-in-banking-and-finance> accessed on March 2, 2022.

[25] *Ibid.*

[26] Deloitte, 'The New Physics of Financial Services: How Artificial Intelligence is Transforming the Financial Ecosystem', available at <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-ai-wef-summary.pdf> accessed on March 2, 2022.

[27] Saman Goudarzi, n 24.

[28] *Ibid.*

and identify those who indulge in such practices.[29] Predictions based on ML models are also contributing to providing customised portfolio management advice including insight into possible price fluctuations to high-end clients, as well as efficient financial plans for even lower-end clients by analysing their income, expenditure and saving data and financial goals.[30] On the security front too, AI-based voice-identifier technology is being integrated into various banking and finance applications, thus reducing the onerous nature of multi-step verifications without compromising with the security of the system.[31] In general, algorithmic trading has also been thriving in the capital market, with AI models having displayed high accuracy in dealing with complex data sets and smooth automation.[32]

Within the second category, there exist sub-categories of operations that are witnessing adaptation of AI-based technology at present. A case in point is the increasing use of chatbots or virtual assistants by banking and financial websites and applications to provide a range of responses to customer queries, using modes such as text, video or speech.[33] Coupled with this is the practice of cognitive analysis of customer needs and wants by tapping into customer data streams on digital platforms and mapping behavioural patterns and transactional history[34] –this in turn is being used to curate customised products and advance assistance for said customers in order to gain a competitive edge over business rivals. On a macro level, such technology also offers more efficient inter-departmental coordination within these banking and finance companies and innovative strategies in product development and marketing by leveraging aforementioned analysis of consumer data, especially in the digital payment platforms and FinTech operations.[35] In addition, a host of back-end operations of these companies have now been streamlined with the usage of AI-based technology such as NLP to mine and

[29] Financial Stability Board, 'Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications', 2017, available at <https://www.fsb.org/wp-content/uploads/P011117.pdf> accessed on March 3, 2022.

[30] *Ibid.*

[31] Jermy Prenio and Jeffery Yong, 'Humans Keeping AI in Check – Emerging Regulatory Expectations in the Financial Sector', 2021, available at <https://www.bis.org/fsi/publ/insights35.htm> accessed on March 3, 2022.

[32] *Ibid.*

[33] Organisation for Economic Cooperation and Development, 'AI in Finance', available at <https://www.oecd-ilibrary.org/sites/39b6299a-en/index.html?itemId=/content/component/39b6299a-en> accessed on March 2, 2022.

[34] *Ibid.*

[35] Organisation for Economic Cooperation and Development, 'Trends and Policy Frameworks for AI in Finance', available at <https://www.oecd-ilibrary.org/sites/cbc9d1af-en/index.html?itemId=/content/component/cbc9d1af-en> accessed on March 2, 2022.

extract relevant information from documents, automated writing of reports, setting up workload management software and dashboards and so on.[36]

The wide range of use of AI technology in the banking sector has been made possible by helping the banks realise the significant value addition arising out of such use. Not only does the superior customer experience provided by such automation and customised curation help the service provider gain more customers, but the lifetime value of each customer also gets increased in the process with the provider being able to connect with each customer vide a wider range of products and services catering to the latter's needs and wants.[37] At the same time, the automation of document-processing and diligence, as well as lowering of credit risks via better screening of loan applications have also led to the banks being able to reduce their operating costs significantly, even after the adaptation costs for the new technology.[38]

In relation to what the future holds for such adaptation in India, a range of suggestions and recommendations have been forthcoming from several domain experts. These include[39] *inter alia*

(i) acquiring customers by processes such as hyper-personalised offers, customer retargeting, propensity-to-buy scoring, channel mapping;

(ii) taking credit-related decisions by ascertaining credit qualifiers, assessing limits, optimising pricing structure of products and services, and preventing fraudulent activities;

(iii) monitoring and supervising by looking out for early-warning signals, ascertaining default probability and then taking self-corrective measures, segmenting customer base via value at risk methodology and mapping customer-agent relationships;

(iv) strengthening relationships with existing customers via intelligent offers, reducing churning and applying fatigue rule engines; and

[36] *Ibid.*

[37] Financial Stability Board, 'Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications', 2017, available at <https://www.fsb.org/wp-content/uploads/P011117.pdf> accessed on March 3, 2022.

