

THE ORACLE’S FORETELLING & THE CASE  
FOR AMBIGUITY: EXPLORING THE PROPHECIES  
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 prophecies 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.*

I. Context and Beginnings . . . . .	2	B. Identity, biometrics and the formation of the State-as-a- platform . . . . .	3
A. From ambiguity to specificity . .	2		

---

\* 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.

C. Chapterisation. . . . .	6	C. Financial Stability and Security with a Side of Surveillance. . . . .	10
II. Tracing the Roots of the International Financial Surveillance Economy: ‘Exceptionalism within the Governmentality of Everydayness’ . .	7	III. Aadhaar and the ‘Deserving Poor’ .	12
A. Contribution to Economic Intelligence . . . . .	7	A. Categorisation and who deserves to be poor . . . . .	12
B. Screening and Profiling. . . . .	9	B. Aadhaar and its Expanding Universe. . . . .	14
		C. Myth-making and Aadhaar . .	16
		IV. Conclusion. . . . .	19

## 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.<sup>1</sup> Cleomenes misunderstood the prophecy and in the end went insane and died of suicide.<sup>2</sup>

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

<sup>1</sup> Julia Kindt, ‘Oracular Ambiguity As a Mediation and Triple’ (2008) 34 CLASSICVM 23, 27.

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

the help of the divine, albeit through severely ambiguous prophecies.<sup>3</sup> This ambiguity played with the limits of description and perception and revealed the complexity and the variety of phenomena in the world.<sup>4</sup>

As a direct anti-thesis to the ambiguous prophetic world of Ancient Greece, in 2020, PwC published a report,<sup>5</sup> 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.<sup>6</sup>

## **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 and forecasting economic growth, and more importantly, moving rapidly towards authorising widespread surveillance.<sup>7</sup>

---

<sup>3</sup> Kindt (n 1) 26.

<sup>4</sup> *ibid.*

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

<sup>6</sup> *ibid.*

<sup>7</sup> 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.

This idea of Aadhaar has been contested by its architect, Mr Nandan Nilekani, who called it a ‘simple’ identity verification method,<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup>

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.<sup>11</sup> 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.

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

---

<sup>8</sup> ‘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.

<sup>9</sup> Ursula Rao, ‘Biometric IDs and the Remaking of the Indian (Welfare) State’ (2019) 21(1) *Economic Sociology. Perspectives and Conversations* <[https://econsoc.mpi.fg.de/38379/03\\_Rao\\_Econsoc-NL\\_21-1\\_Nov2019.pdf](https://econsoc.mpi.fg.de/38379/03_Rao_Econsoc-NL_21-1_Nov2019.pdf)> accessed 20 September 2022.

<sup>10</sup> *ibid* 11.

<sup>11</sup> *ibid*.

surveillance’ was a form of population management strategy.<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup>

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 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

---

<sup>12</sup> Kevin D Haggerty and Richard V Ericson, ‘The Surveillant Assemblage’ (2000) 51 *The British Journal of Sociology* 605, 615.

<sup>13</sup> *ibid.*

<sup>14</sup> *ibid* 616.

<sup>15</sup> *ibid* 615-616.

<sup>16</sup> 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.

<sup>17</sup> *ibid.*

associated with monitoring the financial sphere for legal and/or regulatory purposes.<sup>18</sup> 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.<sup>19</sup>

### 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.

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.

---

<sup>18</sup> 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](https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law_finance/law)> accessed 20 September 2022.

<sup>19</sup> 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](http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315)> accessed 20 September 2022.

## 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.<sup>20</sup> This is also true of the governance of finance, which is aided by digital surveillance technologies and infrastructures.<sup>21</sup> 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.<sup>22</sup> 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’.<sup>23</sup> 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.<sup>24</sup>

<sup>20</sup> Malcolm Campbell-Verduyn *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance* (Routledge 2018) 136.

<sup>21</sup> Anthony Amicelle and Gilles Favarel-Garrigues, ‘Financial Surveillance’ (2012) 5 *Journal of Cultural Economy* 105, 105.

<sup>22</sup> *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.

<sup>23</sup> *ibid*.

<sup>24</sup> 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 the rise 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.<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup>

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.<sup>28</sup>

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](http://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12027&Mode=0)> accessed 20 September 2022

<sup>25</sup> Michael J Casey, 'A Reckoning Looms for America's 50-Year Financial Surveillance System' (2021) 41 *Cato Journal* 367.

<sup>26</sup> 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.

<sup>27</sup> *ibid* 106.

<sup>28</sup> *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.<sup>29</sup> 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.<sup>30</sup> 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.<sup>31</sup>

## 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.<sup>32</sup> 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'.<sup>33</sup> 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

---

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

<sup>30</sup> 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.

<sup>31</sup> Stanley and Buckley (n 26) 111.

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

<sup>33</sup> 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](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.<sup>34</sup> 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<sup>35</sup>

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.”<sup>36</sup>

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

---

<sup>34</sup> ‘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.

<sup>35</sup> ‘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](http://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.

