NLSIR

A CRITIQUE OF THE AADHAAR LEGAL FRAMEWORK

—Vrinda Bhandari and Renuka Sane*

Abstract This paper critically examines the legal framework consisting of the Aadhaar Act, the Aadhaar Ordinance, and the Aadhaar Regulations from the perspective of accountability, delegation, and grievance redressal and enforcement. The paper finds that much is delegated to the Unique Identification Authority of India ('UIDAI') without adequate checks and balances. The UIDAI has further delegated the setting of several standards and procedures to its future self, suggesting that the process is operating in a legal vacuum. The accountability framework of the UIDAI remains weak and beset with conflict of interest, as there are no statutorily mandated accountability standards. This makes the performance of the UIDAI difficult to measure. Regulations relating to grievance redressal and enforcement are also weak.

I. INTRODUCTION

India, today, has the world's largest centralised database of personally identifiable biometric information. This is due to the nation-wide issuance of an "Aadhaar number" to all residents, after the collection of their biometrics (including fingerprints, iris scans, and photograph) and demographic data (including address and date of birth) since 2010. At current count, more than 1.2 billion Aadhaar numbers have been issued.[1]

The genesis of the Aadhaar project was with the view that biometric-based authentication was essential to eliminating ghosts and duplicate beneficiaries that were a drag on the public welfare system. The Aadhaar number was

* Vrinda Bhandari is a practicing advocate in New Delhi and appeared on behalf of one of the Petitioners challenging the constitutionality of the Aadhaar Act and its Regulations. Renuka Sane is an associate professor at the National Institute of Public Finance and Policy, New Delhi. We thank Gautam Bhatia, Anirudh Burman, Pratik Datta, Shubho Roy, and Bhargavi Zaveri for useful discussions. All views expressed are personal. We also thankful to the anonymous peer reviewer, whose feedback was very helpful. All errors are our own.

1 "Aadhaar in numbers" https://uidai.gov.in/ (last visited January 16, 2019).

intended to be used to authenticate the identity of a person at the time of their accessing welfare benefits.

Nevertheless, over the last couple of years, the Government rapidly expanded the scope of Aadhaar, with proposals to link Voter IDs with the Aadhaar number now reportedly in the pipeline.[2] The Aadhaar project was controversial since its inception, fraught with concerns regarding privacy, security, large scale collection of biometrics, and the lack of a legal framework abounding it. Its expansion to uses other than benefits delivery made it even more so, leading to a constitutional challenge against the project in the Supreme Court. In part, this was due to concerns of exclusion, security, and accountability arising due to the poor implementation of the Aadhaar scheme and the absence of any data protection law.[3]

Although the constitutionality of the Aadhaar Act was substantially upheld by the majority in the Constitution Bench of the Supreme Court in 2018 in *K.S. Puttaswamy* v. *Union of India*,[4] the Court did not enter into policy questions on the legal framework and infrastructure surrounding Aadhaar. It did, however, express its view that there was a "*need for a proper legislative mechanism for data protection*" and encouraged the government to bring out "a robust data protection regime" based on the recommendations of the Justice B.N. Srikrishna (Retd.) Committee Report.[5] Interestingly, despite the fact that the Government has not passed, or even introduced, a data protection law; it has passed the Aadhaar (and Other Laws) Amendment Bill in the Lok Sabha in January 2019. The Bill eventually lapsed in the Rajya Sabha, but was almost immediately promulgated as the Aadhaar (and Other Laws) Ordinance in February.[6] The Ordinance will lapse in six months, i.e. in August 2019, unless it is passed as a law by both houses of Parliament.

---

[2] Anubhuti Vishnoi, *Linking of Aadhaar and Voter ID may be made mandatory*, Economic Times (December 13, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/linking-of-aadhaar-voter-id-may-be-made-mandatory/articleshow/67069414.cms (last visited January 16, 2019).

[3] Jean Drezeet et. al., *Aadhaar and Food Security in Jharkhand: Pain Without Gain?*, 52(50) Econ. & Pol. Weekly 50-59; Reetika Khera, *Impact of Aadhaar on Welfare Programs*, 52(50) Econ. & Pol. Weekly 61-70; Prasanna S., *Aadhaar in the dock*, Indian Express (August 21, 2018), https://indianexpress.com/article/opinion/columns/aadhaar-row-right-to-privacy-data-leak-protection-uidai-5316396/ (last visited January 16, 2019); Vanya Rakesh, *Aadhaar Act and its non-compliance with data protection law in India*, Centre for Information & Society (April 14, 2016), https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india (last visited January 16, 2019).

[4] (2019) 1 SCC 1. Justice Sikri authored the opinion on behalf of the majority, with a concurring opinion given by Justice Bhushan. Justice Chandrachud wrote the dissent striking down the Act.

[5] *Id*., at ¶ 259. *See also*, Committee of Experts under the Chairmanship of Justice Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018).

[6] *See* Press Information Bureau, "Cabinet Approves Promulgation of Aadhaar and Other Laws (Amendment) Ordinance, 2019" (February 28, 2016) http://http://pib.nic.in/newsite/PrintRelease.aspx?relid=189069 (last visited January 16, 2019).

Regardless of one's views on the necessity and desirability of a biometric-based authentication system, it is hard to deny that the Aadhaar database has redefined the relationship of Indian residents with the State. Given the ubiquity of Aadhaar in one's daily life, a legal framework that elicits better performance and constrains egregious behaviour by the State is critical. This is also important given the three distinguishing features of Aadhaar that separate it from other national identification systems globally. *First,* the mandatory collection of biometrics such as fingerprints and iris scans of more than a billion people, makes it one of the largest databases in the world. *Second*, all such sensitive and personal information is stored in a centralised database called the Central Identities Data Repository ('CIDR'), with the possibility of seeding[7] the Aadhaar number across multiple services. This facilitates the use of the unique 12 digit number to link disparate data sets, which had previously existed in silos. *Finally,* the feature of automated authentication, including e-KYC authentication, to verify the identity of the Aadhaar number holders can, and has,[8] led to even more marked cases of exclusion.[9]

These features of Aadhaar reflect the intersection of technology, governance, power, and freedom, and thus require that the legal framework surrounding the Aadhaar project be more robust than any other system we know in India. It is not enough to point to current standards of other regulatory systems since, any instance of malfunctioning of Aadhaar resulting in surveillance, exclusion, or theft can adversely affect the already existing power imbalance between the citizen and the State. This places a much greater burden on the Aadhaar ecosystem. In fact, since the constitutionality of the Act has been upheld and the questions of policy have been left open, it is even more important to think about how to improve the existing legal framework surrounding Aadhaar.

This paper examines and evaluates the legal framework consisting of the Aadhaar Act, the Aadhaar Ordinance, and the Aadhaar regulations, on issues of delegation, accountability, grievance redressal and enforcement. In doing so, we consciously abstract away from expressing a view on the merits of the Supreme Court's judgment, or the more fundamental question of whether mandating a biometric-based authentication system is the only, or perhaps the most optimal way to reduce leakages and improve tax compliance, as supporters of Aadhaar seem to suggest. We also abstract away from the core questions

---

[7] Seeding is the process by which the Aadhaar number is introduced into various databases for identity verification. Inorganic seeding transpires when the database is automatically updated by the UIDAI using programming tools and algorithms, without the involvement of the Aadhaar number holder.

[8] Drezeet et. al., *supra* note 3; Anmol Somanchi et. al., *Well Done ABBA?*, 52(7) ECON. & POL. WEEKLY(2017); Government of India, Ministry of Finance, Economic Survey of India 2016-17, ¶ 9.76.

[9] While exclusion is likely in any targeted welfare system, Aadhaar was meant to solve the problem.

of privacy protection under the Act, since these issues were discussed by the Supreme Court in its judgment.