[38] Deloitte, 'The New Physics of Financial Services: How Artificial Intelligence is Transforming the Financial Ecosystem', available at <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-ai-wef-summary.pdf> accessed on March 2, 2022.

[39] Akshat Agarwal et al., 'AI-powered Decision Making for the Bank of the Future', 2021, available at <https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/ai%20powered%20decision%20making%20for%20the%20bank%20of%20the%20future/ai-powered-decision-making-for-the-bank-of-the-future.pdf> accessed on March 2, 2022.

(v) facilitating smart services to customers by providing real-time recommendations, dynamic customer routing, reviewing and training agents via AI and so on.

IV. Legal and Regulatory Concerns

With the exponentially increasing scope of usage of AI in the financial and banking sectors, it is rather obvious that regulation of such technology is more often than not left behind, always trying to catch up to technological disruptions. It is a well-known fact India as a developing nation is yet to have any overarching policy or regulatory regime catering to AI use. One may of course argue that this presents as much of an opportunity as a cause for concern –it may be possible for modifying and adapting at least some of the existing regulations in the banking and finance sectors to render those applicable *mutatis mutandis* to AI-based technology. The two major sectoral regulators who would be required to take the lead in this are the Reserve Bank of India (RBI), the central bank and monetary authority in India, and the Securities and Exchange Board of India (SEBI), the regulator of the Indian capital market.

RBI has traditionally been responsible for regulating the activities of all the scheduled and commercial banks, as well as cooperative banks and regional rural banks. However, the ambit of its jurisdiction is currently being subjected to further growth with non-banking financial companies (NBFCs) offering a wide range of alternative payment services all over the country, including those involving e-commerce, digi-finance and online intermediaries that are gaining considerable popularity in the country. An indication of such widening ambit can be observed in the RBI's efforts to come up with licensing norms for such small and payment banks offering a specific range of services.[40] The major legislations that are applicable in this regard are the Reserve Bank of India Act, 1934 and the Banking Regulation Act, 1949[41], as well as a host of regulations framed by the RBI[42] under these umbrella leg-

[40] Reserve Bank of India, 'Guidelines for Licensing of Payments Banks', available at <https://rbi.org.in/scripts/bs_viewcontent.aspx?Id=2900> accessed March 2, 2022.

[41] Provisions of this Act require and/or enable various banks to identify customers, verify their identity and create customer profiles based on the category of risks that they represent. Such customer data is however, confidential in nature and the banks are not supposed to divulge the same. The Master Direction - Know Your Customer Direction, 2016, issued by the RBI provides for the process of collecting and preserving such data. However, with AI-based models of collecting traditional and non-traditional customer data including personal information and behavioral data, these norms may need to be changed.

[42] Examples include the RBI Master Directions on Access Criteria for Payment Systems, 2021, RBI Master Direction on Issuance and Operation of Prepaid Payment Instruments,

islations along with periodic notifications for governing the functioning of such banks and related financial institutions. RBI has also set up 'regulatory sandboxes' to test fintech products in a controlled setting,[43] however, no such steps have been taken on the aspects of AI.

