New Principles for Governing Aadhaar: Improving Access & Inclusion, Privacy, Security & Identity Management

Nishant Anand[1*]
[1]Department of Science, Technology & Public Policy, University College London, London, UK
Corresponding author: nishant.anand.19@ucl.ac.uk, https://twitter.com/N_Anand, https://www.linkedin.com/in/anandnishant/
ORCID: 0000-0001-6274-4468
Keywords: Aadhaar, e-identity, digital ID, biometrics, responsible governance, trust.

Abstract:

Aadhaar is the largest e-identity programme in the world, linking governmental aid and welfare services to Indian residents. Aadhaar's usage and expansion have been hotly contested and its merits and demerits discussed in the media and academic forums nationally and internationally. This paper looks into the impact Aadhaar has had on Indian society, specifically around access & inclusion to government services as well as on fundamental issues pertaining to privacy, security & identity management. Analysing these dimensions provides evidence for developing new principles for the governance of Aadhaar (and other e-identity programmes). Proposed solutions to address these issues include trust building mechanisms through greater civil society participation in governance of Aadhaar, institutional independence of UIDAI, and the advancement of digital literacy practices for all stakeholders in the Aadhaar system.

Executive Summary:

Legal identification for all by 2030 is a global strategic goal under the UN Sustainable Development Goals (SDG 16.9). Legal identification is perceived as a critical element in increasing people's participation in society and providing them with access to services that can improve their quality of life. Aadhaar, India's digital identity programme, is the world's largest identity project aimed at providing foundational ID and access to state welfare across the nation. By 2019, 1.2 billion people had a registered Aadhaar card. National and state welfare services, and increasingly, a host of private sector services, are linked to Aadhaar. However, India's eID programme has faced significant civil and judicial resistance over matters of privacy, fraud, welfare exclusion and surveillance.

This technology assessment focusses on evaluating Aadhaar using four lenses: the accessibility of Aadhaar and its impact on welfare distribution, privacy concerns and contestations, security issues associated with the Aadhaar architecture, and finally the efficacy of identity management processes. Aadhaar's growing prominence in public and private sector services means that the risks and vulnerabilities in the technology also become embedded in the socio-economic fabric of society. This paper discusses how the current efforts to address highlighted risks are insufficient and drive distrust in the system. This paper concludes by providing recommendations that can help address existing issues. Improving civil society participation in Aadhaar's current and future direction can help foster trust in the Aadhaar ecosystem. Digital rights training presents an avenue to educate all Aadhaar stakeholders on their data

rights, digital risks and mitigation strategies. Formalising UIDAI as an independent authority, not tied to the central government, can also improve the transparency and governance of Aadhaar and provide a pathway for greater participation across public sector, private sector and civil society actors and can provide opportunities to develop acceptable innovations on top of the eID system.

I. Introduction

Effective governance of nations is done through monitoring key indicators that exist at a collective level such as birth rates, life expectancy or health (Rao and Nair 2019). Biometrics-based identification provides a way to not just inform at the collective but also target interventions at a more specific level. Increased migration, security risks and election fraud concerns coupled with a perception of increased wastage in government schemes have driven the need for greater precision in identification systems globally. Digital identity (eID or digital ID) programmes are on the rise both in developing and developed countries and are seen as a mechanism to deliver essential public and private services more efficiently and effectively. The growth of such programmes has increased significantly over the past decade as over a billion people worldwide lack official proof of identity (World Bank 2018).

A lack of legal identification can lead to exclusions from a range of rights and services, such as health care, education, social welfare, and financial services. The United Nations' Sustainable Development Goal 16.9 aims to provide legal identity for all by 2030 (United Nations 2019). As of 2016, the World Bank data indicated that all but 12 low and medium income countries have established a national ID programme (Gelb and Metz 2018). Digital IDs are seen as the most efficient and effective way to provide legal identification and access to welfare. In developed countries, digital IDs are seen as an upgrade to existing identity infrastructure and a means to drive efficiency in public services. Singapore has embarked on a National Digital Identity (NDI) programme to enable citizens and businesses to engage with the government in a more efficient way. Combining its existing ID, Singpass, with a consolidation layer called MyInfo enables citizens to access government services faster and allows businesses to access government verified citizen data. A growing number of developed countries have embarked on similar digital ID programmes, with varied scope, ranging from accessing basic government services to improving financial access (Asia Blockchain Review 2019; eEstonia 2019; Gemalto 2019).

Technological choices made in the design and deployment of eID systems can express a panoply of political motives, which impact how societies operate. The design, deployment and governance of large sociotechnical systems can establish a different public order and power shift among social and political groups (Winner 1980; Hughes 1987). Digital identities rely on an infrastructure that registers and stores population data. The extent of data collection can be limited to basic demographic data or can include extensive biometric information. Many programmes use centralised databases, which result in making central governments data brokers and expose them to security risks. Digital ID authentication can be done through different models (smart cards, mobile apps, biometric authentication etc). The choice of biometrics is highly controversial, since biometric data is unique to each individual. While it may simplify identity verification processes, it can cause significant financial and emotional damage if lost or used fraudulently as there is no recourse to change this data. People in developed countries such as the United States of America and the United Kingdom associate biometrics with criminality and surveillance and hence resist its usage in government programmes, while in developing countries either such risks are perceived to be lower or are supressed (Mansfield-Devine 2015). The selection of partners (private and public sector) to participate in the design, development and maintenance of these socio-technical systems can expand the scope and purpose of eID systems: private sector actors may look to monetise identity data and public sector partners may try to use identification data for security and surveillance purposes.

Aadhaar

This article specifically investigates Aadhaar – the largest digital identity programme in the world, based in India and run by the government of India. An Aadhaar number is a 12-digit unique identifier issued to residents of India as a means for identity verification and access to Government welfare schemes (UIDAI, Government of India 2019d). Access to an Aadhaar number requires registration with demographic and biometric information that is stored in a central database. Prior to Aadhaar's introduction, multiple forms of identity existed in India – Permanent Account Number (PAN) cards for Tax related interactions, passports, ration cards, electoral photo ID cards, birth certificates etc – and these forms of identity continue to exist.

A study by Darlberg highlighted that as of 2019, 1.2 billion people (~95% of the adult population and 75% of children) had enrolled into Aadhaar. Approximately 102 million people had not yet registered on Aadhaar as of 2019, 75 million of whom were children (Totapally et al. 2019). This was driven primarily by a lack of registration in the North-Eastern border States of Assam, Meghalaya and Nagaland where the Central Government-driven Aadhaar programme was met with resistance from residents citing its potential for reducing agency of local residents, enforcing tighter immigration controls and implementing exclusionary social welfare policies in conflict of local tribal customs (Chakravarty 2017). Additionally Aadhaar enrolment had proven exclusionary for specific segments of the population: 30% of the homeless, who lacked documentational evidence required for enrolment, and 27% of the transgender population whose sexual identities had changed over the course of their lifetimes and who felt unable to clarify this during enrolment (Totapally et al. 2019).

