REPUBLIC OF KENYA

IN THE HIGH COURT OF KENYA AT NAIROBI

CONSTITUTIONAL AND HUMAN RIGHTS DIVISION

PETITION NO. 56 OF 2019

AS CONSOLIDATED WITH PETITIONS 58 & 59 OF 2019

IN THE MATTER OF: ARTICLES 1, 2, 6 (3), 10 (2), 12 (1),19, 21, 31 (c), 22, 24 (1), 27, 29 &118 (1) (b)

OF THE CONSTITUTION OF KENYA 2010;

AND

IN THE MATTER OF: ALLEGED CONTARVENTION OF RIGHTS AND FUNDAMNTAL FREEDOMS UNDER ARTICLES 1, 2, 6 (3), 10 (2), 12 (1), 19, 21, 31 (c), 22, 24 (1), 27, 29&118 (1) (b) OF THE CONSTITUTION OF KENYA, 2010;

AND

IN THE MATTER OF ENFORCEMENT OF THE CONSTITUTION OF KENYA, 2010;

AND

IN THE MATTER OF; SECTIONS 3, 5 & 9 OF THE REGISTRATION OF PERSONS ACT CAP 107;

AND

IN THE MATTER OF THE STATUTE LAW (MISCELLANEOUS AMENDMENT) ACT (No. 18 OF 2018)

BETWEEN

NUBIAN RIGHTS FORUM…….....…… PETITIONER

VERSUS

THE HONOURABLE ATTORNEY GENERAL……..……1ST RESPONDENT

THE CABINET SECRETARY MINISTRY OF INTERIOR & COORDINATION OF NATIONAL GOVERNMENT……..2ND RESPONDENT.

AFFIDAVIT OF DR. THOMAS FISHER OF PRIVACY INTERNATIONAL

I, **DR. THOMAS FISHER** of Privacy International, 62 Britton Street, London, EC1M 5UY, United Kingdom, make oath and state as follows: -

I. INTRODUCTION

1. I am a Research Officer with Privacy International and am authorised to swear this affidavit on behalf of Privacy International (PI) PI was established in 1990 as a non-profit, non-governmental organisation based in London although its work is global. PI works at the intersection of modern technologies and rights. It envisions a world in which the right to privacy is protected, respected, and fulfilled. PI believes that privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right. Privacy International is committed to fighting for the right to privacy for everyone, everywhere. We are building the global movement because people must have access to privacy protection without regard to citizenship, race and ethnicity, economic status, gender, age, or education.

2. Privacy International has been working on issues relating to identification systems since its foundation. The organisation played a notable and influential role in scrutinizing the proposed ID system in the UK from 2002 until 2010. The UK government scrapped the ID system in 2010 after having spent over £257 million and issued 15,000 cards.[1] Privacy International also has a network of partner civil society organisations around the globe, in Latin America, Africa and Asia. As a result, it forms a nexus for critically engaging with identity systems around the world, and is a source of research, educational resources, and

[1] The Guardian, 27th May 2010, *ID cards scheme to be scrapped within 100 days.* https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards

analysis. I am an expert in digital systems and privacy rights.

3. I have worked as a Research Officer at Privacy International since February 2016. I lead Privacy International's work on identity systems, working with an interdisciplinary team of lawyers, technologists, and communication specialists at Privacy International on themes surrounding national identity systems. As part of this, I have conducted research on identity systems in Latin America, Asia, and Africa, and supported research conducted by our partner organisations around the world. I am on the UK government's Privacy and Consumer Advisory Group. I have a PhD from the Centre of African Studies at the University of Edinburgh.

4. Where the contents of this statement are within my knowledge, I confirm that they are true; where they are not, I have identified the source of the relevant information, and I confirm that they are true to the best of my knowledge, expertise and belief.