SEBI, on the other hand, is entrusted with regulating the activities taking place in the primary and secondary markets, including intermediaries operating therein and also mutual and investment funds. The Insurance Regulatory and Development Authority (IRDA) is also another sector regulator that frames the regulations for the insurance sector and also acts as the registering authority for all private sector players in the sector –given the proliferation of AI use in the concerned sector by players both private and public, it is therefore important to consider the regulatory framework created by the IRDA too as applicable to such use.[44]

Despite having no dearth of regulatory supervision in the banking and financial sectors therefore, the main concern when it comes to the use of AI-based technology in those sectors is that the regulators have for the most part been accustomed to exercising oversight over traditional operations in those sectors. The disruptive nature of AI is likely to change many of the accepted norms and practices if it is not already doing so, and the onus lies on the regulators to revise their perspectives so as to ensure that their capability matches the new challenges and concerns bound to result from such change. A case in point is the lack of clarity surrounding the precise regulatory jurisdiction that the FinTech companies may fall within, given the multitude of services offered by them that often cut across regulatory borders.[45]

One of the biggest causes for concern with the proliferation of AI in these sectors is the impact on privacy of the parties involved, individual consumers and institutions alike. It is a well-established point that AI models are capable of using traditional as well as non-traditional data in order to create profiles of individuals based on their location, social and financial behaviour,

2020, RBI Master Directions on Prepaid Payment Instruments, 2021, RBI Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks, 2021, RBI Guidelines on Digital Lending, 2022 and many others.

[43] Avimukt Dar, 'RBI's "sandbox" Tests for Fraud-Proof Fintech' *The Hindu Business line* (12 March 2023) <https://www.thehindubusinessline.com/business-laws/rbis-sandbox-tests-for-fraud-proof-fintech/article66608800.ece> accessed 23 March 2023

[44] Department of Economic Affairs, Government of India, Report of the Steering Committee on Fintech Related Issues, 2019, available at <https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech_1.pd> accessed on March 2, 2022.

[45] Margarete Biallas and Felicity O'Neill, 'Artificial Intelligence Innovationin Financial Services', EM Compass 85, International Finance Corporation (2020).

transaction data and so on; the question arises as to whether while doing so, the established principles of privacy[46] such as consent, due notice, limitation of collection and purpose, adequate disclosure etc. are being adhered to. In this relation, there are several legislative provisions that may need to be revisited or repurposed so as to ensure adequate safeguards and governance of AI used in the financial decision-making process, especially given that India as a developing country is yet to come up with any dedicated privacy or data protection regime, instead relying so far on jurisprudence developed from individual case-laws. India is trying out its first foray through the Digital Personal Data Protection Bill, 2022.[47] However, it already suffers from several deficiencies like asymmetric bargaining power in consent, ill-defined powers to the new regulator (the Data Protection Board of India), no specific mention of permitted usage (especially in a sandbox situation). This bill also subsumes s43A of the Information Technology Act, 2000.

Amongst the existing regulations, we would need to focus on the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. In particular, Section 43A of the Act lays down an obligation on companies collecting data to adopt a slew of security measures with regard to such data. However, the definition of 'financial data' and the specific usage restrictions would undoubtedly have to be re-examined once AI models are used for collecting and analysing such data and making predictions based on the same. The aforementioned principles of privacy need to be statutorily reflected in these provisions, and new concepts such as automated data collection and anonymisation need to be specifically addressed. Specialist committees such as the Srikrishna Committee set up by the Ministry of Electronics and Information Technology[48], as well as the RBI Working Group on FinTech and Digital Banking,[49] have already recommended dedicated data protection and privacy regulations in the light of the technological advancements in general and AI use in particular in this domain.

[46] *Ibid.*

[47] Digital Data Protection Bill, 2022 <https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf> accessed 23 March 2023

[48] 'White Paper of the Committee of Experts on a Data Protection Framework for India', 2017, available at, <https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed March 4, 2022.

[49] Report of the Working Group on FinTech and Digital Banking, 2017, available at <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF> accessed Mach 4, 2022.