Aadhaar was pursued as a newer ID programme with the objective of weeding out erroneous data in India's existing identity databases. However, to obtain an Aadhaar number, a resident has to provide two other existing forms of ID – creating the risk of inputting the same erroneous data into the Aadhaar database (Khera 2019). Aadhaar was envisaged as a foundational identity that would improve participation in government welfare programmes as well as tailored private sector services. However, with no approved data protection and privacy policies in place, such an ambitious programme can leave residents vulnerable to identity fraud and surveillance risks.

The discourse around Aadhaar has been polarised with Indian ruling party politicians and government agencies showcasing the benefits achieved from the use and expansion of Aadhaar in service delivery (Nilekani 2016; Gupta 2019; ENS Economic Bureau 2015), while academics and activists highlight risks, issues and potential falsification of calculated benefits achieved from said technology (Khera 2019; Drèze et al. 2017; Mali and Avila-Maravilla 2018; Amrute, Khera, and Willems 2020; Henne 2019). Aadhaar has been debated on multiple occasions in judicial and legislative settings as well. This article focusses on addressing the following questions: (a) how has Aadhaar delivered on its promises of access & inclusion, (b) what intended and unintended consequences have occurred through the introduction of this system and what can be done about them, and (c) what lessons can be learned on governing such complex digital sociotechnical systems.

I.I. Methodology

This paper reviews Aadhaar as a technology, the legislative and judicial aspects of its formalisation as well as the social impacts of the programmes with which it has been linked. Keyword searches on academic databases (Scopus, Springer, UCL Library) were done using keywords such as "Aadhaar" in combination with keywords that represented implications from the use of the eID system ("privacy", "access"). A full list of keywords used can be found in Table 1.

In an attempt to ensure a rounded opinion, sources from outside academia were also reviewed, such as the Indian Government documents on Aadhaar and other IT projects, legislative and judicial briefs on Aadhaar from the Indian Parliament and Supreme Court obtained from online resources of the Indian Government. Reports from think tanks and developmental agencies such as the World Bank, GSMA, Omidyar Network and commercially published books on Aadhaar were also reviewed.

II. Aadhaar's political and technological development

By the early 2000s, multiple Central Governmental initiatives in India required better citizen identification paradigms. National security concerns following the Kargil war of 1999 drove a requirement for a multi-purpose National Identity Card, especially in border districts (PRS Legislative Research 2011). In 2006, the Department of Information Technology of the Indian Government developed a unique ID programme to better aid in welfare distribution for the poor through the use of technology (PRS Legislative Research 2011). In 2008, the Planning Commission of India published a financial sector reforms report called "A Hundred Small Steps" with a series of proposals to improve financial inclusion, stability and growth in India. The report urged for "expanding access to financial services, such as payments services, savings products, insurance products, and inflation-protected pensions" (Planning Commission of India 2009). Proposal 29 of the report specifically recommended "expediting the process of creating a unique national ID number with biometric identification" (Planning Commission of India 2009).

Topic	Keyword Used
Aadhaar	Aadhaar, Aadhar, Biometric ID in India, UID, UIDAI, Unique Identification Authority of India, National ID
Background	Background, history
Technology	Biometrics, eID, Digital Identity, Identity Management, Design, Technical Design, Database
Roll out	Roll out, Implementation, Deployment, Registration, Enrolment
Impact	Impact, Implication, Benefit, Beneficiary, Welfare scheme, Financial Inclusion, Costs
Access	Access, Accessibility, Inaccessibility, Inclusion, Exclusion, Availability
Security	Security, Privacy, Safety, National Security, Risks, Harm, Surveillance, Data Privacy
Law & Government	Government, Indian Government, Supreme Court, Regulation, Privacy Law, Data Protection Law
Governance	Governance
Citizenship	Citizenship, Citizen, Resident, Enrolee, Rights, Digital Rights
Trust	Trust, Engagement

Table 1: Keywords used to search for pertinent articles on the impact of Aadhaar in India

The Unique Identification Authority of India (UIDAI) was established on the 28th of January 2009, with the objective to create unique identities for all Indian residents. The Aadhaar Act 2016 provided legal backing to the eID programme with UIDAI placed under the purview of the Ministry of Electronics and Information Technology.

Two principles, as per UIDAI, underpinned the design of this identity "(a) robustness to eliminate duplicate and fake identities, and (b) verifiable [confirming identity data on ID creation] and authenticable [confirming identity each time it is used] in an easy, cost-effective way" (UIDAI, Government of India 2009). Nandan Nilekani, co-founder of Infosys, was appointed as the head of UIDAI. Nilekani's negotiated status within government as a cabinet minister peer allowed him to drive an expedited agenda and hire private sector staff to develop and design a technology-driven unique identity project within the government. There was limited public consultation or stakeholder engagement on the design features of such an identity system. The UIDAI team also declined to merge or use existing ID systems to avoid inheriting coding errors perceived to be present in existing ID databases. Aadhaar was positioned as a new voluntary ID, A year after UIDAI's launch the first Aadhaar numbers were given out.

Process of registration

Aadhaar registration follows a tiered process and is done either by governmental registrars or by third party agencies partnering with UIDAI. Three private sector vendors provide automatic biometric identification systems (ABIS) for enrolment centres. In an effort to reduce vendor lock-in, each ABIS vendor competes for work based on their registration throughput. The enrolment process requires a mix of demographic data (name, gender, date of birth as well as proof of address) and biometric data (10 fingerprints, iris scans and a photograph). Additional data such as a phone number or email address can be provided voluntarily (Abraham et al. 2017). This data is then sent to the Central Identities Data Repository (CIDR) through a Secure File Transfer Protocol (SFTP) or through encrypted hard disks sent via approved carriers. The CIDR compares each new enrolee's data with all the others enrolled in the database. This process is called de-duplication. If the enrolee clears this process, a 12-digit Aadhaar number is generated and posted to the individual. If enrolment is rejected, then the registrar is informed of the reasons of rejection and the next steps that need to be taken (Abraham et al. 2017).