Specifically, the paper asks three questions in respect of the legal framework. *First*, if the law and regulations are precisely and clearly drafted. Precision and clarity in law relates directly to certainty and the ability of individuals to plan their lives. We find that the law and regulations are vague and have failed to notify several important guidelines and processes on issues ranging from enrolment to security standards, which has resulted in various parts of the Aadhaar scheme operating in a legal vacuum.

Second, we ask if the law embeds accountability principles that shape the structure and functioning of the Unique Identification Authority of India, the agency responsible for administering the Aadhaar scheme. Every government organisation functions as an agent, and the journey to building high performance agencies lies in setting up a sound principal-agent relationship in the law. We find that apart from a financial audit (by the Comptroller and Auditor General), there exist no adequate performance accountability mechanisms. For instance, there is nothing in the law requiring the UIDAI to set performance standards for itself, nor is there any evaluation of its work, in terms of number of people enrolled, number of authentication failures, number of data breaches, etc. In fact, the Act is unique, inasmuch as the UIDAI is both a data controller (i.e., it controls the procedure/process of data usage) and a data protection authority (i.e., it is in charge of the grievance redressal process). The UIDAI thus wields extraordinary power over the lives of Aadhaar number holders, without adequate accountability mechanisms.

Third, we evaluate the grievance redressal and enforcement provisions that are integral to the integrity of the system and are supposed to create a sufficient deterrent effect against fraud, negligence, or errors. Here again, we find that the legal framework does not provide for a good grievance redressal mechanism, and while the Aadhaar Ordinance has made some improvements to the enforcement mechanism, it still suffers from some problems.

The Aadhaar story in India still has a long way to go. India's experience with Aadhaar ¾ the privacy and surveillance concerns and the technological and logistical challenges it faces are likely to shape debates regarding the benefits and challenges of mandating biometric identity/identification cards across the world.[10] At any rate, it will have had an indelible impact on one-fifth of

[10] In 2018, officials from the Malaysian Government, who were interested in setting up an identity-based architecture for implementation of welfare schemes, visited India to understand India's experience with Aadhaar. *See* Abhishek Waghmare, *Five key lessons Malaysia can learn from India's Aadhaar experience*, Business Standard, (October 17, 2018), https://www.business-standard.com/article/economy-policy/five-key-lessons-malaysia-can-learn-from-india-s-aadhaar-experience-118101601226_1.html (last visited January 16, 2019). In January 2019, the Kenyan government amended the National Integrated Identity Management System, which

humanity. Given that the Aadhaar infrastructure is now here to stay, it is important to understand the legal framework and the areas that need improvement to bring in a robust system for the use of a biometric based digital ID.

II. DESCRIPTION OF THE CURRENT LEGAL FRAMEWORK

The first Aadhaar number was issued in September 2010 by the UIDAI.[11] In December 2010, the Government introduced the National Identification Authority of India Bill 2010 in the Rajya Sabha, in an attempt to give the Aadhaar project a statutory basis. When the Bill came before the 42nd Parliamentary Standing Committee on Finance of the Lok Sabha in December 2011, "serious lacunae and concern areas" were identified, such as the lack of clarity on the collection of biometric information; conceptualisation of the UID scheme; security concerns; involvement of private agencies; and the functioning of UID without a statutory basis.[12]

However, despite this, no changes were made to the Bill, and it eventually lapsed. The Aadhaar project thus, continued without any legislative backing till the passage of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 ('Aadhaar Act') in March 2016 and its publication in the Gazette of India in July and September 2016.

The Act is aimed at targeted delivery of subsidies, benefits, and services by providing unique identity numbers based on an individual's demographic and biometric information. It tasks the UIDAI with serving as the administrator and regulator of the Aadhaar ecosystem, making its functioning integral to the success of the entire system.

After the passage of the Act, five different regulations were notified by the UIDAI in September 2016. These include:

1. *The Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016*, which govern the transaction of business at UIDAI's meetings by specifying, for instance, the number of meetings that have to take place in a

is a DNA-linked national ID. *See* Alice Munyua, *Kenya Government mandates DNA-linked national ID, Without Data Protection law*, Mozilla Blog (February, 8, 2009), https://blog.mozilla.org/netpolicy/2019/02/08/kenya-government-mandates-dna-linked-national-id-without-data-protection-law/ (last visited January 16, 2019).

[11] This was set up by an executive notification of the Planning Commission, Government of India (A-43011/02/2009-Admin. I), dated the January 28, 2009.

[12] Standing Committee of Finance, "42nd Report: National Identification Authority of India Bill, 2010", 15th Lok Sabha (2011) https://www.prsindia.org/uploads/media/UID/uid%20report.pdf (last visited January 16, 2019).

financial year, the quorum required, the role of the Chief Executive Officer, and the decision making process.

2. *The Aadhaar (Enrolment and Update) Regulations, 2016*, which govern the process of enrolment, the generation of Aadhaar numbers and its delivery to residents, update of information, appointment of registrars and enrolling agencies, omission and deactivation of the Aadhaar numbers, and grievance redressal. These Regulations also prescribe a Code of Conduct (in Schedule V), which requires service providers to make "best efforts" to protect the interests of the residents (Rule 1).

3. *The Aadhaar (Authentication) Regulations, 2016* detail the different modes of authentication, namely demographic, OTP, biometric, and multi-factor authentication; the procedure for appointing requesting entities and authentication service agencies; and the storage and access of transaction data and authentication records. These Regulations also introduced an e-KYC authentication facility, which is not specified in the Act.

4. *The Aadhaar (Data Security) Regulations, 2016* provide for the specification of an information security policy, emphasises confidentiality, prescribe the security obligations of service providers and personnel, and provide for audit and inspection. To the best of the authors' knowledge, no such information security policy has been specified till date.

5. *The Aadhaar (Sharing of Information) Regulations, 2016*, which regulate how identity information association with the Aadhaar number holder can be shared with third parties. Interestingly, while the regulations incorporate the principle of purpose limitation for Aadhaar numbers via Regulation 6(5),[13] no such principles limits the use of biometric or demographic information of Aadhaar number holders. Regulation 3 currently follows section 29(1)(a) of the Act by stipulating that core biometric information, namely fingerprints and iris scans, shall not be shared with anyone for "any reason whatsoever".

The Supreme Court largely upheld the constitutionality of the Aadhaar Act and the Regulations, by upholding the passage of the Act as a Money Bill;

[13] Regn. 6(5) states that, "*No entity, including a requesting entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent*."

ruling that the Act was not unconstitutional on the grounds of facilitating surveillance, for violating the right to privacy, or for causing any exclusion under Section 7. The Court also endorsed the Aadhaar project, as it had evolved from 2009, prior to the enactment of the Aadhaar Act in 2016.[14] Apart from this, the Supreme Court upheld Section 139AA of the Income Tax, making Aadhaar linking mandatory with the PAN number for the payment of taxes.

However, it struck down the amendment to the Prevention of Money Laundering Rules, which required linking of Aadhaar number with one's bank account, and the Circular dated March 23, 2017, which amounted to mandatory linking of mobile connections with Aadhaar. The Court also struck down Section 33(2) of the Act on the disclosure of information in the interest of national security, which has far-reaching effects on the status of surveillance law,[15] as well as Section 57, insofar as it relates to body corporates and individuals seeking authentication.[16] In addition, various provisions were read down, including those pertaining to the disclosure of an individual's information without affording her an opportunity of hearing (Section 33(1)); archiving of authentication records for five years (Regulation 27(1) of Authentication Regulations); and storage of metadata (Regulation 26 of Authentication Regulations).[17]

As stated earlier, in response to the Supreme Court Judgment and the Justice Srikrishna Report, the Government eventually promulgated the Aadhaar Ordinance, to amend the Aadhaar Act, the Prevention of Money Laundering Act, 2005, & the Indian Telegraph Act, 1885. The Ordinance, *inter alia*, introduced the idea of "offline verification" and civil penalties, changed the nature and scope of involvement of private entities, inserted a provision

---

[14] The Court, however, interpreted the word "benefit" in Sec. 7, to exclude the requirement of Aadhaar for availing government pension, availing UGC scholarships, or writing exams conducted by CBSE/NEET/JEE. It also gave specific directions in respect of children, including their admission to schools, and accessing benefits under Sarva Shiksha Abhiyan.