In addition, we have the Credit Information Companies (Regulations) Act, 2005 and the associated 2006 Regulations, which require credit decisions to be transparent and reasonable and also lays down certain protocols to be followed for collection of credit information; in the light of the use of AI models to collect and analyse such information, the relevant provisions may need to be changed so as to ensure a more contemporary definition of credit information and that the rights of the credit applicants include the right to get such automated decisions reviewed by human beings.[50]

The Payment and Settlement Systems Act, 2007, the associated 2008 Regulations, and related instruments such as the RBI's Policy Guidelines on the Issuance and Operations of Prepaid Payment Instruments in India collectively form one of the most significant frameworks in this context, because they may apply to the FinTech companies and the latter's modes of operation in consonance with AI-adaptation even now; this is because the said Act and Regulations encompass all payment-related activities within the country regardless of the identity of the players involved or the medium in which they operate.[51] While the 2007 Act and 2008 Regulations entrust the RBI with regulatory supervision and standard-setting for such activities, and also require the players to comply with the aforesaid Policy Guidelines, they are yet to be amended so as to reflect dedicated provisions towards AI usage in financial decision-making, an oversight that needs to be remedied at the earliest under the present circumstances.[52] The Guidelines may eventually be superseded by the RBI's Master Directions on Issuance and Operation of Prepaid Payment Instruments in India, 2021 –an examination of this instrument will reveal that the regulator is more keen addressing security concerns, upgradation of information security infrastructure, regular review, monitoring and audit by the RBI,risk management and adequate grievance redressal of customers, especially in the light of greater technology integration including AI-based processing in the PPIs.[53]

Another piece of legislation that is likely to gain traction when it comes to using AI in the capital market via algorithmic trading and robo-advisors is the Securities and Exchange Board (Investment Advisers) Regulations, 2013 –while at this stage the Regulations do not yet create any template for dealing with such use, the Consultation Paper on Amendments/Clarifications

[50] Saman Goudarzi, (n 24).

[51] *Ibid*.

[52] *Ibid*.

[53] Ashima Obhan and Nishtha Jaisingh, 'India: The RBI's New Master Direction on Prepaid Payment Instruments', available at <https://www.mondaq.com/india/financial-services/1111936/the-rbi39s-new-master-direction-on-prepaid-payment-instruments> accessed March 4, 2022.

to the SEBI (Investment Advisers) Regulations, 2013,[54] as released by SEBI, provides a series of recommendations *inter alia* assigning liability on investment advisors for using robo-advisors and requiring such usage to be in consonance with the fiduciary duties owed by the former to their clients in line with the 2013 Regulations. The paper offers an interesting stance by treating the robo-advisors as mere tools to be wielded by human advisors, and carves out a liability regime based on that stance, besides trying the safeguard the interests of retail investors trying to participate in a market not only characterised by hitherto unknown processes like automated trading and asset management, but also prone to associated dangers like flash crashes.

Apart from these, if issues pertaining to liability related to products and services offered in the financial markets arise, one may also consider seeking recourse to the Consumer Protection Act, 2019 and accordingly modify provisions within that Act to meet such needs. If the entity creating an AI-based product and the entity using such product to offer financial services to customers are different ones, then such matters may add additional layers of complexity when challenged under the consumer rights jurisprudence. As of now, the FinTech companies appear to be saddled with the liability arising out of any decision-making on their end regardless of the significance of the role that AI may play in such decision, yet as the nature of the AI used evolves from its narrower version to a more general form capable of functioning independent of human supervision, affixation of such liability solely on the user company may become more difficult. Further research and consultation is required in order to appropriately apportion liability in such cases of mistakes by the AI. The liability should not be too high as it would unnecessarily hamper companies from using AI and consumers from benefitting from it, however it should not be too low, such that the AI produces too many errors and become less useful.

Finally, while the use of AI can give rise to legal concerns for the financial sectoral players, AI may also provide a wide range of solutions to those very players when it comes to ensuring adherence to compliance, vide what is now being popularly referred to as 'RegTech', which is nothing in essence but an array of technology-based solutions to facilitate regulatory compliance, timely reporting, adequate monitoring, risk control and dynamic predictions,

[54] Securities and Exchange Board of India, Consultation Paper on Amendments/Clarifications to the SEBI (Investment Advisers) Regulations, 2013, available at <https://www.sebi.gov.in/reports-and-statistics/reports/oct-2016/consultation-paper-on-amendments-clarifications-to-the-sebi-investment-advisers-regulations-2013_33435.html> accessed March 4, 2022.

leveraging AI models, Big Data and breakthroughs in cybersecurity.[55] Other than fraud detection and malpractice prevention uses, RegTech is also capable of providing sustainable means of navigating the ever-growing labyrinth of regulatory compliances to the banks and other participants in the financial market.