Process of authentication

Authentication is required for Indian residents to access state or central government benefits. This can be done via demographic authentication (based on Aadhaar number and demographic data), biometric authentication (based on Aadhaar number and fingerprint or iris scan data), multi-factor authentication or through an OTP (text message) based authentication mechanism (UIDAI, Government of India 2019a). Biometric authentication is the most commonly used method. The authenticating system encrypts this data package and sends it to the CIDR via the authenticating service agency server (see Figure 1 for a simplified authentication process flow). The CIDR validates the received data package against its stored parameters and sends back a confirmation or rejection (yes/no) response.

Security measures instituted by UIDAI include encryption of all data collected at enrolment agencies and decryption only at the CIDR. Contractually ABIS vendors cannot store source data. They are only allowed to store templates of enrolee data that are then sent for de-duplication. Once decrypted, all biometric data is stored offline. Only UIDAI approved authentication systems must be used. Authentication must be done through an encrypted protocol and digitally signed by an Authentication User Agency (AUA) or Authentication Service Agency (ASA) (Abraham et al. 2017).

III. Aadhaar's impact on society

Since its launch in 2009, Aadhaar has been at the centre of an intense socio-political debate. Its role and relevance have expanded from a voluntary ID to a mandatory requirement for accessing state and private sector benefits. However, its expansion into the private sector has, at least temporarily, been curbed by civil society protests against it on the grounds of privacy infringement. Its boundaries are still being defined by legislature, judicial rulings and civil protests (Baxi 2019).

Through Aadhaar, the government seeks to change the citizen-state relationship – from one that was hampered by bureaucratic inefficiencies and an error-prone system into one that works on the definitiveness of technology, albeit ignoring the fact that such technology is still heavily reliant on the inputs fed into it and people involved in running it. This section analyses Aadhaar's impact on the citizen-state relationship through the lenses of availability, access and inclusion, privacy, security, and identity management, highlighting intended and unintended consequences of this technological intervention. Through this analysis, issues associated with the current governance structure of Aadhaar come to the fore. A proposal for addressing these issues is then discussed in Section 4.

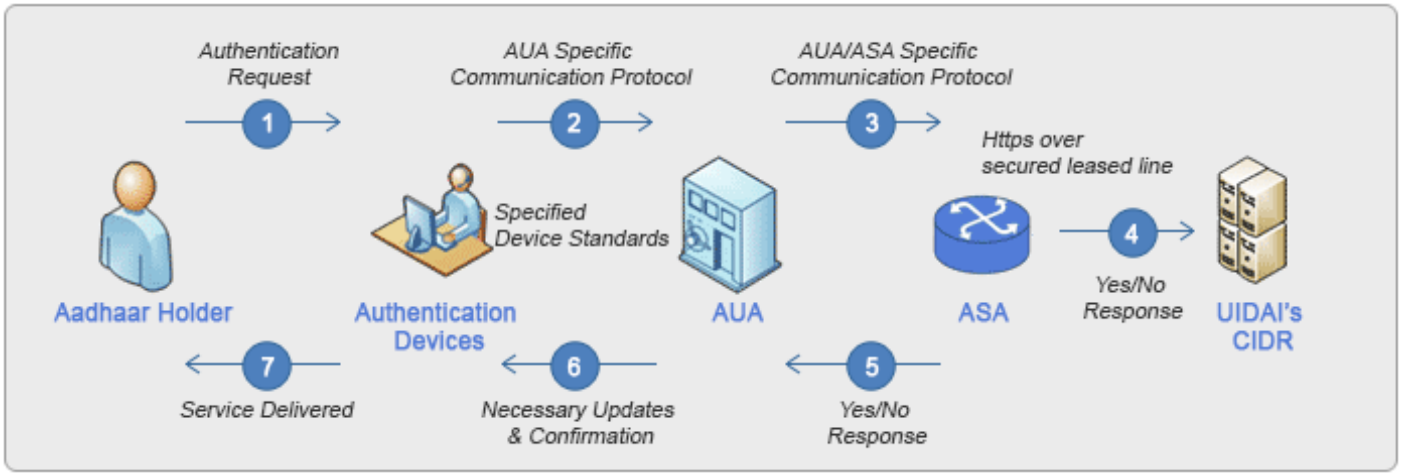

Figure 1: Simplified Aadhaar Authentication Ecosystem (UIDAI, Government of India 2019c)

III.I. Availability, access & inclusion

While the primary purpose of Aadhaar was identification, it has subsequently been used in a number of governmental welfare programmes. The speed at which Aadhaar was designed, developed and rolled out is often discussed in a positive light. By ceding design responsibilities to private sector actors, the overall development of the solution were freed from governmental politics (Ramnath and Assisi 2018). This allowed the design team to think of the solution as being foundational (an identity card) as opposed to functional (ID for a purpose). In contrast to previous identity projects in India, Aadhaar's aim was not provide rights associated with citizenship, benefits or entitlements on its own. It was voluntary to sign up and every Indian resident was eligible to apply for an Aadhaar number, driving demand amongst residents for a government validated proof of identity without an assumed value-laden assumption on its use. However, no public consultations were recorded to discuss the design elements or requirements of such a solution.

Enrolment

The process of enrolment aimed at being as easy as possible – with enrolment centres accepting 18 different documents as proof of identity and up to 35 different documents as proof of address, which were the only documentational requirements in the enrolment process (GSMA 2017). A key focus during enrolment was to develop an accurate national ID register and avoid the errors perceived to be present in existing national ID databases. Although by using existing forms of ID during the registration process accuracy may have been compromised. An ID Insight report survey indicated that the demographic error rate in Aadhaar was 1.5 times the error rate found in the voter ID database (Abraham et al. 2018). ID Insights also found that correcting data errors on Aadhaar systems was perceived to be more challenging by users than enrolment.

Enrolment via biometrics can be inherently exclusionary. Iris scans work subotimally on cataract patients, of which India has the highest proportion in the world (Sobti, Sahni, and Bala 2020). Fingerprint scans tend to be suboptimal for manual labourers as well as older people (Rao 2013). A study by Rashid et al. (2013) on the use of biometrics for attendance at university highlighted the most probable causes of non-registry to biometric attendance systems were wear and tear of fingers (80%), age (8%), physical injuries to fingers (8%), and anaemia (4%) indicating that a system developed to be more inclusive could be marginalising certain groups even further. There are exception handling processes in the Aadhaar system, such as using a secure OTP on a resident's mobile for authentication. Per the Global System for Mobile Communication (GSMA), an industry organisation representing mobile network operator interests worldwide, India's mobile penetration rate is expected to rise to 68% of the adult population by 2020 (GSMA 2016). The remaining 32% that do not have access to mobile telephony lack the financial

means for it and may be the ones most in need of state benefits available through Aadhaar. So, OTP based authentication may put this population at the highest risk of exclusion.