[15] The Court struck down Sec. 33(2) which authorised the disclosure of sensitive and personal identity information in the interest of national security, pursuant to a direction of an Executive officer not below the rank of Joint Secretary to the Government. While doing so, the Court ruled that giving such an important power in the hands of a Joint Secretary was not enough, and preferably, a Judicial officer was required. This view, on the need for judicial authorisation/review of surveillance actions, is a change from the standard approved in *People's Union for Civil Liberties* v. *Union of India* (1997) 1 SCC 301, and along with the judgment of the nine-Judge Bench in *K.S. Puttaswamy* v. *Union of India* (2017) 10 SCC 1 ('Puttaswamy'), has laid the foundation for a fresh challenge to surveillance laws.

[16] For a better understanding of the implications of the Court's ruling on Sec. 57, *see* Vrinda Bhandari and Rahul Narayan, *In Striking Down Section 57, SC has Curtailed the Function Creep and Financial future of Aadhaar*, The Wire (September 28, 2018), https://thewire.in/law/in-striking-down-section-57-sc-has-curtailed-the-function-creep-and-financial-future-of-aadhaar (last visited January 16, 2019).

[17] On Sec. 47, pertaining to taking cognizance of offences, the Court was of the view that it was in the fitness of things if Sec. 47 was amended to allowing individuals/victim whose rights were violated, to file a complaint and initiate the proceedings.

to prevent the denial of services for authentication failures, and increased the powers of the UIDAI.

Keeping the judgment of the Constitution Bench and the Ordinance in the background, we now turn towards a critical examination of the legal framework, focusing first on the need for precision and clarity in the law.

III. PRECISION IN THE LAW

The quality of a law depends on the efficacy of its drafting, and the clarity and precision it manages to achieve. Legislative quality is ascertained by the quality of the substantive content of the law, the quality of its form and language, the quality of the operation of the law, and the quality of the processes for producing and implementing legislation.[18]

The test of the quality of law depends on its "effectiveness", namely the extent to which it manages to introduce adequate mechanisms that are capable of producing the desired regulatory results[19] and that can create certainty regarding obligations.[20] The paper evaluates the precision in the Aadhaar legal framework against these parameters, focusing on the excessive delegation in the Act; the future 'delegation' in the Regulations by the UIDAI to itself; and the vaguely-worded nature of the provisions in the Act and Regulations.

A. Excessive delegation

The doctrine of excessive delegation stipulates that Parliament lays down legislative policy and principles governing the rule of conduct, and does not delegate these functions to the Executive.[21] While delegation is undoubtedly a feature of a modern and complex economy, the extent and manner of delegation has an impact on accountability, efficacy, and the democratic character of a government (evidenced through the separation of powers doctrine).[22] Principles of democratic accountability, thus require that the Legislature lays down guidelines for the exercise of rule-making power by the delegated

[18] Victoria Aitken, *An Exposition Of Legislative Quality And Its Relevance For Effective Development*, 2 PROLAW STUDENT J. 1-43.

[19] HELEN XANTHAKI, DRAFTING LEGISLATION: ART AND TECHNOLOGY OF RULES FOR REGULATION (Hart Publishing, 2014); HELEN XANTHAKI, THORNTON'S LEGISLATIVE DRAFTING (5th edn., Bloomsbury Professional Ltd: Hayward's Heath, 2013)

[20] OECD, Improving the Quality of Laws and Regulations: Economic, Legal and Managerial Techniques, OCDE/GD(94)59 (1994) http://www.sigmaweb.org/publications/36976805.pdf (last visited January 16, 2019).

[21] Nathan Chapman and Micheal McConnell, *Due Process as Separation of Powers*, 121 YALE L.J. 1672-1807 (2012); Frank Ditta, *Leading the Way in Unconstitutional Delegations of Legislative Power: Statutory Incorporation of the LEED Rating System*, 39 HOSTRA L. REV. 369-404 (2010) .

[22] Eoin Carolan, *Democratic Accountability and the Non-Delegation Doctrine*, 33 DUBLIN UNI. L.J. 220-252 (2011).

authority, i.e. the Executive, to prevent it from acting in an unbridled and capricious manner.[23]

A central problem with the Aadhaar Act is that it delegates basic policy matters and essential legislative functions – relating to the collection, storage, and use of identity information – to be specified by the Executive i.e., the UIDAI, through Regulations. For example, Section 2(g) of the Aadhaar Act defines "biometric information" as photograph, finger print, iris scan, "*or such other biological attributes of an individual as may be specified by regulation*." The definition of "core biometric information" in Section 2(j) is similarly worded, while "demographic information" in Section 2(k) includes information relating to the name, date of birth, and address of an individual "*and other relevant information of an individual, as may be specified by regulations"*.[24]

The collection of biometric information forms the core of the Aadhaar project, and is also one of its most controversial characteristics. Yet, in the foreseeable future, the UIDAI may, by a simple Executive notification, add DNA within the definition of biometric and core biometric information of an individual under the ambit of "such other biological attribute". This will enable the collection, storage, and use of the underlying genetic code of individuals by the government, through a simple Executive notification, with the only safeguard being the laying down of the Rules before Parliament, *after* they have been drafted, under Section 55 of the Act.

Section 23 represents another instance of excessive delegation, where Parliament has failed to indicate the conditions for the exercise of power by the UIDAI, when it frames regulations on core policy issues of data collection, data sharing, security, and grievance redress. Thus, the demographic and biometric information required for enrolment [Section 23(2)(a)], the procedure for omitting and deactivating an Aadhaar number [Section 23(2)(g)], the standards governing the sharing of an Aadhar number holders' information [Section 23(2)(k)], and the processes related to data management, security protocols, and other technology safeguards [Section 23(2)(m)] are left to be specified by Regulations.

In the process, the Executive, through the UIDAI, has been given uncanalised discretion to set the policy on these issues, without any guidance in the parent legislation. These provisions thus cumulatively create ambiguity about

---

[23] See Delhi Laws Act, In re AIR 1951 SC 332; Ajoy Kumar Banerjee v. Union of India (1984) 3 SCC 127; and A.N. Parasuraman v. State of T.N. (1989) 4 SCC 683 on excessive delegation.

[24] However, the definition of demographic definition expressly excludes the identification of race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history, as part of the definition.

the scope and ambit of the Aadhaar Act, apart from concerns about the lack of Parliamentary scrutiny over any subsequent Regulations.[25]

Notably, although the Supreme Court in the Aadhaar judgment held that "*We do not find that this provision (Section 23 read with Section 54) gives excessive delegation to the Authority*",[26] it did not provide any reasons for the same, nor did it discuss the above provisions and the resulting lack of clarity caused by them.

Unfortunately, the problems of excessive delegation in the Aadhaar Act seem to be replicated in the recently promulgated Aadhaar Ordinance. The constitutionality of Section 7 of the Aadhaar Act was upheld primarily on the Government's assurance that no person would be denied the benefit of a scheme on the failure of authentication, and that the plea of exclusion remained "unproven".[27] The Government has attempted to give this legislative backing through the insertion of a proviso to Section 8(2)(b) that, in case of authentication failure, the requesting entity shall "*provide such alternate and viable means of identification of the individual, as may be specified by regulations*". However, the important task of identifying these alternative and viable means – means that can potentially save the lives of many people – has once again been left to the Executive, without providing any guidance.