On an international level, there appear to exist consensus-building exercises such as the ones carried out by the Oragnisation for Economic Cooperation and Development (OECD) and the Artificial Intelligence High-Level Expert Group established by the European Commission –the purpose of these exercises is to produce a set of principles acceptable to governments across the world for regulating AI usage in multiple sectors, of which financial sector is definitely meant to be one.[56] In India we must first ensure individual data protection through more public consultation of the Digital Personal Data Protection Bill, 2022. Only when we have created a safe environment for personal data can we hope to achieve accurate AI construction which would need to be fed with a 'starter' data. Ensuring human oversight of automated processes on a macro level, developing robust and safe frameworks committed to the ideals of fairness, non-discrimination, diversity, transparency and accountability, advocating privacy and data governance and working towards the goals of societal and environmental well-being are some of the more prominent principles[57] emerging from such exercises –yet one must remember that the extent of adaptability of these principles in the domestic AI regulations would doubtless depend to a considerable degree on the socio-economic realities of the concerned jurisdiction, as well as the ground realities singular to such jurisdiction.

V. Conclusion

It is clear from the discussion above that there exists a need to draft new legal provisions, or restructure existing one to address more effectively the concerns that may arise out of AI usage in the financial market. At the same time, one should not lose sight of the fact that even *prima facie* legal use of AI to any significant extent in the financial decision-making system may further exacerbate the flaws of the already highly subjective and occasionally discriminatory and/or biased processes that are in vogue especially in the

[55] Jermy Prenio and Jeffery Yong, 'Humans Keeping AI in Check – Emerging Regulatory Expectations in the Financial Sector', 2021, available at <https://www.bis.org/fsi/publ/insights35.htm> accessed on March 3, 2022.

[56] Jon Truby, (n 3).

[57] *Ibid.*

banks and credit decision-making companies. The large data sets used by AI to train itself via ML and DL stand the risk of being monetised without the data subjects being any the wiser.

One of the major concerns for AI integration in any market, including the financial market in a developing country like India, include lack of access to accurate, affordable and objective training data. While some of the major players may have the resources to obtain such data, many of the start-up FinTech companies may be lacking in it and despite that, the products and services offered by them to a sizable populace have considerable AI-involvement –referred to as a problem of data parity, this issue needs to be acknowledged and specifically addressed before such companies plan to scale up their operations even further in the garb of greater financial inclusion.

Another major issue is that of data privacy, while the 2022 bill on digital data privacy is a welcome step, however, it suffers from several issues which need to be resolved before it can provide any reasonable solutions. In addition to this, in a country like India where recorded instances of systemic and historical discrimination exist, chances of such discriminatory practices seeping into the collection of data and leaving so-called 'dark spots' in it that may be apparently invisible to an external observer once the data has been used by AI models to arrive at financial and credit decisions, cannot be entirely discounted either. Even assuming that the dataset that is used to train a model can be purged of such bias, the choice of design at the model level, including selecting appropriate features or according suitable weights to various attributes, may also be susceptible to discrimination. While principles like fairness are certainly laudable goals to pursue, one ought to also consider the geographically, socially and culturally appropriate definition of fairness in the context of a developing nation like India, and ensure that such definition encompasses the constitutional values and ethos including the various rights, affirmative action considerations and so on. The privacy challenges further assume significant proportion in the light of India's continuing inability to establish a formal and dedicated privacy and data protection regime.