II. RIGHT TO PRIVACY

5. The right to privacy is a fundamental right enshrined in many constitutions around the world, as well as in international human rights law, including in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

6. The right to privacy is multi-faceted and enables other rights. A fundamental aspect of it, increasingly relevant to people's lives, is the protection of individuals' data. As early as 1988, the UN Human Rights Committee, recognised the need for data protection laws to safeguard the fundamental right to privacy.[2] In 2011, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report similarly noting that "the protection of personal data represents a special form of

[2] U.N. Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, para 10.

respect for the right to privacy."[3]

7. The use of any data by the State including the implementation of an ID system must be done against this backdrop with respect for all fundamental human rights.

8. In understanding the use of data by the state, it is necessary to differentiate some terms. *Civil registration* – including birth registration – is distinct from the concept of *identity systems*. Civil Registration is defined by the United Nation's Department of Economic and Social Affairs:

> "Civil registration is defined as the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements in each country."[4]

9. As was made clear in the analysis by Privacy International on Sustainable Development Goal 16.9 – "By 2030, provide legal identity for all, including birth registration" – this is distinct from a broader identity system that can include features such as unique identification numbers, biometrics, and ID cards[5].

[3] U.N. Doc. A/HRC/17/27, 58 (May 16, 2011).

[4] Annexed hereto and marked as "TF-1" is "United Nations (2014), *Principles and Recommendations for a Vital Statistics System*, Revision 3", also available from: https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf

[5] Annexed hereto and marked as "TF-2" is "Privacy International (2018) *The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?",* also available from https://privacyinternational.org/feature/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk

10. While the benefits of civil registration systems are broadly accepted, identity systems remain a deeply contested domain. As outlined in this affidavit, features of identity systems raise serious concerns for human rights.

II. CONCERNS AND SAFEGUARDS

11. This section highlights some of the concerns that Privacy International has seen emerging from identity systems around the world. Some of these concerns can be partially mitigated by legal, procedural and technological safeguards. As the World Bank's ID4D initiative states: "Identification systems must be underpinned by legal and regulatory frameworks and strong policies that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability."[6]

12. However, it is essential that these mitigations are implemented at the design stage, rather than implemented later. As the ID4D says: "With the rollout of digital identification systems, there is a unique opportunity to ensure that privacy is embedded at the onset into these systems, as opposed to having it be an afterthought, as has been the case in many developed countries."[7]

13. There would be no good reason that a system being implemented today should not learn the lessons from systems around the world, as later implementation will mean that the mitigations are significantly less effective.

14. However, mitigations cannot solve all problems with identity systems, and challenges remain. This statement focusses on particular concerns with identity systems relating to the

[6] ID4D, World Bank (2017) *Principles on Identification for Sustainable Development: Toward the Digital Age:* page 16. Available from: http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf

[7] Annexed hereto and marked as "TF-3" is "ID4D, World Bank (2019) *Privacy by Design: Current Practices in Estonia, India and Austria"* Also available from http://documents.worldbank.org/curated/en/546691543847931842/pdf/132633-PrivacyByDesign-02282019final.pdf

use of biometrics and unique identifiers (as described in Section C below); consequences such as exclusion, data breaches, mission creep, access to and retention of data; and safeguards/ mitigation like data protection.

A. Biometrics

15. Biometrics is the "measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals".[8] Modalities can include fingerprints, iris, facial photographs, vein patters, etc. Key features of the physical body are extracted and stored as an electronic template[9], that is then stored – usually in either a centralised database, or in a smartcard. This template can be used to authenticate the identity of an individual – this is a 1-1 match of the individual against the stored template, to answer the question, "Is this x?". Biometrics can also be used to identify an individual – this is a 1-many match, to answer the question "Who is this?"[10]

16. The use of biometrics presents a unique set of concerns. In 2018, the United Nations High Commissioner for Human Rights issued a Report on the right to privacy in the digital age[11], which highlights significant human rights concerns with the creation of mass databases of biometric data:

> "Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be

[8] Annexed hereto and marked as "TF-4" is "Privacy International (2013) *Biometrics: Friend or Foe of Privacy?"* https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf: page 5

[9] An electronic template is the storing of key, distinct features of a biometric sample. When the individual presents themselves for authentication, their physical features are compared to this template.