B. Further delegation

There are various provisions in the Aadhaar Act that leave the further specification to the Regulations. These include the procedure for authentication in Section 8(1), access to information in Section 28(5), and sharing and publishing of identity information under section 29. However, while notifying the Regulations, the UIDAI has failed to exercise the powers delegated to it, and has left the working of the provisions to be further specified by itself at an undetermined date. Specifically, in 45 instances,[28] the Regulations have

[25] *See* Vrinda Bhandari and Renuka Sane, *Towards a Privacy Framework in the Age of the Internet* (NIPFP Working Paper No. 179), http://macrofinance.nipfp.org.in/releases/BhandariSane2016 privacy.html (last visited January 16, 2019); Vrinda Bhandari and Renuka Sane, *Is Aadhaar grounded in adequate law and regulation?*, Leap Blog (March 22, 2017) https://blog.theleapjournal.org/2017/03/is-aadhaar-grounded-in-adequate-law-and.html (last visited January 16, 2019); Prashant Reddy T., *The Aadhaar Bill is Yet Another Legislation that Leaves Too Much Power With the Government at the Centre*, The Caravan (March 15, 2016), https://caravanmagazine.in/vantage/aadhaar-bill-another-legistlation-leaves-power-centre (last visited January 16, 2019); Madhav Khosla and Ananth Padmanabhan, *Another Challenge Supreme Court Must Address: Excessive Delegation*, The Print (June 28, 2018), https://theprint.in/opinion/another-aadhaar-challenge-supreme-court-must-address-excessive-delegation/76024/ (last visited January 16, 2019).

[26] Puttaswamy, *supra* note 4, at ¶ 400.

[27] Puttaswamy, *supra* note 4, at ¶¶ 375 and 511.12.

[28] *See* Regns. 3(2), 4(5), 7(2), 8(2), 8(4), 11(2), 11(5), 13(2), 14(2), 17, 19(*c*), 20, 22(2), 23(5), 25(1), 29(2), 31(2), 32(1), 32(2)(*d*), 32(3) and Rr. 17, 19, 22, 23, 24, 25, and 26 of the Code of Conduct in Aadhaar (Enrolment and Update) Regulations 2016; Rr. 6(2), 7(3), 12(4), 13(1),

left multiple aspects of the functioning of the Aadhaar Scheme to be "specified by the Authority", i.e., to be specified by the UIDAI itself, causing further uncertainty about the working of the entire Aadhaar Scheme.

In some cases, the failure to specify the process may be justified because the standards relate to technical aspects such as the payment of convenience fees, certification processes, procedure for appointment as Authentication Service Agencies and for establishing secured lease lines, or even the mode of updating residents' information. It could be plausibly argued that such technical aspects are better specified through separate notifications outside the Regulations.

However, important issues surrounding the enrolment, storing, and sharing of data– issues that determine how our sensitive, personal information is collected, authenticated, stored, used, and shared with third parties – have been left unspecified, thus creating a legal vacuum.

For instance, under Section 23(2)(m) of the Act, the UIDAI does not lay out any specific measures for ensuring the security of the biometric and demographic information collected or the authentication logs generated. Instead, this is left to the Regulations. However, Regulation 3(1) of the Data Security Regulations only states that:

> *"*The Authority may specify an information security policy setting out interalia the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and Authentication Service Agencies.*"*

Regulation 5(a) then further requires service providers engaged by the UIDAI to ensure compliance with such information security policy, which to the best of our knowledge, has not yet been notified. Thus, the standards for ensuring information security remain unknown, which is worrying given the vast quantities of sensitive, personal data being stored in one centralised repository.

Similarly, Regulation 29(2) of the Enrolment Regulations leaves the procedure to be followed while inquiring into cases of deactivation or omission of an Aadhaar number by an agency nominated by the UIDAI to be "specified by the Authority for this purpose." Similarly, the form/contents of the

---

14(1)(*d*), 16(8), 18(2), 19(1)(*a*), 19(1)(*h*), 22(2), 22(3), 23(2)(*a*), 28(1), 28(3), and 28(4)(*a*) of the Aadhaar (Authentication Regulations); Rr. 3(1), 4(2), and 6(1) of the Aadhaar (Data Security) Regulations).

subsequent Report that has to be submitted to the UIDAI by this agency are also left unspecified. Regulations 3(2) and 4(5) leave the "standards" for collecting biometric and demographic information required for enrolment, to be "specified by the Authority for this purpose". Another instance of the ambiguity created by the failure to specify the provisions can be found in Regulation 32(2)(d), which stipulate that grievance redressal contact centres have to comply with procedures and processes "as may be specified by the Authority for this purpose."

The incompleteness, and consequent ambiguity, of the Aadhaar Regulations extends to each of the four substantive Regulations. Thus, we have Regulation 16(8) of the Authentication Regulations, which states that the e-KYC User Agency shall maintain auditable logs of all transactions where e-KYC data has been shared with other agencies, "for a period specified by the Authority". Similarly, Regulation 18(2) of the Authentication Regulations states that the process by which the Aadhaar number holder shall have a right to access their logs shall be "specified" by the UIDAI.

The Aadhaar (and Other Laws) Amendment Ordinance 2019, that follows the lapsed Aadhaar (and Other Laws) Amendment Bill, 2018 continues the practice of further delegation. It inserts a proviso to Section 8(2)(b) of the Act, clarifying that:

> "Provided that the requesting entity shall, in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, provide such alternate and viable means of identification of the individual, as may be specified by regulations."

Thus, once again, the actual alternative means of verification have been left to be "specified by regulations".

The Aadhaar Act and Regulations raise an important question as to the consequences of a regulator's (UIDAI) failure to exercise the power that has been delegated to it, and to instead postpone the specification of important standards and procedures to a future undetermined time. Even after the passage of the Act and Regulations, and after more than 1.2 billion residents have been enrolled, there is no clarity on if, and when, any future regulations will be notified by the UIDAI. In the meanwhile, the UIDAI is carrying on, and in fact, hastening, the roll out of the entire Aadhaar project, without any of these guidelines and processes having been notified. Interestingly, although some of these arguments were advanced before the Supreme Court, they do not find any mention in the judgment.

C. Vague and contradictory provisions

A reading of the Act and Regulations together, reveals that core aspects of the Aadhaar project have been vaguely-worded and suffer from contradictions, further undermining the precision of the law.

The vagueness inherent in the Act is demonstrated by Sections 3(2)(a) and (b), which requires enrolling agencies to inform the individual undergoing Aadhaar enrolment about the "manner in which information shall be used" and the "nature of recipients with whom the information is intended to be shared during authentication". However, the Act and Regulations (including the Enrolment Form in Schedule I of Enrolment Regulations) do not give any further guidance, making it difficult to ascertain how compliance with these sections will be achieved, and whether such compliance is actually happening on the ground.[29] This is also mirrored in the Regulations, where Regulation 14(1) of the Enrolment Regulations permits the UIDAI to reject an enrolment on account of duplicate enrolment, quality, "or any other technical reason".

Similarly, even the Aadhaar Ordinance, suffers from vague provisions. Although the Ordinance introduces the idea of "offline verification", presumably in response to multiple reports of authentication failures, it is completely silent on the mechanism for how such a verification system would work in parallel with biometric verification. Even the different modes of offline verification have not been specified. Nor are there any details about the measures being adopted to ensure the security and privacy of the Aadhaar number holder while conducting offline verification.[30]

Apart from this, various provisions of the Aadhaar Regulations cross-cite each other, instead of providing the substance of the Regulation, contributing to further uncertainty. For instance, Regulation 3(3) of the Sharing Regulations states that the UIDAI shall share authentication records of the Aadhaar number holder with her "*in accordance with Regulation 28 of the Aadhaar (Authentication) Regulations*." However, instead of prescribing a procedure for access, Regulation 28(1) of the Authentication Regulations only states that the Aadhaar number holder shall have the right to access their authentication records "*subject to conditions laid down and payment of such fees as prescribed by the Authority*".