Access to services

Another angle of access and inclusion can be seen on the lines of gender. Prior forms of identity for the poor – such as the ration cards for households (230 million currently in usage) – were in the name of the male household head. This provided household identity but not individual identity. Voter IDs (500 million currently in usage) may be used as individual identity documents but may not be used to access benefits. However, as a foundational ID, Aadhaar allowed for women to have their own identification documentation that wasn't tied to the household (Sen 2019). State schemes aimed at gender parity have tapped into using Aadhaar as a mechanism of breaking the patriarchal hierarchy in a household. The Rajasthan Bhamshah scheme is aimed at female empowerment through direct benefits transfer into the bank account of the eldest woman of the household using Aadhaar for authentication (Rajasthan Administrative Services 2019; Ramnath and Assisi 2018). The success of this programme, however, is contested, as this has led to an increased number of bank accounts for women in Rajasthan, but a vast majority of a household's financial transactions in India are carried out by men in the women's names (CGD 2017).

In 2010, it was estimated that two in three Indians did not have bank accounts, which limited access to key financial resources. Eight years on, 80% of Indian residents now hold bank accounts with a large majority having signed up through the usage of Aadhaar as an identification document (Abraham et al. 2018; GSMA 2017; Misra 2019). An Aadhaar Payments Bridge System (APBS) allows for cash-based government subsidies to directly reach beneficiary bank accounts without the involvement of local officials and institutions perceived by the general public to be rife with fraud. The government of India and the World Bank estimated that $11 billion of subsidy disbursement was done through APBS (CGAP 2015). Although the increase in cash subsidies is also a means to reduce and dismantle the food subsidy system, a long-standing social welfare mechanism on which millions of poor Indians still rely. Cash transfers instead of food subsidies would mean that the poor now have to buy food at market prices (Mander 2015).

Many central and state governmental programmes have mandated the use of Aadhaar to access welfare scheme benefits. Aadhaar seeding was authorised across all major government schemes: food rations, LPG subsidies, pensions, rural employment programmes and disbursements are done per head. If the old system was rampant with fraud, the new system brings new issues. Inaccurate Aadhaar seeding has led to reduced food rations disbursement in certain regions (Drèze et al. 2017).

Availability & inclusion

Accessing Aadhaar enabled welfare benefits requires the availability of inclusionary and accurate point of service (PoS) devices at welfare distribution centres. This requires investment in technological infrastructure that covers the nation and can cater to a diversity of ages, demographics and socio-economic segments. Drèze et al (2019) highlight that small households (such as elderly couples, widows living alone) faced the largest risk of PoS-based exclusion, approximately 7% of their sample study population. These families also tended to be the poorest, with no mobile phones to enable biometric exception handling. A lack of internet connectivity, common in rural India, required for PoS systems and Aadhaar based authentication, is another cause for exclusion on welfare benefits. The "failure to match" rate, which drives inclusion / exclusion on welfare distribution, is state dependent and the rural state of Jharkhand had a failure to match rate of 49%, Rajasthan of 37%, Gujarat of 6% and Andhra Pradesh of 5% (Dixon 2017). Higher failure to match rates in Jharkhand and Rajasthan can be attributed to lagging technological infrastructure investments required to connect remote welfare distribution centres to the central Aadhaar database.

Critically, biometric authentication may not address fraud that is often cited in Indian welfare distribution systems. Khera (2019) points out that three types of fraud exist in welfare distribution: eligibility, quantity and identity. Eligibility fraud pertains to inclusion of people in welfare schemes where they are ineligible, quantity fraud relates to eligible people receiving less than their share of welfare and identity fraud pertains

to fraudulent people masquerading as eligible ones to access the latter's benefits. Biometric authentication can only solve identity fraud (Khera 2019). Eligibility and quantity fraud cannot be addressed by biometric systems; in fact in sample districts studied quantity fraud was still as high as pre-Aadhaar levels (Drèze et al. 2017). The main problem cited is a lack of power of the welfare receiver in comparison to the local welfare supplier, which cannot be solved by a technological solution. A local supplier's incentives and renumerations have not changed in this new Aadhaar based model whilst his costs have gone up: it can take much longer to distribute Aadhaar based rations in a village due to the difficulty of the authentication process (Drèze et al. 2017). Addressing eligibility and quantity fraud requires a closer look upstream in the welfare distribution supply chain – with a critical study into governmental practices and actors that enable such fraud to exist.

III.II. Privacy

The right to privacy is documented in multiple transnational charters (United Nations 1966; 1948). Privacy, in the developed world at least, is seen as a fundamental human right that allows people to define their own boundaries and have agency in terms of decision making. In India, the right to privacy in the context of Aadhaar is topical and nascent. Family structure, economic necessity and cultural foundations make privacy (or the lack thereof) hard to attain in daily life and an alien concept. In fact, most Indian languages don't have a specific word for privacy (Satpathy 2017). A right to privacy is especially essential when it comes to emergent digital technologies, such as mobile phone apps and platforms, as they tend to monitor, track, suggest and categorise without consent and knowledge.

The right to privacy

In 2012, Retired Justice K.S. Puttuswamy filed a petition in the Indian Supreme Court challenging the constitutionality of Aadhaar on the grounds that it violated a right to privacy. The Supreme Court ruled that the right to privacy, while not specifically stated in the Indian constitution, was indeed a constitutional right for all citizens and covered under the constitutional right to life and fundamental liberty (Tomlinson 2017). This has curbed the expansion of Aadhaar usage and seeding across governmental and private sector programmes. It also cut short the government's plan to link multiple databases (mobile, national security) using Aadhaar. Aadhaar could only be mandated in welfare subsidy schemes that are financed by the consolidated fund of India and the government had to provide an optionality for other means of ID if beneficiaries did not have an accessible Aadhaar number. However, this give and take between the government and the citizen's right to privacy continues to be hotly contested.

Aadhaar is no longer mandatory to access welfare but it is also not unconstitutional. So, while government programmes have to provide an alternative to Aadhaar for identification, most programmes are devised to use Aadhaar as a default primary identification mechanism. The ease of registration with Aadhaar makes other ID usage unattractive in comparison. The government also continues to expand the scope and reach of Aadhaar seeding across non-welfare programmes as well (taxes, financial inclusion, India Stack) and across private sector services. Since over 90% of the population is already registered, a lot of effort is now focused on creating a critical mass of services on the supply side to cater to the registered population. An increase in digitally enabled services that utilise Aadhaar as the preferred form of ID will continue to cement its dominance as identity of choice evidencing platform economics at its most basic and operative.