[10] Privacy International (2013) *Biometrics: Friend or Foe of Privacy?* https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

[11] Annexed hereto and marked as "TF-5" is "United Nations High Commissioner for Human Rights (2018) *The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29"

used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-base projects without having adequate legal and procedural safeguards in place."[12]

17. Some individuals may have biometric features that make it challenging or impossible to enrol or authenticate an individual, for example manual labourers can have worn fingerprints[13]. In some occasions, it may be inappropriate or privacy invasive to collect facial photographs, for example for those who wear headgear for religious reasons[14], or are part of communities who object to having their photograph taken[15]. Thus, for some, enrolling in a biometric system can be physically impossible or privacy invasive. Risks with exclusion are covered further in Section A below.

18. Another challenge is that biometrics can potentially be used to identify an individual for their entire lifetime. This means that caution has to be shown in the face of changing regimes or political contexts, and also the changes in technology. The technology surrounding biometrics is continually evolving, which places new pressures and risks on

[12] United Nations High Commissioner for Human Rights (2018) *The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29

[13] European Commission (2016) *Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council:* page 105. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0328&from=EN%20page%20207

[14] Council on American-Islamic Relations Research Center (2005) *Religious Accommodation in Driver's License Photographs: A review of codes, policies and practices in the 50 states* Available from: https://moritzlaw.osu.edu/electionlaw/litigation/documents/LWVJ.pdf

[15] The Globe and Mail, July 24th 2009, "Supreme Court Upholds Photo Rules". Available from: https://www.theglobeandmail.com/news/national/supreme-court-upholds-photo-rules/article4280260/

biometric systems. For example, it is possible to clone a fingerprint from a photograph, using commercially-available software[16].

19. Unlike a password, an individual's biometrics cannot be changed. The dissenting judgment from Justice Chandrachud of the Supreme Court of India when ruling on the Aadhaar case recognised that: "Once a biometric system is compromised, it is compromised forever…. Passwords and numbers can be changed, but how does one change the basic biological features that compromise biometrics in the event that there is a theft?" [17]

20. A further issue is that biometrics are essentially probabilistic. Other means of authenticating the individual are deterministic: for example, when a PIN is entered, there is either a match with the stored PIN or there is not. However, biometrics are different. As the UK's National Cyber Security Centre puts it, "However, no two captures of biometric data will produce truly 'identical' results. So, a biometric system must make an *estimation* as to whether two biometric samples come from the same individual."[18] Thus, a biometric system is not making a definitive decision on whether an individual is who he or she claims to be, but rather a probabilistic one. This means that some are going to be excluded from what they are entitled to, or falsely accepted as somebody they are not, as a result.

21. The use of a centralised database for biometrics compounds concerns. In considering the fundamental rights implications of storing biometric data in identity documents and residents cards, the European Union Agency for Fundamental Rights ("FRA") found, "The creation of national dactyloscopic [fingerprint biometric] databases of all identity and residence cards holders would constitute a grave interference with the right to respect for private and family life (Article 7 of the Charter [European Union Charter of Fundamental

[16] BBC News, 29th December 2014, "Politician's fingerprint 'cloned from 'photos' by hacker". Available from https://www.bbc.co.uk/news/technology-30623611

[17] Dissenting judgement of Justice Chandrachud, WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS **,** para 132. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[18] National Cyber Security Centre, *Biometric Recognition and Authentication Systems.* Available from: https://www.ncsc.gov.uk/collection/biometrics?curPage=/collection/biometrics

Rights]) and with the right to protection of personal data (Article 8 of the Charter)."[19]

22. The FRA also found: "The establishment of a central national database would also increase the risk of abuse for using the data for other purposes than those originally intended. Due to its scale and the sensitive nature of the data which would be stored, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights."[20]

Mitigations

23. In recognition of the particular concerns raised by the use of biometrics, consideration should be given to whether the stated purpose could be achieved by a less intrusive approach and any use requires to be accompanied by legal, procedural and technical safeguards.