The various Regulations that have been framed under the Aadhaar Act are very important inasmuch as they provide the details about how the Aadhaar infrastructure will work in practice. However, as we have shown above, the

---

[29] This fact was recognised by Justice Chandrachud in his dissent.

[30] *See* Vrinda Bhandari, *Why Amend the Aadhaar Act Without First Passing a Data Protection Bill*?, The Wire (January 4, 2019), https://thewire.in/law/aadhaar-act-amendment-data-protection (last visited January 16, 2019)

Act and the Regulations are often bereft of important details, vague, and excessively delegate important decisions to be made by the Executive. Such drafting can lead to potential abuse or transgression of power, a problem that is exacerbated by the weak accountability and grievance redressal frameworks in the Aadhaar ecosystem, as will be discussed in the next few sections.

IV. THE NEED FOR ACCOUNTABILITY

A central element in the history of the evolution of the State is the idea of "checks and balances". The State has the power to coerce its citizens, and therefore, has to subject itself to scrutiny to ensure that it does not abuse such power. This is typically done through the system of representative democracy, where the sovereign is accountable to the elected representatives of the people.[31]

Over the last several decades, the State has outsourced key administrative and regulatory functions to agencies. These agencies are either purely administrative agencies (such as the Social Security Administrator in the United States), or regulatory agencies (such as SEBI, TRAI, or IRDAI in India). As these agencies are one step removed from the people, there have been increasing concerns about the dilution of the accountability of such institutions.[32] Regulators are not directly accountable to Parliament, and their decisions, which have a far reaching impact on the ability of citizens to conduct business, can escape public scrutiny. The rise of what is now known as "new public management" has further invigorated the debate on the appropriate accountability measures.[33]

A response to the unfettered power of agencies, has been to embed accountability frameworks within the laws that create such agencies. The idea is to balance the requirement of autonomy with that of responsibility and responsiveness.[34]

---

[31] Martino Maggetti, *Legitimacy and Accountability of Independent Regulatory Agencies: A Critical Review* 2 Living Review in Democracy 1-9 (2010); Center for Comparative and International Studies, ETH Zurich and University of Zurich, https://www.ethz.ch/content/dam/ethz/special-interest/gess/cis/cis-dam/CIS_DAM_2015/WorkingPapers/Living_Reviews_Democracy/Maggetti.pdf (last visited January 16, 2019).

[32] Giandomenico Majone, *The Regulatory State and Its Legitimacy Problems*, 22(1) J. of West European Politics, 1-34 (1998) .

[33] Colin Scott, *Accountability and the Regulatory State*, 27(1) J. of Law & Soc. 38 (2000) .

[34] For a discussion on ex-ante and ex-post mechanisms for accountability, *see* Vrinda Bhandari, Renuka Sane, and Bhargavi Zaveri, *The Accountability Framework of UIDAI: Concerns and Solutions*, Leap Blog (August 20, 2017), https://blog.theleapjournal.org/2017/08/the-accountability-framework-of-uidai.html (January 16, 2019).

A. Measuring Accountability

Accountability can be assessed *ex-ante* or *ex-post*. Some of the *ex-ante* mechanisms to ensure accountability require clearly setting out the objectives and permissible instruments that could be used to achieve an agency's objectives; having performance oriented goals against which the agency can be benchmarked over a period of time;[35] regular internal audits to review the performance of the agency and its compliance with the law; mechanisms to facilitate transparent decision making, such as mandating public consultations or a white paper before notifying any rules or regulations; publishing a clear rationale for each decision of the agency; and maintaining a well-functioning website.[36]

Other accountability mechanisms include *ex-post* actions such as laying all quasi-legislative instruments before Parliament, to ensure legislative scrutiny; [37] publishing reports showing the goals set out at the beginning of the year, the extent to which they have been achieved at the end of the year, and a statement of reasons explaining any failure to achieve the same;[38] and requiring the conduct of performance evaluations and/or audits by external independent agencies and publishing the reports of such audits. While the *ex-ante* focus is more process-based, the *ex-post* focus is more outcome-based.[39]

---

[35] For example, the Social Security Administration (SSA) Sets Out Strategic Goals for it to Achieve Every Year. *See*, Social Security Administration, "Overview of out Fiscal Year 2012: Goals and Results" https://www.ssa.gov/finance/2012/Overview%20Performance.pdf (last visited January 16, 2019).

[36] For instance, TRAI has recently invited responses to its Consultation Papers on "Regulatory Framework for Over the Top (OTT) Communication Services" (December 2018); "Review of Television Audience Measurement and Ratings in India" (December 2018), "Draft Telecom Commercial Communications Customer Preference Regulations, 2018" (June 2018). *See* TRAI, "Press Releases", https://www.trai.gov.in/notifications/press-release. Similarly, the Ministry of Electronics and Information Technology ("MEITy") has solicited comments on the Draft Data Protection Bill, 2018 "Feedback on Draft Personal Data Protection Bill, 2018" (August 14, 2018) http://meity.gov.in/content/feedback-draft-personal-data-protection-bill (last visited January 16, 2019).

[37] For instance, in Germany, the Parliament has set up the Parliamentary Oversight Panel, which is "*responsible for scrutiny of the work of the intelligence services at Federal level. The Panel can demand the submission of detailed information by the Federal Government on the federal intelligence services' general activities and on operations of particular importance*". *See* Deutscher Bundestag, "Committee: Bodies Exercising Scrutiny" https://www.bundestag.de/en/committees/bodies/scrutiny (last visited January 16, 2019).

[38] For a comparison of reporting by the US SEC and Indian SEBI, *see* Shubho Roy et. al., *Building State Capacity for Regulation in India*, *in* REGULATION IN INDIA: DESIGN, CAPACITY, PERFORMANCE (Devesh Kapur and Madhav Khosla eds.), (Forthcoming) (Oxford: Hart Publishing 2019); https://macrofinance.nipfp.org.in/PDF/RSSS_building-state-capacity.pdf (last visited January 16, 2019).

[39] Monique Pollman et. al., *Risk Taking by Agents: The Role of Ex-Ante and Ex-Post Accountability*, 123(3) ECON. LETTERS 387 (2014).

Both mechanisms have in common, an emphasis on transparency.[40] The OECD suggests seven principles for the governance of regulators. These include, role clarity; preventing undue influence and maintaining trust; decision making and governing body structure; accountability and transparency; engagement; and funding and performance evaluation.[41] The metrics outlined here are based on the understanding that agencies are accountable to the legislature, and therefore the citizens. The agency has to discharge its responsibilities effectively, within the powers ascribed to it.

The legal apparatus surrounding Aadhaar, and the UIDAI, must therefore provide for such a framework. This is important as research demonstrates that there is a correlation between the laws that mandate transparency of a regulator and the responsiveness of such regulators to citizens' preferences.[42] Such requirements would also be in line with emerging thinking on regulatory governance in India.

One example is the Financial Sector Legislative Reforms Commission, which made detailed recommendations on the accountability framework for financial sector regulators.[43] These mandated that *first,* regulators build a system of periodical internal audits and publish the reports of such audits, *second,* that performance audits be carried out by an external auditor, *third,* that systems be built for measuring the performance and efficiency of regulators, and *fourth,* that public consultations and a cost-benefit analysis be carried out before the regulator exercises quasi-legislative powers. We now examine whether the Aadhaar ecosystem has built in such accountability metrics.

B. The accountability framework of the UIDAI

There are two ways to analyse the current accountability framework of the UIDAI. It can either begin with an independent enumeration of what the UIDAI should be held accountable for, or restrict itself to the minimum accountability requirements, given the prevalent legislative framework.[44] This section will evaluate the existing Aadhaar framework from both the lenses.