Privacy lapses in design & enrolment

Biometrics are inherently invasive as they collect unique and sensitive information about individuals, which is stored in a centralised database operated by an external entity. A paper-based system for legal identity provides "privacy by obscurity" while a digital systems like biometrics, without robust legal safeguard or mature policies, can cause a complete loss of privacy (Sen 2019). Digitization provides a rich source of personal data that is instantly accessible. Such a change puts profound responsibility on the government and policymakers to ensure responsible use (Dixon 2017).

Given such responsibility, Aadhaar's design, development, enrolment and usage across multiple governmental programmes have been completed without any legal safeguards besides the policies defined by UIDAI themselves. Only in December

2019, almost a decade after Aadhaar's inception, was a data protection bill was introduced in the Indian Parliament. The law firm, Linklaters, indicates that the draft bill "borrows heavily from EU GDPR" and allows transnational businesses to replicate some processes already implemented to comply with GDPR (Christopher 2019). Privacy analysts, however, have indicated that aspects of the bill are an attempt to re-access Aadhaar data in the name of national security, a specific remit that was rejected by the Supreme Court in 2018 (Parkin 2019b). In June 2019, the National Crime Records Bureau (NCRB) of India expressed a plan to introduce facial recognition software that would match people of interest against a database of facial images – allowing for "fast and accurate face recognition in a live environment" (Parkin 2019a). The NCRB denied that such a system would link to Aadhaar; however, it is unclear whether such connections can be made in light of the new, and still under review, data protection bill that permits access to Aadhaar data on the grounds of national security.

While enrolling into welfare schemes like National Food Security (NFS), enrolees unknowingly consent to UIDAI sharing basic biographic data with the organisations running the welfare schemes (Rao 2019). Explicit consent in the usage of biometric data is not discussed in the enrolment process nor is such usage required to be notified to enrolees, which is in sharp contrast to EU GDPR where consent is mandated (Dixon 2017).

A lack of privacy within Aadhaar-linked welfare schemes makes the marginalised more exposed. Ramanathan cites key examples where a lack of Aadhaar ID was used as a deterrent in providing services to marginalised and vulnerable social groups: lower caste manual scavengers were denied rehabilitation services, women rescued from prostitution were refused entitlements and medical aid, and disabled individuals were refused skills training and necessary aid (Ramanathan 2017).

Digital rights awareness

A general understanding of data rights within India is low, an issue that can be highlighted using the digital divide metrics in India as a proxy. Internet usage in India is limited to about 50% of the population (500 million), of which 200 million were rural users, though rural India represents 65% of the population (Mathur 2019). Accessing the internet itself does not mean the user understands their data rights. The Indian government has embarked on a Digital Inclusion initiative (Digital India) to deliver digital infrastructure and services to the Indian public, though none of its pillars focus on digital rights education (Government of India 2019). In Aadhaar's context, a deeper understanding of how people understand what they are signing up for (or signing away) has not been evaluated nor has their perception of such requirements been evaluated when they are told about their data rights and risks associated with the technological infrastructure of Aadhaar.

III.III. Security

The right to privacy in the context of Aadhaar rests heavily on the security of the overall system. Aadhaar was initiated partly by a requirement of national security, yet the government's own practices in embedding robust security measures for the Aadhaar system have often seemed inadequate. Multiple security breaches have surfaced: Microsoft Excel files containing Aadhaar numbers and demographic data have been accidentally published from government offices, bank details of 1.6 million pensioners were uncovered in a security breach, and 2 million pregnant women's personal details were leaked (Medianama 2018). Such security breaches point to a range of issues: a lack of security training of government officials, a lack of defined data security policies, a proliferation of insecure data files used across government departments, system vulnerabilities within Aadhaar and its linked API network, and external cybersecurity threats from hackers exploiting system vulnerabilities (Medianama 2018). At present, reported data security leaks have led to no legal action nor was any financial compensation provided to the victims.

As a single centralised database holding the sensitive data of over 1.2 billion people, Aadhaar is a target for cyberattacks. Any compromises to such a database are irreversible considering the unique and unchanging nature of the data stored in it. The UIDAI response to criticism on its security practices has been to point to the technical safeguards put in place in the Aadhaar database rather than addressing risks from a sociotechnical lens (UIDAI, Government of

India 2019b). To see Aadhaar's ecosystem just as a technological solution, with issues that can be solved by better technology, is a shortcoming in itself. Government departments (that pull Aadhaar data) have displayed sensitive information of individuals online such as their Aadhaar number, caste, religion, address, photographs and financial information (Sinha and Kodali 2017). Such gaps point to a lack of strategic design and education on data protection across interlinked governmental systems and departments. Four government portals have disclosed 130-135 million Aadhaar numbers and 100 million bank account details (Sinha and Kodali 2017). The Aadhaar seeding process in all participating governmental schemes is a fundamental security risk, as the Aadhaar number is not just in one database but is seeded across multiple databases of which UIDAI has no control.

The scale of security lapses reveals a lack of strategic thinking around systems security issues pertaining to interlinked governmental databases. It points to a gap in India's own security policies, specifically the National Data Sharing and Accessibility Policy and Cyber Security Policy, which provide classification criteria for data but no recommendations on how different categories of data should be treated (Sinha and Kodali 2017).

III.IV. Identity management

Maintaining the accuracy of data relies on an easily accessible process to update one's own information. Yet, surveyed citizens perceived the cost and process of updating their information in Aadhaar to be more onerous than the process of enrolment (Abraham et al. 2018). The UIDAI does not have a process for decommissioning issued numbers. It can be estimated that since its inception in 2009, there are now approximately 76 million enrolees in Aadhaar (6% of the database) that are now dead (St_Hill 2019). Aadhaar was originally intended to weed out "ghost accounts," yet now as many as 76 million ghost Aadhaar numbers exist and this number will continue to grow. It is unclear how Aadhaar is useful to monitor population trends or the success of governmental programmes if the dormant accounts are not weeded out. In addition, these ghost accounts are prime targets for identity fraud.

Identity fraud instances

Within Aadhaar, identity fraud can be perpetrated through forgery of Aadhaar credentials during registration or authentication, or via collusion between authenticating agents. An Aadhaar number can also link various relational databases and services (financial, welfare, mobile) together, opening the door to impersonation and identity fraud. One of the biggest risks is collusion between insiders (Agrawal, Banerjee, and Sharma 2017). The notion of an insider here goes beyond just authenticators and bureaucrats but all parties that work in environments enabled by an Aadhaar based authentication bridge. Between 2011 and 2018, 164 cases of fake or forged Aadhaar usage were reported in news media (Somanchi and Paikra 2018; Saldanha 2018). While this is a small fraction of total Aadhaar enabled transactions, the overall rise in fraud incidents has been exponential: 3 in 2012 to 73 in 2018. In one such example, eight accused were charged with forging existing Aadhaar details of bank customers, adding their own photographs to these cards and obtaining loans based on the victims' Aadhaar details and bank balances (Tribune News Service 2018). The accused were financial services employees who could access Aadhaar details through their employers. The Aadhaar system is also vulnerable to biometric identity fraud – by forging fingerprints from objects that may have been handled and extracting iris scans from high resolution photographs, although instances of such crimes have not yet been reported (Rajput and Gopinath 2017).