Whether tools and methodologies used by AI models in the financial sector such as sentiment analysis and surveillance, ostensibly for the sake of credit profiling, may also have graver implications including chilling effects for freedom of expression of the data subjects, is also a point to ponder upon. There also exist specific challenges posed by the financial sector itself when it comes to AI usage -those posed by data margins, diversity in financial behaviour of the data subjects, lack of equality and accountability in data collection, usage of proxy markers for features otherwise protected against information extraction, ensuring informed consent given by data subjects, facilitating information security, accounting for granularity and scrutability in the models used, providing for grievance redressal and impact assessment, are some that deserve mention in particular.[58]

In the aftermath of the COVID-19 pandemic in particular, preceded by the event of demonetisation, the Indian economy is well on its way to assimilating digital banking, payment system and associated financial services. The banks are slowly yet steadily evolving into so-called 'AI-First' institutions in order to achieve goals like increased profits, scaled-up customisation for their various products and services to their diverse customer base, specific user experiences across channels, greater financial inclusion and quicker innovation cycles.[59]

With this development comes the possibility of rising and evolving expectations from those customers, resorting to AI-based solutions gaining more popularity as technology-based firms enter the financial space and the digital ecosystem starting to complement if not replace traditional financial operations. The competitive race to provide intelligent, personalised and omnichannel customer experiences are likely to motivate the FinTech companies and banks to automate to a high extent most existing manual tasks and to augment if not entirely replace decisions by human being with diagnostic ML and DL processes in more than one area of banking.[60] If advanced automation and ML models can be deployed at scale in both laboratory environment as well as factory conditions, and those models can be further augmented with edge capabilities to provide enhanced customer-service experiences, the entire nature of the Indian financial sector can be radically transformed in the coming years.

The government of India is not oblivious of such potential, as is evident from the setting up of the Task Force on Artificial Intelligence and the Steering Committee on FinTech Issues, as well as the formulation of the National Strategy for Artificial Intelligence by NITI Aayog, all three recommending a series of measures for capacity building, research, deployment and regulatory governance of AI.[61] Other measures such as advocating use of

[58] Vidushi Marda, (n 10).

[59] Suparna Biswas et al., 'AI-Bank of the Future: Can Banks Meet the AI Challenge?' available at <https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge> accessed on March 2, 2022.

[60] *Ibid.*

[61] Rajat Kathuria et al., 'Implications of AI on the Indian Economy', 2020, available at <http://icrier.org/pdf/Implications_of_AI_on_the_Indian_Economy.pdf> accessed on

Unified Payment Interfaces for payment and settlement services, encouraging the growth of peer-to-peer lending platforms, the use of technology-based solutions including blockchain, AI and distributed ledger techniques not only for banking, insurance, pension fund investment and capital markets, but also for account aggregator services, cross-border payments, smart contracts, trade finance, security settlements, credit rating services, digital currencies and utility and security tokens, are all instances of the overall governmental approach of facilitating the integration of AI and related technology in the Indian financial sector.[62] In this context, the government's positive stance with regard to the G20 High Level Principles for Digital Financial Inclusions deserves mention, as do the various initiatives put in place for the use of FinTech in the growing MSME sector in India to further accessibility and affordability of finance.[63]

To conclude, one will not be far off the truth in opining that there exist very tangible concerns when it comes to adopting AI-based technology in any sector in a developing country like India, the financial sector not being an exception. The core legacy systems of any existing organisation including banks need to undergo significant overhaul and procure access to quality data in order for proper integration of such processes and models, and while doing so, ensure adherence to the principles that have been proposed for better AI regulation.[64] Using RegTech and SupTech (Supervisory Technology) for compliance, risk monitoring and management, data analysis and flagging, some of the concerns can be alleviated in a sustainable manner. At the same time, the significant impact on the economy, society and labour markets of such technology integration cannot be overlooked either. Given the potential positive outcomes of adopting AI-based policy measures, such as financial inclusion, innovative solutions, customer acquisition and value addition, cost reduction, managing of risk, the economy and the players in the financial sector cannot stay away from such measures for long.[65]

While the Indian government is already taking certain policy measures and legislative initiatives to address the regulatory concerns involved, it would do well to implement the recommendations of the expert committees set up to look into such matters so far. These suggestions including *inter alia*-

(i) having a nodal agency within the existing governmental structure to cater to developing and supporting AI research and diffusion thereof,

March 2, 2022.