<sup>36</sup> *ibid* 40.

and reducing systemic risk through information exchange and international cooperation in the supervision and surveillance of financial markets.<sup>37</sup> It tends to combine various forms of bilateral and multilateral surveillance to solve multiple challenges in digital technology, climate change, inequality, demographics, and geopolitics.<sup>38</sup> 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”.<sup>39</sup> including money laundering and financing of terrorism.<sup>40</sup>

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.<sup>41</sup> 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’.<sup>42</sup>

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.<sup>43</sup> 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

---

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

<sup>38</sup> Anthony Amicelle, ‘Towards A “New” Political Anatomy of Financial Surveillance’ (2011) 42 *Security Dialogue* 161, 162.

<sup>39</sup> ‘Suspicious transactions’ is defined in clause (h) of sub-rule (1) of Rule 2 of Prevention of Money-Laundering (Maintenance of Records) Rules 2005.

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

<sup>41</sup> *ibid.*

<sup>42</sup> Amicelle ‘Towards A “New” Political Anatomy of Financial Surveillance’ (n 43) 165.

<sup>43</sup> 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.<sup>44</sup>

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.<sup>45</sup> 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.<sup>46</sup> 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).<sup>47</sup>

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.<sup>48</sup> identity to over a billion people. Over the years, it has come to be the fulcrum of several innovative

---

<sup>44</sup> *ibid* 167.

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

<sup>46</sup> *ibid*.

<sup>47</sup> *ibid*.

<sup>48</sup> ‘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.<sup>49</sup> 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.<sup>50</sup> 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.<sup>51</sup> amongst scores of gender, caste and other socio-cultural and legal barriers that people regularly face.<sup>52</sup> The focus of Aadhaar and its analysis<sup>53</sup> 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.<sup>54</sup> This is also expressed as an idea of ‘coded citizenship’, which transforms citizens into a set of data points.<sup>55</sup>

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”.

<sup>49</sup> Derryl D’Silva et al, ‘The design of digital financial infrastructure: lessons from India’ [2019] BIS Papers Series 106, 8.

<sup>50</sup> *ibid* 4.

<sup>51</sup> 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](http://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf)> accessed 7 October 2022.

<sup>52</sup> 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

<sup>53</sup> 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.

<sup>54</sup> 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.

<sup>55</sup> *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.<sup>56</sup> privacy, work, and reproductive freedom.<sup>57</sup> 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.<sup>58</sup> 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.<sup>59</sup>

---

<sup>56</sup> *ibid* 278.

<sup>57</sup> Rao (n 9) 15.

<sup>58</sup> *K.S. Puttaswamy v Union of India* (2018) 1 SCC 809.

<sup>59</sup> ‘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](http://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’,<sup>60</sup> 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.<sup>61</sup> The scheme has been widely popularised, with the RUPI, is NPCI website mentioning 16 “live banks”<sup>62</sup> 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.<sup>63</sup> through KYC registrations linked to Aadhaar, or direct Aadhaar linkage. As such, e-RUPI, the latest venture in

---

<sup>60</sup> *ibid.*

<sup>61</sup> *ibid.*

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

<sup>63</sup> 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.<sup>64</sup> Before the judgement in *K.S. Puttaswamy v Union of India*<sup>65</sup> This creates a financial information system that consists of heterogeneous classes of data that are shared between regulators, fintech providers and other third parties. The honeypot of heterogeneous 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.<sup>66</sup> 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.<sup>67</sup> 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

---

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

<sup>65</sup> 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.

<sup>66</sup> 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.

<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup> 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.<sup>70</sup> This has resulted in massive exclusions, exploitation of individuals' data and identity, and the seeding of a surveillance state<sup>71</sup>

Biometric governance in particular, contrary to claims of precision, extends these illusions of transparency, incorruptibility and social inclusion.<sup>72</sup> 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<sup>73</sup>

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

---

<sup>68</sup> *Supra* 97 pg. 220.

<sup>69</sup> 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.

<sup>70</sup> Sawhney, Chima and Aggarwal (n 69) 9.

<sup>71</sup> *Supra* 97 p 231.

<sup>72</sup> 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.

<sup>73</sup> 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<sup>74</sup>**

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.<sup>75</sup> 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’.<sup>76</sup> 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’<sup>77</sup>) 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.<sup>78</sup> and had links to slave plantations (particularly Rose Hall Estate) in Jamaica.<sup>79</sup> 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.<sup>80</sup>

---

<sup>74</sup> *ibid.*

<sup>75</sup> *Supra* 114 p 232

<sup>76</sup> Vere A. da Silva, ‘Commercial Law in India’ (1964) 8 *International and Comparative Law Quarterly Supplementary Publication* 51, 55.

<sup>77</sup> 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.

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

<sup>79</sup> Sissoko and Ishizu (n 122) 3.

<sup>80</sup> ‘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](http://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.<sup>81</sup>

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).<sup>82</sup>

As Rosenthal states, ‘control’, which is at the heart of modern accounting practices, has its etymological roots in “verification”, and later by the 16<sup>th</sup> century, the direction, management, and surveillance that verification required.<sup>83</sup>

#### 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 prophecies were never meant to be precise, and simply allowed a reflective discourse on the world and the human place within it.<sup>84</sup> 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

---

<sup>81</sup> *ibid* 27.

<sup>82</sup> *ibid* 41.

<sup>83</sup> *ibid* 120.

<sup>84</sup> *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.<sup>85</sup> 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.

---

<sup>85</sup> Weitzberg (n 101) 43.