24. The High Commissioner of Human Rights, recommends that States, *inter alia* "Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim;[21]

[19] Annexed hereto and marked as "TF-7" is "European Union Agency for Fundamental Rights (2018) *Fundamental rights implications of storing biometric data in identity documents and residence cards:* page 14. Available from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf"

[20] European Union Agency for Fundamental Rights (2018) *Fundamental rights implications of storing biometric data in identity documents and residence cards:* page 14. Available from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf

[21] United Nations High Commissioner for Human Rights (2018) *The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29

25. This is emphasised in the U.N. General Assembly Resolution on The Right to Privacy in the Digital Age, "*Noting* the increase in the collection of sensitive biometric information from individuals, and stressing that States must respect their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, considering the adoption of data protection policies and safeguards,"[22]

26. Increasingly data protection laws recognise the need to afford extra protection to biometric data. The following are examples of data protection instruments that recognise the sensitivity of biometric data and require special protections. The Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("Convention 108 +"). Article 6, provides that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law, complementing those of Convention 108 +. The European General Data Protection law ("GDPR"). Article 9, prohibits the processing of biometric data for the purpose of uniquely identifying a natural person subject to limited exceptions. The Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018, Article 5 also provides special protections for biometric data. These additional protections for biometric data are in addition to other safeguards provided for in data protection law as set out below.

27. Another example, of a mitigation for the use of biometrics is to avoid storing the biometric templates in a centralised database, to seek to mitigate the concerns highlighted in above. This may avoid the risks of a system being used for identification, rather than just authentication. It is possible to store biometric data locally – for example, on a smartcard in an individual's possession. As the London School of Economics report on the UK Identity Card, stated, "There is an enormous difference in the implications for the human right to privacy between this type of system, and one where a biometric is only stored locally in a

[22] U.N. Doc. A/RES/73/179 (17 December 2018)

smartcard "[23]. The use of a smartcard alternative to a centralised biometric database is found, for example, in the UK's biometric passport. A biometric facial image is stored on a chip on the passport, and there is no centralised database. This meets the ICAO requirements for a biometric travel document, which does not require a centralised database[24]. Designing systems without a centralised database can also reduce the risk of a major data breach of biometric data, discussed in Section D below.

B. Exclusion

28. One of the concerns of identity systems is that they lead to exclusion: individuals not being able to access goods and services to which they are entitled, thus potentially impacting upon other rights, including social and economic rights. This exclusion as a result of an identification system can come in various forms.

29. Exclusion can impact individuals who are entitled to but not able to get an identification card or number. Privacy International conducted research in Chile, where a single identity number is used for a very broad range of purposes in the public and private spheres. It is required to access state health care, to sign some contracts, and is used as a 'loyalty card' in some shops. Privacy International conducted research, in particular with migrants who were entitled to but not able to get a card, often – as they saw it – because of the pressure that the bureaucracy was under. The research found that as a result these individuals experienced difficulties in accessing state healthcare, change jobs, move house, or even getting married.[25]

30. The exclusion connected to identity cards can take other forms. Even people enrolled onto a biometric system can suffer exclusion. In India, the State of Aadhaar report found that

[23] Annexed hereto and marked as "TF-8" is "LSE (2005) *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*: page 255. Available from: http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf"

[24] House of Commons Library (2010) *Biometric passports parliamentary briefing*. Available from: https://www.statewatch.org/news/2010/jun/uk-biometric-passports-hoc-briefing.pdf

[25] Annexed hereto and marked as "TF-9" is "Privacy International (2018) *Exclusion and identity: Life without* ID Available from: https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id"

Aadhaar-related issues prevented an estimated 2 million people receiving the food subsidy they were entitled to due in three Indian states alone. This included biometric failure in the authentication of individuals; failings in the seeding of Aadhaar numbers; and failings in the connectivity or electricity supply of Point-of-Sale devices[26].

C. Unique identifiers

31. One of the features of many identity systems is the problems emerging from the use of the unique identifier. This is a unique number or code, for example an ID number. It is a feature of an ID system that proves particularly problematic. The 'seeding' of this ID number, across multiple government or private sector databases, provides the risk of providing a "360 degree view" of an individual. This proves a challenge in both the public and private spheres.