Identity negotiation

Official identification bestows a social status upon a person that then defines their relationship with government and society. Biometric identity systems are deployed with an aim to deliver a greater accuracy in the transactions that an individual has with the State. Yet, these technological systems are often underpinned by legacy processes, individual judgments and significant manual readjustments – all of which remain unchanged. In her fieldwork evaluating the Aadhaar-enabled Public Distribution System, Rao (2019) highlights these very attributes. She describes that post Aadhaar verification welfare applications are manually checked against assumed electricity usage per household, assumed family size, informal interviews with neighbours, and household

and car ownership – none of which is a direct indicator of household identity or economic status. Inspectors then checked the approved applications on site, but they too could be corrupted through bribes. Government programmes are also still constrained by delivery capacity issues. As Rao (2019) explains in her study "Delhi's ration system excluded people considered affluent, everyone without an Aadhaar number, families who were absent from home during an inspector's visit, and every family that submitted an application after the cap of 7,277,996 NFS cards had been reached."

Identification through Aadhaar (and any technological identity system) is done through attributes or identifiers. Identity in the eyes of the government is thus no longer about the social, but it is about the absolute (Sarkar 2014). On the face of it, this may seem fair, but such a system works on absolutes and binary decisions regarding welfare entitlements for the vulnerable with no process for appeal, correction or negotiation. Such an absolutist process denies identification through standardisation and considers the errors smaller in comparison to the vast majority for whom the system may work, regardless of their social or economic needs. Further, the onus of identity shifts to the individual, who needs to be authenticated via a centralised mechanised system, and can no longer rely on local knowledge and judgements of site-based governmental officials (Sarkar 2014).

4. Recommendations

Responsibility for science and technology should be built on the understanding that artefacts – such as Aadhaar – are not just technically created but also socially constructed (Hughes 1987; Stilgoe, Owen, and Macnaghten 2013; Winner 1980). Governance of such technologies needs to be a negotiated exercise – built on a shared understanding of current and future implications of the technology in question. Aadhaar's development and current situatedness has been devoid of such negotiation outside of acrimonious civil or judicial settings. Greater adoption of Aadhaar based innovations can come through opening avenues for greater participation from civil society. This could take the form of legislative debate or open citizen consultation forums that involve Aadhaar enrolees in decisions on how their data is being used/managed and what future partnerships are acceptable. Representative consultation forums can help bring together various points of view, develop a shared narrative and build trust in the overall ecosystem.

Trust entails two aspects: trust in the information received about the technology itself and trust in the institutions developing and running such technologies (Nelson and Gorichanaz 2019). When trust is high, perceived benefits tend to be higher and perceived risks tend to decline on technologies (Siegrist, Cvetkovich, and Roth 2000). Trust building requires proactive engagement of the institution that goes beyond ensuring technical safeguards. UIDAI's track record in addressing risks to Aadhaar often have either focussed on retaliation against dissenting voices or public statements defending the technical capabilities of Aadhaar. A changed public engagement strategy and a focus on building bridges with civil society can help foster trust in the ecosystem.

In parallel to greater participation and deliberation, the organisational arrangement for UIDAI needs further consideration. In its current set up, the Indian Central Government is the owner, manager and auditor of the Aadhaar repository, which reduces incentives to address underlying process issues or security risks. A separation of duties between day-to-day management, oversight and audit would create a system of checks and balances.

While UIDAI has constantly stated that the Aadhaar enrolees own their data, no enrolee can delete their own data or affect how it is secured and stored. Ownership changes can be made organisationally by separating UIDAI from any Central Government department and running it as a standalone entity. Funding to such a body can be through a combination of state funding and membership fees charged to private sector actors wishing to participate in the Aadhaar ecosystem. Audit and performance management can be done by a government department or a third-party auditing firm. Such structural changes would require a legislative mandate defining a new remit for UIDAI and additional measures to curb risks such as institutional capture by special interest groups.

The deployment of Aadhaar linked services should be complemented with programmes to improve digital

literacy and an understanding of data rights across the nation. Increasing awareness of the risks inherent in the overall Aadhaar system will allow people to be more vigilant and reduce the likelihood of harm. Cybersecurity training should be mandated for all governmental officials, especially those handling Aadhaar data. Technical standards should be developed that define the Aadhaar seeding process, limit data access to only authorised personnel.

Digital ID methods are the lynchpin in an ever-growing technology infrastructure to provide tailored services to citizens/consumers at the lowest cost. Such programmes typically follow platform-based models, linking supply (government aid and private sector services) to demand (citizens and consumers). However, these new arrangements can cause significant exclusions and harm if a technocratic approach is taken that disregards the socio-political milieu of these technologies. Often trade-offs between privacy and innovation are seen as a necessity that must be accepted – although such trade-offs need not exist at all. Trust in systems and institutions are crucial to the adoption and continued expansion of such programmes. Including civil society in the design and management of Aadhaar, through public consultation and governance boards, and driving for greater institutional independence of UIDAI provide pathways for improving trust across the Aadhaar ecosystem.

References

Abraham, Ronald, Elizabeth S. Bennett, Rajesh Bhusal, Shreya Dubey, Qian (Sindy) Li, Akash Pattanayak, and Neil Buddy Shah. 2018. 'State of Aadhaar Report 2017-18.Pdf'. ID Insight.

Abraham, Ronald, Elizabeth S Bennett, Noopur Sen, and Neil Buddy Shah. 2017. 'STATE OF AADHAAR REPORT 2016-17', May, 24.

Agrawal, Shweta, Subhashis Banerjee, and Subodh Sharma. 2017. 'Privacy and Security of Aadhaar: A Computer Science Perspective'. *Economic and Political Weekly*, 15.

Amrute, Sareeta, Reetika Khera, and Adam Willems. 2020. 'Aadhaar and the Creation of Barriers to Welfare'. *Interactions* 27 (6): 76–79. https://doi.org/10.1145/3428949.

Asia Blockchain Review. 2019. 'South Korea EID'. *Asia Blockchain Review - Gateway to Blockchain in Asia* (blog). 9 July 2019. https://www.asiablockchainreview.com/south-korea-approves-blockchain-based-id-authentication-service-for-sandbox/.