---

[40] Lindsay Stirton and Martin Lodge, *Transparency Mechanisms: Building Publicness into Public Services* 28(4) J. OF LAW & SOC. 471 (2001) .

[41] OECD, 2014, "The Governance of Regulators", OECD Best Practice Principles for Regulatory Policy, OECD Publishing, https://www.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en (last visited January 16, 2019).

[42] ANIRUDH BURMAN AND BHARGAVI ZAVERI, REGULATORY RESPONSIVENESS IN INDIA: A NORMATIVE AND EMPIRICAL FRAMEWORK FOR ASSESSMENT WILLIAM AND MARY POLICY REVIEW, (Forthcoming 2018), http://ifrogs.org/releases/BurmanZaveri2016_regulatoryresponsiveness.html. (last visited January 16, 2019).

[43] Government of India, Report of the Financial Sector Legislative Reforms Commission, Volume I: Analysis and Recommendations, 2013 https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf (last visited January 16, 2019).

[44] Bhandari et. al., 2017, *supra* note 34.

The primary concern regarding the accountability framework of the UIDAI is the conflict of interest that may arise due to its dual role – that of an administrator as well as a regulator. The UIDAI maintains the biometric data of all Indian residents and oversees the process of authentication and now, offline verification. In this capacity, thus, it acts as a data administrator. Significantly, it is also a regulator, inasmuch as it licenses and regulates various agencies and entities, has the quasi-judicial powers to suspend Registrars and Aadhaar enrolment agencies, writes subordinate-legislation, and is in charge of grievance redressal.[45] Pursuant to the Aadhaar Ordinance, the UIDAI is now also vested with the regulatory powers under Section 23A to issue binding directions to any entity in the Aadhaar ecosystem.

Nevertheless, there is no provision in the law that helps separate the often conflicting responsibilities that come with this dual role. For instance, under Sections 10, 23, and 28 of the Act, the UIDAI is tasked with maintaining the privacy and security of the information in the CIDR, which is the centralised database containing the biometric and demographic data of all Aadhaar number holders. However, under Section 47 of both the original Act and the Ordinance, only the UIDAI is competent to initiate criminal action for the offences under Sections 38 and 39 of tampering with the CIDR. The UIDAI faces a clear conflict of interest in reporting an offence, which would expose its own inadequacies as an administrator. Unfortunately, the draft Data Protection Bill and the Report submitted by the Justice Srikrishna Committee once again conflates this distinction. Under the provisions of the Bill, the UIDAI would be classified as a "significant data fiduciary", but the Committee simultaneously proposes to increase UIDAI's regulatory enforcement and penal powers.[46]

At the very least the UIDAI needs to be held accountable for the following functions: the enrolment and periodic authentication of persons, to ensure that there is no exclusion [Sections 7, 11 and 23(1)]; data quality of the biometric and demographic information of the Aadhaar number holder [Section 3(2)(c) read with Section 32(2)]; the regulation of enrolment agencies and other service providers licensed by it [Section 23(2)(i)]; the security and confidentiality of the data shared by persons who have enrolled with the UIDAI, both at its level in the CIDR and at the level of the other requesting entities/authentication service agencies/enrolment agencies [Section 23(2)(j) and (k)]; and finally, for the adequacy and effectiveness of its grievance redress system [Section 47 and Regulation 32 of the Enrolment Regulations]

---

[45] Vrinda Bhandari and Renuka Sane, *Data Privacy: Too Many Hats for UIDAI*, The Economic Times (July 29, 2018), https://economictimes.indiatimes.com/blogs/et-commentary/data-privacy-too-many-hats-for-uidai/ (last visited January 16, 2019); SFLC, Evaluating the Aadhaar Bill against the National Privacy Principles (November 3, 2016) https://sflc.in/evaluating-aadhaar-bill-against-national-privacy-principles (last visited January 16, 2019)..

[46] Justice Srikrishna Committee Report, *supra* note 5, at 99, 160.

However, a bare perusal of the Act suggests that the Aadhaar Act does not provide adequate performance accountability mechanisms. There is nothing in the law requiring the UIDAI to set performance standards for itself or account for core responsibilities such as number of people enrolled, number of authentication failures, or number of data and security breaches. Despite the Data Security Regulations envisaging the specification of an "information security policy" by the UIDAI, there is no mechanism to ensure that such a policy is actually notified. To the best of our knowledge, no such policy has been notified. Notably, RTI queries have revealed that the UIDAI has never even appointed a Chief Information Security Officer.[47]It is thus unsurprising that there are several stories of security breaches and authentication failures for availing benefits.[48] This is particularly important, since any incident of data breach or biometric authentication failure (leading to deprivation or death) is met with a standard response that the UIDAI keeps "optimal ignorance" about the purpose and manner in which the Aadhaar identity information is used,[49] which allows the UIDAI to evade responsibility.

The Aadhaar Act is also silent on *ex-post* accountability mechanisms, insofar as it neither requires a performance audit nor demands a justification for failures or lapses on UIDAI's part. In fact, the Act does not provide for a data breach notification principle, and thus, Aadhaar number holders may not even be aware of a security lapse. While the Act does provide for an audit by the Comptroller and Auditor General of India ('CAG'), and after the Ordinance, the creation of a UIDAI Fund, this does not by itself guarantee that the CAG will do a performance audit, over and beyond just a financial audit.

In the absence of such statutorily mandated accountability standards, measuring the performance of the UIDAI is difficult. For instance, as recorded in

---

[47] *Aadhaar Truth: UIDAI Never Appointed a Chief Information Security Officer, Reveals RTI*, Moneylife (February 5, 2019), https://www.moneylife.in/article/aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html (last visited January 16, 2019)..

[48] Amber Sinha and Srinivas Kodali, *(Updated) Information Security Practices of Aadhaar (Or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information*, Centre for Internet and Society (2017), https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/ (last visited January 16, 2019).; *State Bank of India Officials Allege Aadhaar Data Misused, UIDAI Dismisses Charge*, Business Today (January 29, 2019), https://www.businesstoday.in/current/corporate/state-bank-of-india-officials-allege-aadhaar-data-misused-uidai-dismisses-charge/story/314752.html (last visited January 16, 2019); *Aadhaar Security Breaches: Here Are Major Untoward Incidents that Have Happened with Aadhaar and What Was Actually Affected*, FirstPost (September 25, 2018) https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html (last visited January 16, 2019).

[49] Ashwini Kumar Sharma, *UIDAI Collects Minimal Information and (Keeps) Optimal Ignorance*, LiveMint (April 23, 2017), https://www.livemint.com/Money/UXfhHHbjdrYW5s4ZWfiqTJ/UIDAI-collects-minimal-information-and-keeps-optimal-ignor.html (last visited January 16, 2019).

the judgment of the Supreme Court, the UIDAI did not track the authentication failure rates at the State level, nor did it conduct any surprise checks/field studies to check the authenticity of exemption registers. When specifically queried on the status of enrolments carried out by 49,000 blacklisted enrolment operators, the UIDAI failed to give any clear response.[50]

Similarly, *Scroll.in* queried the UIDAI about the authentication requests received between September 2010 (when the first Aadhaar number was issued) till October 2016, and how many failed or succeeded. The UIDAI replied that it had not maintained any records between September 2010 and September 2012 and that it did not maintain authentication data state-wise. More importantly, the UIDAI revealed that data about the success or failure of the over 331 crore authentication requests was "not readily available", nor was the breakup of the negative reply to the requesting authority on each of the five modes of authentication "readily available".[51] Accountability and transparency require that such data be proactively shared by the UIDAI with Parliament, and not in response to litigation or RTIs.