32. The linking and seeding of databases with a single number gives the opportunity for all information about an individual, across multiple databases, to be accessed. As a judge in a UK case stated: "[I]f the information obtained by the police, the Inland Revenue, the social security services, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state."[27]

33. Dangers also exist in the use of these unique identifiers by the private sector. It can lead to the exploitation of individuals and their data. As the London School of Economics explained in their report of the UK identity scheme, "Furthermore, service providers and other parties would be able to electronically profile individuals across multiple activities on the basis of

[26] This research is based on state-level representative research in three Indian states in the Indian states of Andhra Pradesh, Rajasthan, and West Bengal.
Annexed hereto and marked as "TF-10" is "IDInsight (2018) *State of Aadhaar Report 2017-18*: pages 24-25. Available from: https://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Report_2017-18.pdf"

[27] Marcel v Commissioner of Police of the Metropolis [1992] Ch 225, 240 (Browne- Wilkinson VC).

the universal electronic identifiers that would inescapably be disclosed when individuals interact with service providers."[28]

34. In the ruling of the Indian Supreme Court on Aadhaar, the section of the Aadhaar Act that allowed private companies to use Aadhaar authentication was declared unconstitutional. The Court found, "Allowing private entities to use Aadhaar numbers will lead to commercial exploitation of an individual's personal data without his/her consent and could lead to individual profiling."[29]

35. There are also new opportunities for fraud presented by the presence of a single ID system. As the report by the LSE states, in the case of someone making use of ID information maliciously, an ID with a limited purpose also limits the harms that can be caused to the individual. However, an ID with a broad purpose presents more opportunities for a malicious actor to act fraudulently: "the damage that identity thieves can cause would no longer be confined to narrow domains, nor would identity thieves be impaired any longer by the inherent slowdowns of today's non-electronic identification infrastructure."[30]

Mitigations

36. An identity system does not have to have a unique, single, persistent identifier or 'identity number' for the citizens enrolled. For example, the UK's Verify.gov system enables a citizen to verify their identity online, for example when accessing government services. This does not involve a single, unique identity number for individuals to authenticate their identities[31],

---

[28] LSE (2005) *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*: page 259. Available from: http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf

[29] WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS **,** para 241. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[30] LSE (2005) *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*: page 259. Available from: http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf

[31] Annexed hereto and marked as "TF-11" is "Whitley, Edgar (2018) *Trusted digital identity provision: GOV.UK Verify's federated approach* Available from: http://eprints.lse.ac.uk/90577/1/Whitley_Trusted%20digital%20ID_2018.pdf

but rather makes use of third-party identity providers that can gave varying levels of assurance that an individual is who that they calim to be.

37. Similarly, in Germany, it is prohibited by law for there to be a unique identification number of general application[3233]. While there are sector-specific identification numbers, the ban on having a general identification number means that it is less likely that any of these will become a de facto general identification number (as seen with social security numbers in the US, see below).

38. Since it was launched in 2009, the Aadhaar system in India has had several important features added. It has undergone design changes that have an impact on the privacy of users of the system. These changes include Virtual ID and tokenisation. The importance of the measures introduced has been emphasised by the Indian Ministry of Electronics and Information Technology. They wrote in Circular 4 of 2018: "It may be noted that Virtual ID, UID Token and Limited E-KYC are crucial for enhancing security and privacy of resident's Aadhaar number and e-KYC data in the Aadhaar authentication eco-system." The World Bank's ID4D also discussed these as being an essential part of having 'privacy by design' in the Aadhaar system[34].