[62] *Ibid*.

[63] *Ibid*.

[64] Vidushi Marda, (n 10).

[65] *Ibid*.

especially in the financial sector given the broad implications of sudden disruptions within that sector,

(ii) carrying out collaborative and joint efforts involving the various stakeholders from the industry, academia and the government including cross-border collaboration and ventures,

(iii) framing a suitable data strategy and explore alternative data sharing models suitable to the needs and realities of a developing economy on the one hand and enhancing the capability of existing public institutions to process available data in a format compatible with AI-use,

(iv) delineating basic workflows and standardising document and data parameters for specific application contexts within the existing AI-research ecosystem in India and bolstering the latter with relevant skill development from grassroot level including but not limited to interdisciplinary training via the educational institutions,

(v) addressing the gaps in finance in the developing economy by resorting to options such as AI-enabled supply chain management, consolidating financial lives via multi-provider platforms and building customer-centric banking infrastructure, sponsoring microservices and cloud functions and also externalising best-in-class procedures, and

(vi) controlling the cultural and management shifts taking place within organisations that are seeking to integrate AI within back-office as well as front-office solutions.[66]

Greater focus on 'explainability', reliability, fairness, transparency of AI/ML models, susceptibility of such models to ethical and security audits at the development stage as well as during and post-use, reengineering legal processes to better suit the concerns of the digital world, setting up of regulatory sandboxes for AI products, and placing greater reliance on open data to enhance competition in the financial sector without compromising on data integrity, privacy and security, are some of the other steps that the authors would recommend in order for effective, sustainable and competitive AI-integration and use to take place in the Indian banking and financial industries in their current form.

[66] Department of Economic Affairs, Government of India, Report of the Steering Committee on Fintech Related Issues, (n 44).

Information About the Journal

The *Indian Journal of Law and Technology* (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;

OPEN ACCESS POLICY

The *Indian Journal of Law and Technology* is a completely open access academic journal.

- Archives of the journal, including the current issue are available online with full access to abstracts and articles at no cost.
- Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process. Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "ijltedit@gmail.com".

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an oiler of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification or the offer. If there is no response, then the journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
  (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.

  (2) the résumé(s)/curriculum vitae(s) of the author(s).

  (3) an abstract of not more than 200 words describing the submission.

- All submissions in electronic form should be made in the Microsoft Word file format (.doc or .docx) or in the Open Document Text file format (.odt).
- All text and citations must conform to a comprehensive and uniform system of citation. The journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

The selected authors shall grant a licence to edit and publish their submissions to the Journal but shall retain the copyright in their submissions. The aforementioned licence shall be modelled as per a standard author agreement provided by the Journal to the selected authors.

DISCLAIMER

The opinions expressed in this journal are those of the respective authors and not of the Journal or other persons associated with it.

PERMISSIONS

Please contact the Chief Editor of the Indian Journal of Law and Technology for permission to reprint material published in the Indian Journal of Law and Technology.

ORDERING COPIES

Price Subscription (inclusive of shipping) of the IJLT is as follows:

Hard Copy for 2022	Rs.
Hard Copy for 2021	Rs. 1100
Hard Copy for 2020	Rs. 900
Hard Copy for 2019	Rs. 900

Order online: www.ebcwebstore.com

Order by post: send a cheque/draft of the requisite amount in favour of ‘Eastern Book Company’ payable at Lucknow, to:

Eastern Book Company,

34, Lalbagh, Lucknow-226001, India

Tel.: +91 9935096000, +91 522 4033600 (30 lines)

[2022]