Baxi, Parul. 2019. 'Technologies of Disintermediation in a Mediated State: Civil Society Organisations and India's Aadhaar Project'. *South Asia: Journal of South Asian Studies* 42 (3): 554–71. https://doi.org/10.1080/00856401.2019.1602808.

CGAP. 2015. 'From Cash to Digital Transfers in India: The Story So Far'. CGAP. 2015. http://web.archive.org/web/20170613055012/https://www.cgap.org/sites/default/files/Brief-From-Cash-to-Digital-Transfers-in-India-Feb-2015_0.pdf.

CGD. 2017. 'Impact of Bhamashah on Digital Governance Reforms in Rajasthan'. 2017. https://www.microsave.net/files/pdf/171212_Household_Perception_Impact_of_Bhamashah_Digital_Governance_Reforms_in_Rajasthan.pdf.

Chakravarty, Ipsita. 2017. 'Aadhaar Has Run into Pockets of Resistance in Three States of the North East'. Text. Scroll.In. https://scroll.in. November 2017. https://scroll.in/article/857074/aadhaar-has-opened-up-pockets-of-resistance-in-three-states-of-the-north-east.

Christopher, Deepa. 2019. 'India – Full Analysis of the Proposed New Privacy Law| DigiLinks | Linklaters'. Linklaters. 2019. /en/insights/blogs/digilinks/india-full-analysis-of-the-proposed-new-privacy-law.

Dixon, Pam. 2017. 'A Failure to "Do No Harm" -- India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.' *Health and Technology* 7 (4): 539–67. https://doi.org/10.1007/s12553-017-0202-6.

Drèze, Jean, Nazar Khalid, Reetika Khera, and Anmol Somanchi. 2017. 'Aadhaar and Food Security in Jharkhand'. *Economic and Political Weekly*, no. 50 (December): 12.

eEstonia. 2019. 'Estonia EID'. E-Estonia. 2019. https://e-estonia.com/solutions/e-identity/id-card/.

ENS Economic Bureau. 2015. 'Happy That NDA Has given Aadhaar a Big Push: Nilekani'. *The Indian Express* (blog). 7 December 2015. https://indianexpress.com/article/india/india-news-india/happy-that-nda-has-given-aadhaar-a-big-push-nilekani/.

Gelb, Alan, and Anna Diofasi Metz. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?*

Gemalto. 2019. 'Belgium EID'. 2019. https://www.gemalto.com/brochures-site/download-site/Documents/gov_belgium_id.pdf.

Government of India. 2019. 'Programme Pillars | Digital India Programme'. 2019. https://digitalindia.gov.in/content/programme-pillars.

GovTech Singapore. 2021. 'GovTech Singapore - Organisational Overview'. 2021. https://www.tech.gov.sg/who-we-are/our-role/.

GSMA. 2016. 'The Mobile Economy - India 2016'. https://www.gsmaintelligence.com/research/?file=134a1688cdaf49cfc73432e2f52b2dbe&download.

———. 2017. 'Aadhaar: Inclusive by Design'. GSMA. March 2017. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf.

Gupta, Komal. 2019. 'Aadhaar a Game Changer, Helped Govt Save ₹90,000 Cr till Mar 2018: Arun Jaitley'. Mint. 6 January 2019. https://www.livemint.com/Politics/JufOIND7IUPjnyZCE4BrfL/Aadhaar-is-a-game-changer-Arun-Jaitley.html.

Henne, Kathryn. 2019. 'Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India'. In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 223–45. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-14540-8_11.

Hughes, Thomas Parke. 1987. 'The Evolution of Large Technological Systems'. In *The Social Construction of Technological Systems*. MIT Press.

Khera, Reetika. 2019. *Dissent on Aadhaar: Big Data Meets Big Brother*. Orient BlackSwan Private Limited.

Mali, Nidhi Vij, and Martha A. Avila-Maravilla. 2018. 'Convergence or Conflict?: Digital Identities vs. Citizenship Rights: Case Study of Unique Identification Number, Aadhaar, in India'. In *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, 443–48. Galway Ireland: ACM. https://doi.org/10.1145/3209415.3209487.

Mander, Harsh. 2015. 'Replacing Food with Cash'. Mint. 20 October 2015. https://www.livemint.com/Opinion/hnytasM4zVTEWmQnt1fc1N/Replacing-food-with-cash.html.

Mansfield-Devine, Steve. 2015. 'Biometrics in Developing Countries'. *Biometric Technology Today* 2015 (4): 5–8. https://doi.org/10.1016/S0969-4765(15)30060-6.

Martens, Tarvi. 2010. 'Electronic Identity Management in Estonia between Market and State Governance'. *Identity in the Information Society* 3 (1): 213–33. https://doi.org/10.1007/s12394-010-0044-0.

Mathur, Nandita. 2019. 'India's Internet Base Crosses 500 Million Mark, Driven by Rural India'. Livemint. 11 March 2019. https://www.livemint.com/industry/telecom/internet-users-exceed-500-million-rural-india-driving-growth-report-1552300847307.html.

Medianama. 2018. '#AadhaarLeaks - A Continuously Updated List of All Aadhaar Data Leaks'. *MediaNama* (blog). 4 May 2018. https://www.medianama.com/2018/05/223-aadhaar-leaks-list/.

Misra, Prakhar. 2019. 'Lessons from Aadhaar: Analog Aspects of Digital Governance Shouldn't Be Overlooked'. *Pathways for Prosperity Commission* Background Paper Series; no. 19: 34.

Nelson, Jake, and Tim Gorichanaz. 2019. 'Trust as an Ethical Value in Emerging Technology Governance: The Case of Drone Regulation'. *Technology in Society* 59 (November): 101131. https://doi.org/10.1016/j.techsoc.2019.04.007.

Nilekani, Nandan. 2016. 'Basis of a Revolution'. *The Indian Express* (blog). 9 March 2016. https://indianexpress.com/article/opinion/columns/aadhaar-bill-lpg-subsidy-mgnrega-paperless-govt-basis-of-a-revolution/.

Parkin, Benjamin. 2019a. 'India Defends Plans for Facial Recognition System'. Financial Times. 9 November 2019. https://www.ft.com/content/d50dcf96-0223-11ea-b7bc-f3fa4e77dd47.

———. 2019b. 'India Proposes First Major Data Protection Law'. Financial Times. 11 December 2019. https://www.ft.com/content/df6fd8d4-1bf1-11ea-9186-7348c2f183af.

Planning Commission of India, ed. 2009. *A Hundred Small Steps: Report of the Committee on Financial Sector Reforms*. New Delhi : Thousand Oaks, Calif: Planning Commission, Government of India ; SAGE Publications.