[32] As noted in an article in the Stanford Law Review, "One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as "undesirables") was the extensive repositories of personal data available not only from public sector but also from private sector sources." This, the author emphasises, was not data collected for the purpose of committing genocide; rather, it was the misuse of data collected for other purposes. Pamela Samuelson, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1143 (2000) – Avaialble: http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf

[33] Vandezande, N. (2011), 'Identification numbers as pseudonyms in the EU public sector', European Journal of Law and Technology, Vol. 2, No.2. Available from: http://ejlt.org/article/view/65/142

[34] Also see the world bank report on privacy by design on these improvements. ID4D, World Bank (2019) *Privacy by Design: Current Practices in Estonia, India and Austria* http://documents.worldbank.org/curated/en/546691543847931842/pdf/132633-PrivacyByDesign-02282019final.pdf

39. Virtual ID was introduced in 2018. This is a temporary, revocable 16-digit number that an individual can use instead of their Aadhaar number. An individual can generate a Virtual ID on the UIDAI website, and it can be used in place of the individual's Aadhaar number to access services. The Virtual ID is a tool that seeks to enable people to protect their privacy. It means that the user does not have to give their Aadhaar number to each service provider seeking to verify or authenticate their identity, but rather a temporary number that is possible for the user to change.

40. Tokenisation is related to how an agency stores an individual's data. When an individual uses Aadhaar (or their Virtual ID) for authentication, a unique 72-character token is generated. This is unique to the agency and the Aadhaar number of the individual. This is then stored by the agency, rather than the individual's Aadhaar number. This prevents the linking of databases by different agencies or companies on the basis of the Aadhaar number.

41. These technologies are examples of how Aadhaar has changed to introduce new measures to seek to protect the privacy of the users of Aadhaar. However, the deadline for implementation was pushed back a number of times[35]. Developers were required to make changes to both their frontend clients and their backend applications to make use of the new systems[36]. These challenges and additional costs would have been mitigated if the system had implemented these measures from the start, as this would have possibly both saved the implementation time and money as well as meaning that individual's privacy was more protected in this time.

---

[35] UIDAI (2019) *Compendium of Regulations, Circulars & Guidelines for AUTHENTICATION USER AGENCY (AUA)/E-KYC USER AGENCY (KUA), AUTHENTICATION SERVICE AGENCY (ASA) AND BIOMETRIC DEVICE PROVIDER).* Available from: https://uidai.gov.in/images/resource/Compendium_Feb_2019_11032019.pdf

[36]UIDAI (2019) *Compendium of Regulations, Circulars & Guidelines for AUTHENTICATION USER AGENCY (AUA)/E-KYC USER AGENCY (KUA), AUTHENTICATION SERVICE AGENCY (ASA) AND BIOMETRIC DEVICE PROVIDER).* Available from: https://uidai.gov.in/images/resource/Compendium_Feb_2019_11032019.pdf: page 135

42. In Singapore, the data protection authority notes that the national ID number, the NRIC number, is a "permanent and irreplaceable identifier which can potentially be used to unlock large amounts of information relating to the individual"[37]. The risks include identity fraud and theft. As a result, the authority prohibits the collection, use, or disclosure of NRIC numbers by non-public sector organisations, except when required by law or when it is necessary to identify individuals to a high level of fidelity[38].

43. The design of the Estonian system involves a platform known as X-Road, that allows institutions to exchange data[39]. However, this also enables a system called the Personal Data Usage Monitor that enables citizens to monitor how their data has been used by government departments. A log record is created whenever an individual's data are accessed, and the time-stamped logs enable the citizen to know what government departments have accessed his or her data[40].

D. Data breaches and security

44. To maintain the trust and integrity of a system, it must be kept secure. As illustrated here, breaches associated with identity systems tend to be large in scale, with rectification of the issue either being impossible or incurring a significant cost and affecting individuals in a number of ways, whether identity theft or fraud, financial loss or other damage. The more data and the more sensitive that data, the higher the risk.

---

[37] PDPC (2018) *ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS* available from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf

[38] PDPC (2018) *ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS* available from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf

[39] Republic of Estonia Information Security Authority, *X-Road* Factsheet, available from: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/x-road-factsheet-2014.pdf

[40] ID4D, World Bank (2019) *Privacy by Design: Current Practices in Estonia, India and Austria* http://documents.worldbank.org/curated/en/546691543847931842/pdf/132633-PrivacyByDesign-02282019final.pdf: page 11

45. A data breach of the South Korean ID system, in October 2014, meant that the records of 27 million people - 80% of the population - had their ID details stolen[41].