Given that the Act provides unguided discretion to the UIDAI to frame regulations, and given the UIDAI's failure to fully exercise the power that has been delegated to it, the lack of an accountability framework is doubly disturbing. Unfortunately, the Aadhaar Ordinance only increases the powers of the UIDAI, without improving the accountability mechanisms. We have already spoken about the UIDAI's power to issue binding directions under section 23A to any entity in the Aadhaar ecosystem. The "Aadhaar ecosystem" has been defined very broadly under the Ordinance and would include requesting entities and offline-verification entities such as banks.[52] Apart from that, Section 21 of the Act has also been amended such that the UIDAI no longer requires the approval of the Central Government before appointing its officers and employees, and deciding their salaries and allowances. This lack of accountability makes it even more important to have a credible and functioning grievance redressal and enforcement framework, which unfortunately, is missing.

V. GRIEVANCE REDRESS AND ENFORCEMENT FRAMEWORK

A key component of a system, especially one that interfaces with individuals, is its ability to provide protection to its intended users from being

---

[50] Puttaswamy, *supra* note 4, at ¶ 60-61.

[51] Anumeha Yadav, *How Efficient is Aadhaar? There's No Way to Know Since the Government Won't Tell*, THE SCROLL (April 5, 2017), https://scroll.in/article/833060/how-efficient-is-aadhaar-theres-no-way-to-know-as-the-government-wont-tell (last visited January 16, 2019).

[52] Raghu, *Six Reasons Why the Aadhaar Amendment Ordinance Undermines Democracy*, THE WIRE (March 12, 2019), https://thewire.in/government/aadhaar-amendments-ordinance-democracy (last visited January 16, 2019).

harassed, misled, or deceived. Laws and Regulations have force only when enforcement mechanisms leave no ambiguity about the costs of violation, and the probability of getting caught is non-trivial. One way of ensuring this is to provide access to a reasonable mechanism of grievance redress, where citizens can complain and seek remedies. An effective dispute resolution body is one which ensures access, convenience, efficiency, standardisation in procedure, and speedy remedies.[53] Experiences of the World Bank[54] and redressal agencies and Ombudsman such as the Financial Ombudsman Service[55] in the UK suggest that there are five aspects to the design of any grievance redress mechanism.

First, having a one point contact centre for complaints collection. When users face a problem, the grievance redressal system should provide for a mechanism whereby customers can take their complaints. The mechanism should be easily accessible to users from across the country, and be able to deal with all manner of complaints - either by addressing the complaints at that point in time, or by channeling the complaint to the right authority. The system should leave no ambiguity in the minds of users of where to go and whom to seek.

Second, the ease of receipt of complaints. When users approach the contact centre, it should be able to receive all the complaints. The contact centre should be able to provide the customer a token number for the complaint, and an expected time of resolution. It should then channel the complaint for resolution to the appropriate authority, and keep the user informed as the complaint travels through the system.

Third, timely resolution of complaints. The grievance redress system should have mechanisms for complaints to be resolved in a specified timely manner, including after exhausting the avenues for appeal, and should be accompanied by a provision for independent review.

Fourth, enforcement provisions and mechanism have to be strong, such that there is an actual deterrence for future action, and should be proportional to the violation.

Finally, meta-analysis of complaints should feed into policy. The system should be able to analyse all the complaints and understand the patterns in the complaints, which may be symptomatic of problems in the underlying system. For example, it is possible that the process flow in enrolment is broken, which

[53] FSLRC, *supra* note 43.

[54] Varun Gauri, *Redressing Grievances and Complaints Regarding Basic Service Delivery* (World Bank, Policy Research Working Paper, 5699), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1871596 (last visited January 16, 2019).

[55] Financial Ombudsman Service, UK, https://www.financial-ombudsman.org.uk/(last visited January 16, 2019).

leads to complaints of a particular nature. This requires change at the policy level, so that such complaints do not arise in the future. Therefore, analysis of the complaints is crucial for establishing the feedback loops for improved policy design.

These factors together create an expectation of an effective and credible grievance redressal system, and will incentivise higher reporting of complaints.[56] Against this background, we now examine the grievance redressal procedure that is present under the Aadhaar Act and the strength of the enforcement mechanisms.

A. Grievance redress under the Aadhaar Act

While assessing the efficacy of the grievance redress framework in Aadhaar, it is important to consider that unlike other regulators such as SEBI or RBI, the UIDAI plays a far more important and pervasive role in the lives of ordinary Indian residents. Aadhaar is almost *de facto* mandatory, being used as a condition for access to entitlements, benefits, and services, and for the payment of taxes. It is thus imperative that the Aadhaar Act puts in place effective grievance redress frameworks, that can handle a diverse range of complaints ranging from enrolment and updating problems, to authentication failures and seeding issues, to deactivation/omission issues.

Accountability in respect of data quality also requires the data controller i.e., the UIDAI, to ensure the reliability of the data, to prevent any denial of services.[57] Unfortunately, however, the proviso to Section 28(5) of the Act precludes an Aadhaar number holder from even accessing her own core biometric information, much less consider correcting it, which violates a tenet of data ownership.[58] This increases the burden on the UIDAI to guarantee the accuracy of identity information on its server to ensure that there are no authentication failures due to incorrect data entries or seeding errors, whilst simultaneously limiting the options of the aggrieved Aadhaar number holders.

The Aadhaar Regulations establish a civil grievance redress mechanism of a "contact centre", *vide* Regulation 32 of the Enrolment Regulations and

---

[56] The UK Report of the Department for Work and Pensions (DWP) found that a majority of dissatisfied customers did not file complaints with the Pension Service, since they did not expect to achieve any satisfactory resolution. *See* DWP, The Pension Service Customer Survey 2007, Research Report No. 532 (2007) 140.

[57] White Paper on the Committee of Experts on Data Protection Framework for India, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf (last visited January 16, 2019).

[58] Telecom Regulatory Authority of India, "Recommendations on Privacy, Security, and Ownership of Data in the Telecom Sector" (2018), http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf at 27-37 (last visited January 16, 2019).

Regulation 8 of the Data Sharing Regulations. This contact centre is envisaged as providing a mechanism to log queries, ensuring safety of the information received, and compliance with the procedures and processes "as may be specified" by the UIDAI for this purpose. Residents are also permitted to raise grievances by visiting the UIDAI's regional offices, or through any other officers or channels as may be specified by the Authority for this purpose.

The handling of grievance redressal in the Aadhaar Regulations, however, suffers from various problems, including the lack of *ex ante* or *ex post* accountability measures described above.[59] *First*, the regulations leave the actual processes of redressal, including the procedure for raising a grievance, the composition of the grievance redress/contact centre, and the timelines envisaged for resolving a query, unspecified. They are silent on the identity/qualifications of the final decision maker, and on whether the inquiry process will be administrative or quasi-judicial in nature.

Second, although grievances can be raised by visiting one of UIDAI's regional offices, there are only 8 regional offices, namely Bangalore, Chandigarh, Delhi, Guwahati, Hyderabad, Lucknow, Mumbai, and Ranchi, which are primarily Tier I cities. Further, these regional offices are not spread out throughout India - for instance, Western India only has one regional office in Mumbai, whereas North India has three offices in Delhi, Chandigarh, and Lucknow. Given the geographical spread of Aadhaar, and the fact that many problems are being faced at a village level, such a clustering of offices in Tier I cities may be inadequate.

Third, the efficacy and performance of these contact/call centres is hard to assess, since the regulations do not prescribe any minimum standards, or even a Code of Conduct (as has been prescribed in the case of Registrars, Enrolling Agencies, and other service providers) that would govern the behaviour of these centres. The Regulations are also silent on the performance standards that can be used to assess the grievance redressal system as a whole, and ensure that the UIDAI can be held accountable.

Fourth, in the case of the Authentication Regulations and the Data Security Regulations, no grievance redressal mechanism has been specified, and no reference has been made to the grievance redressal mechanism provided for in the Enrolment Regulations. This suggests that there is, in effect, no mechanism to redress these two regulations at all.