PRS Legislative Research. 2011. 'The National Identification Authority of India Bill'. *PRS Legislative Research*, 6.

Rajasthan Administrative Services. 2019. 'Bhamashah Yojana'. *RajRAS - Rajasthan RAS* (blog). 15 July 2019.

https://www.rajras.in/index.php/bhamashah-yojana/.

Rajput, Ajinkya, and K. Gopinath. 2017. 'Towards a More Secure Aadhaar'. In *Information Systems Security*, edited by Rudrapatna K. Shyamasundar, Virendra Singh, and Jaideep Vaidya, 10717:283–300. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-72598-7_17.

Ramanathan, Usha. 2017. 'A Shaky Aadhaar'. *The Indian Express*, March 2017. https://indianexpress.com/article/opinion/columns/aadhar-card-uid-supreme-court-a-shaky-aadhaar-4591671/.

Ramnath, N. S., and Charles Assisi. 2018. *The Aadhaar Effect: Why the World's Largest Identity Project Matters*. Oxford University Press.

Rao, Ursula. 2013. 'Biometric Marginality: UID and the Shaping of Homeless Identities in the City'. *Economic and Political Weekly* 48 (13): 71–77.

———. 2019. 'Population Meets Database: Aligning Personal, Documentary and Digital Identity in Aadhaar-Enabled India'. *South Asia: Journal of South Asian Studies* 42 (3): 537–53. https://doi.org/10.1080/00856401.2019.1594065.

Rao, Ursula, and Vijayanka Nair. 2019. 'Aadhaar: Governing with Biometrics'. *South Asia: Journal of South Asian Studies* 42 (3): 469–81. https://doi.org/10.1080/00856401.2019.1595343.

Saldanha, Alison. 2018. 'From Cheating Banks to Faking Identity, Aadhaar Frauds Peak in 2018: Report'. *Business Standard India*, 3 June 2018. https://www.business-standard.com/article/economy-policy/from-cheating-banks-to-faking-identity-aadhaar-frauds-peak-in-2018-report-118052300151_1.html.

Sarkar, Swagato. 2014. 'The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India'. *Oxford Development Studies* 42 (4): 516–33. https://doi.org/10.1080/13600818.2014.924493.

Satpathy, Tathagata. 2017. 'The Aadhaar: "Evil" Embodied as Law'. *Health and Technology* 7 (4): 469–87. https://doi.org/10.1007/s12553-017-0203-5.

Sen, Srijoni. 2019. 'A Decade of Aadhaar: Lessons in Implementing a Foundational ID System', no. 292: 12.

Siegrist, Michael, George Cvetkovich, and Claudia Roth. 2000. 'Salient Value Similarity, Social Trust, and Risk/Benefit Perception'. *Risk Analysis* 20 (3): 353–62. https://doi.org/10.1111/0272-4332.203034.

Sinha, Amber, and Srinivas Kodali. 2017. 'Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information', May, 31.

Sobti, Shalini, Bhavna Sahni, and Kiran Bala. 2020. 'Surgical Coverage of Cataract in a Rural Area of North India: A Cross-Sectional Study'. *Journal of Family Medicine and Primary Care* 9 (8): 4112. https://doi.org/10.4103/jfmpc.jfmpc_520_20.

Somanchi, Anmol, and Vipul Paikra. 2018. 'Database of Aadhar-Related Forgeries, Fraud'. Google Docs. 2018. https://docs.google.com/spreadsheets/d/1NhVZuQ-wgy-I77iGiFVimL5eWOOPnjH4gA_r0NOM62c/edit?usp=sharing&usp=embed_facebook.

St_Hill. 2019. 'Death of an Aadhaar Holder'. Medium. 17 July 2019. https://medium.com/karana/death-of-an-aadhaar-64fb38be07c8.

Stilgoe, Jack, Richard Owen, and Phil Macnaghten. 2013. 'Developing a Framework for Responsible Innovation'. *Research Policy* 42 (9): 1568–80. https://doi.org/10.1016/j.respol.2013.05.008.

Tomlinson, Hugh. 2017. 'Case Law, India: Puttaswamy v Union of India, Supreme Court Recognises a Constitutional Right to Privacy in a Landmark Judgment – Hugh Tomlinson QC'. Inforrm's Blog. 4 September 2017. https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/.

Totapally, Swetha, Petra Sonderegger, Priti Rao, Jasper Gosselt, and Gaurav Gupta. 2019. 'State of Aadhaar Report 2019. Dalberg, 2019.' 2019. https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf.

Tribune News Service. 2018. 'Challan in Cheating, Forgery Case Points to Aadhaar Data Breach'. Tribuneindia News Service. 2018. https://www.tribuneindia.com/news/archive/challan-in-cheating-forgery-case-points-to-aadhaar-data-breach-575238.

UIDAI, Government of India. 2009. 'Unique Identification Authority of India'. 2009. https://uidai.gov.in/about-uidai/unique-identification-authority-of-india.html.

———. 2019a. 'Authentication Ecosystem - Unique Identification Authority of India'. 2019. https://uidai.gov.in/ecosystem/authentication-ecosystem.html.

———. 2019b. 'Security in UIDAI System'. Unique Identification Authority of India | Government of India. 2019. https://uidai.gov.in/my-

aadhaar/about-your-aadhaar/security-in-uidai-system.html.
———. 2019c. 'Simplified Aadhaar Authentication Ecosystem'. Unique Identification Authority of India | Government of India. 2019. https://uidai.gov.in/ecosystem/authentication-ecosystem/operation-model.html.
———. 2019d. 'About Your Aadhaar'. Unique Identification Authority of India | Government of India. 24 January 2019. https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.
United Nations. 1948. 'Universal Declaration of Human Rights'. 1948. https://www.un.org/en/universal-declaration-human-rights/.
———. 1966. 'OHCHR | International Covenant on Civil and Political Rights'. 1966. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
———. 2019. 'SDG Indicators'. UN Stats. 2019. https://unstats.un.org/sdgs/metadata/?Text=&Goal=16&Target=16.9.
Winner, Langdon. 1980. 'Do Artifacts Have Politics?' *Daedalus* 109 (1): 121–36.
World Bank. 2018. 'Identification for Development'. 2018. https://id4d.worldbank.org/global-dataset/visualization.

Nishant Anand is a PhD student in the department of Science, Technology, Engineering & Public Policy (STEaPP) at University College London. His research investigates the application of responsible governance practices for digital identity systems. He is passionate about understanding the intricate interplay between technology, society and policy.

Acknowledgements – No external funding was provided in preparation for this research.

Disclaimer – No potential conflict of interest was reported by the author.