46. In 2015 the US Government's Office of Personnel Management, which maintains identity and sensitive security clearance information on federal employees, was compromised, with up to 21.5 million peoples' data breached[42]. This included the fingerprint biometric data of 5.6 million US government employees.[43]

47. In March 2016, the Philippines had a breach of over 55 million registered Filipino voters' data following a breach on the Commission on Elections' (COMELEC's) database. The security breach provided access to the COMELEC database that contained both personal and sensitive information, and other information that may be used to enable identity fraud. The personal data included in the compromised database contained fingerprint data, passport information and tax identification numbers.[44]

48. In India there have been numerous reported examples of ways in which the data held by the UIDAI (the authority that runs the Aadhaar scheme and database) and has leaked: through faulty access-points by third parties, or by using patched enrolment software. Many of these are linked to decisions made in the design of the system, including the design of enrolment and the push to encourage its use across the public and private sectors.[45]

---

[41] BBC News, 14th October 2014, *South Korean ID System to be Rebuilt from Scratch,* available from https://www.bbc.co.uk/news/technology-29617196

[42]. Washington Post, 12th June 2015, *Chinese hack of federal personnel files included security-clearance database,* available from: https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html?utm_term=.98fe2c6d23b4

[43] Washington Post, 23rd September2015, *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches

[44] BBC News, 11th April 2016, *Philippines elections hack 'leaks voter data', available from https*://www.bbc.co.uk/news/technology-36013713

[45]The Tribune, 4th Jan 2018, *Rs 500, 10 minutes, and you have access to billion Aadhaar details https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html;*

49. In May 2017, India's Centre for Internet and Society reported that the personal details, including Aadhaar numbers, of potentially 130-135 million Indians were publicly available on government websites, portals and dashboards[46].

50. In January 2018, it was reported that access to the entire Aadhaar database – including the names, addresses, phone numbers, and photographs, but not fingerprint or iris scan data – was being sold for 500 rupees on a WhatsApp group[47].

51. Security failings have also been reported in Estonia. The Estonia government is suing the biometrics company Gemalto for 152 million Euros over alleged security failings in the ID cards that they have supplied[48].

E. Function creep

52. As with any processing and centralisation of data, the mere existence of the data in particular in a centralised identification system could lead to the development of new justifications for its use. This is known as 'mission or function creep'.

53. In 2004, the European Asylum Dactyloscopy Database ("EURODAC") was established to facilitate the application of the Dublin Regulation, which determines the EU Member State

---

ZDNet 23rd March 2018 *A new data leak hits Aadhaar, India's national ID database* https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

[46] CIS (2018) *(Updated) Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information* Available from: https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

[47] The Tribune, 4th Jan 2018, *Rs 500, 10 minutes, and you have access to billion Aadhaar details https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html;*

[48] Reuters, September 27th 2018, *Estonia sues Gemalto for 152 mln euros over ID card flaws* https://www.reuters.com/article/estonia-gemalto/estonia-sues-gemalto-for-152-mln-euros-over-id-card-flaws-idUSL8N1WD5JZ

responsible for examining an asylum application. In 2009, EU Member States proceeded to decide that EURODAC should made accessible for law enforcement purposes in order to fight terrorism, a purpose for which the data processed was never intended, as noted by the European Data Protection Supervisor ("EDPS") in its Opinion on the matter.[49] The EDPS's opinion also raised that the use of EURODAC for law enforcement purposes, and specifically for terrorism, means that a particular vulnerable group in society, namely applicants for asylum, could be exposed to further risks of stigmatisation, even though they are "not suspected of any crime" and "are in need of higher protection because they flee from persecution."[50]