The failure to specify the process of grievance redress in the Act or Regulations creates great uncertainty on the remedial measures available to

---

[59] *See also* Vrinda Bhandari and Renuka Sane, *The Aadhaar Legal Framework is Broken*, THE MINT (May 30, 2017), https://www.livemint.com/Opinion/EernT2O2yhSZThNPRs5L1O/The-Aadhaar-legal-framework-is-broken.html (last visited January 16, 2019).

an Aadhaar number holder if, for instance, there is an authentication failure or their Aadhaar number is deactivated or omitted. This potentially excludes citizens from accessing various benefits and services that are mandatorily linked to Aadhaar.

B. Enforcement

An enforcement framework is effective if it constrains certain behaviour and disincentivises stakeholders from violating the provisions of the legal framework. In other words, it should induce compliance.[60] For the purpose of this article, we consider two kinds of violations, and evaluate the current enforcement framework as it is set up to deal with these two.

Violations may occur at the time of enrolment. For example, enrolment agencies may not follow proper procedure, may refuse service, or may leak data that is supposed to be kept private. In fact, 49,000 operators were initially blacklisted by the UIDAI for illegally charging residents for Aadhaar enrolment; poor demographic data quality; invalid biometric exceptions; and other process malpractices.[61] These enrolment activities are being monitored by the UIDAI under the Aadhaar Regulations, and any violations may result in immediate suspension and eventual cancellation of the service providers' or the concerned persons' credentials and permissions under the Act.

Another set of violations pertain to security and confidentiality of identity information, and authentication records. These are dealt with in Sections 28(1)-(3) of the Aadhaar Act, which require the UIDAI to ensure the security and confidentiality of identity information and authentication records of individuals and to take all necessary measures to ensure that information under its possession or control is secured. To this end, Section 28(4) mandates the UIDAI to adopt and implement appropriate technical and organisational security measures and to ensure that its agencies, consultants, advisors, or any other person appointed have similar measures in place.

Prior to the Ordinance, the Act did not provide any information on the consequences of non-compliance of either the provisions of the Act, the Regulations, or the "Code of Conduct". There was no gradation of offences and no mention of consequent punishments depending on the offence. For instance, the Enrolment Regulations and the Authentication Regulations suggest that violation of enrolment practices may result in "disincentives", immediate suspension and eventual cancellation of the service providers' or the concerned persons' credentials and permissions under the Act. However,

---

[60] John Armour et. al., Agency Problems, Legal Strategies, and Enforcement, Harvard Law and Economics Research Paper Series No. 644 (2009), http://www.law.harvard.edu/programs/olin_center/papers/pdf/Kraakman_644.pdf, at 10; Roy et al., *supra* note 38.

[61] Puttaswamy, *supra* note 4, at ¶ 1335.

the application of this penalty was left completely up to the discretion of the UIDAI, inasmuch as Regulation 26(3) of the Enrolment Regulations only states that "*such cancellation will take place after holding due inquiry as deemed fit by the Authority*."

Thus, without proportionate penalties and clear procedures for imposing liabilities, stakeholders had limited incentives to comply with the provisions of the Act and the regulations. In this sense, the enforcement framework in the Act was very weak.

Further, Section 47 of the Aadhaar Act originally permitted only the UIDAI to initiate criminal prosecution for offences under the Aadhaar Act, and eliminated the involvement of the Aadhaar number holder entirely. Consequently, its constitutionality was challenged before the Supreme Court for vesting unguided discretion with the UIDAI to decide if, and when, to file a criminal complaint; and for the conflict of interest inherent in the UIDAI initiating criminal action that would reveal a flaw in its security apparatus around Aadhaar. The Constitution Bench of the Court struck down Section 47 in its present form, noting "*... we are of the opinion that it would be in the fitness of things if Section 47 is amended by allowing individual/victim whose right is violated, to file a complaint and initiate the proceedings. We hope that this aspect shall be addressed at the appropriate level and if considered fit, Section 47 would be suitably amended*."[62]

In a positive step forward, the Aadhaar Ordinance has amended Section 47 to permit individuals to file to criminal complaints for most offences punishable under the Act. The Ordinance has also introduced Chapter VI-A on "Civil Penalties" that prescribes various penalties for failure to comply with the provisions of the Act, Regulations, and Directions. Section 33A gives the UIDAI the power to levy a monetary penalty up to Rs.1 crore and an additional penalty, which may extend to Rs. 10 lakh for every day during which the failure continues after the first contravention. Section 33C also designates the TDSAT as the Appellate Tribunal to hear appeals against the decision of the Adjudicating Authority.

Nevertheless, the Ordinance seems to replicate the problems of unguided discretion and conflict of interest inherent in the original Act, particularly Section 47. Section 33B(2), as introduced by the Ordinance does not permit the initiation of anyinquiry by the Adjudicating Officer – for failure to comply with the provisions of the Act, Regulations, Directions – except on a complaint by the UIDAI itself.

Additionally, the Ordinance does not provide any details on the procedure to be followed when determining a violation. It also does not provide for a system

[62] Puttaswamy, *supra* note 4, at ¶ 414.

of gradation of violation such that one gets a sense of proportionate penalties. Thus, the process for determining whether a violation was indeed committed under Section 33A, and what kind of penalty would a specific action deserve, is left to the complete discretion of the UIDAI-appointed Adjudicating Officer. Within the enforcement framework, and within the UIDAI, there is not enough clarity about how the roles of investigator, prosecutor and judiciary will be delineated, and what the relationship between the three entities will be. This brings us back to the question of accountability of the UIDAI raised earlier.

Finally, an Ordinance only remains in force for six months, and after the judgment of the Supreme Court in *Krishna Kumar Singh* v. *Union of India*,[63] re-promulgation of an Ordinance is a fraud on the Constitution. The Aadhaar Ordinance was promulgated in February 2019, after the Aadhaar (Amendment) Bill had lapsed in January 2019, without any ascertainable circumstances under Article 123 of the Constitution that rendered it "necessary" to take "immediate action".[64] Thus, unless both Houses of the Parliament pass the Aadhaar (Amendment) Bill, the Ordinance will lapse in August 2019, undermining even the modest improvements made by the Ordinance.

VI. CONCLUSION

Through this paper, we have sought toevaluate the legal framework under which the Aadhaar Act and the Aadhaar Regulations operate. Specifically, we asked three questions in respect of the legal framework. *First*, we examined if the law and regulations are precisely and clearly drafted. *Second*, if the law embeds accountability principles that shape the structure and functioning of the UIDAI, the agency responsible for administering the Aadhaar scheme. *Third*, we evaluated the grievance redressal and enforcement provisions that are integral to the integrity and success of the system and are supposed to create a sufficient deterrent effect.

Analysis suggests that too much is delegated to the UIDAI without adequate checks and balances. The UIDAI has further delegated the setting of several standards and procedures to its future self, suggesting that that process is operating in a legal vacuum. The accountability framework on the UIDAI remains weak as there are no statutorily mandated accountability standards. This makes measuring the performance of the UIDAI difficult. Regulations relating to grievance redress and enforcement are weak.

Regardless of where one stands on the desirability of a mandatory biometric based identification system for improving services delivery or tax compliance, it is hard to not demand that while the system is running it should clearly

[63] (2017) 3 SCC 1.

[64] For more details see, Vrinda Bhandari, *The Recent Aadhaar Ordinance Undermines the Democratic Nature of Our Polity*, THE TELEGRAPH (March 15, 2019).

enumerate the rights of users, and provide mechanisms to safeguard those rights. In doing so it must provide for checks and balances on the behaviour of the State (i.e. the government and the UIDAI). The several stories regarding data leakages, filing of FIRs against reporters, failures of biometric authentication, mismatch between names on various cards, are an outcome of the weaknesses in the legal framework analysed in this paper, that requires a complete overhaul. Hopefully, that overhaul will come in the form of a comprehensive amended Aadhaar Act, that is passed by Parliament after enacting a data protection law.