54. Another example of function creep is the USA's Social Security number (SSN). In the USA, the SSN has expanded in purpose. Originally created in 1936 as a number for record keeping within the social security system[51], the use of the number has spread across the public and private sectors, in fields including employment, healthcare, and the private sector. This has led it to become a key concern in the fight against identity theft. As the President's Identity Theft Task Force found in 2007, "The SSN is especially valuable to identity thieves, because often it is the key piece of information used in authenticating the identities of consumers. An identity thief with a victim's SSN and certain other information generally can open accounts or obtain other benefits in the victim's name. As long as SSNs continue to be used for authentication purposes, it is important to prevent thieves from obtaining them."[52] Limiting the use of the SSN became a key recommendation of the President's Identity Theft

[49] European Data Protection Supervisor, Opinions, 2010/C, C92/1, 10 April 2010, . Available here: https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_en.pdf

[50] Annexed hereto and marked as "TF-12" is "European Data Protection Supervisor, Opinions, 2010/C, C92/1, 10 April 2010, paragraph 29. Available here: https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_en.pdf"

[51] Puckett, C (2009) The Story of the Social Security Number in Social Security Bulletin, Vol. 69, No. 2, 2009 https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html

[52] The President's Identity Theft Task Force (2007*) Combating Identity Theft: A Strategic Plan* https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf page 23

Task Force. The Social Security Administration in the US advises treating social security number as confidential information, and to avoid giving it out unnecessarily[53].

55. As illustrated by the case of Aadhaar in India which saw the Supreme Court rule to roll back on the emerging new uses of Aadhaar beyond the original purpose of delivering of subsidies. The Court has required for Aadhaar not be required for some services, including for people applying to get a SIM card for their mobile phone, for opening a bank account, for government grants, and schools, and has imposed limitation on the use by the private sector.[54]

F. Collection, access to and retention of data in the identity system

56. The introduction of an identification system entails the mass collection, aggregation and retention of people's personal data and an interference with the right to privacy. International human rights law thus requires consideration is required as to the legality, necessity and proportionality of any such system and adequate safeguards put in place.

57. These requirements have been examined in a large body of case law, in particular from the European Court of Human Rights[55] and the European Court of Justice[56], that places limits on

[53] Social Security Administration, *Your Social Security Number and Card,* https://www.ssa.gov/pubs/EN-05-10002.pdf

[54] WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS **,** para 241. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf. Paragraph 285, Paragraph 432, Paragraph 322 (c), Paragraph 219 (e) and Paragraph 241

[55] See for example, *Malone v. The United Kingdom*, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984); *Weber and Saravia v. Germany*, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006); *Szabó and Vissy v. Hungary*, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

[56] See for example, *Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12),* Joined Cases, Judgment Court of Justice of the European Union, Grand Chamber (8 April 2014) and *Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al.* (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016).

the collection, interception, access and retention of data. In the case of *S v. Marper,* the European Court of Human Rights found there had been a violation of the right to privacy by the UK, as a result of the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences which failed to strike a fair balance between the competing public and private interests. The Court emphasised:

> "…The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored … The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse …The above considerations are especially valid as regards the protection of special categories of more sensitive data …and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family"[57]

58. Of particular concern and linked to the concept of function creep above, is access by law enforcement and intelligence services to identification system data. Some systems place limitations on the access of the police or security services to the identification databases.

59. In India, Section 33(2) of the Aadhaar Act[58] allowed, for the purpose of national security, access to the Aadhaar database (including biometrics) if authorised by an intelligence officer of Joint Secretary or above. This provision was struck down by the Aadhaar judgment[59].

---

[57] *S. and Marper v. The United Kingdom*, App. Nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment (4 December 2008) , para 103

[58] THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

[59] WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf *Paragraph 219 (c) and (d)*

60. The Philippines has similar restriction. It is not permitted for anyone to disclose, use, give access to or give copies of the information in the database to any third party or entity, including law enforcement entities, national security agencies, or units of the armed forces; the exceptions are when an individual gives prior consent, or if there is a "compelling interest of public health or safety" that is a "risk of significant harm to the public". In that case, an order is required from a competent court, and the individual shall be notified within 72 hours[60].

G. Data Protection law

61. As of January 2019, over 120 countries around the world have enacted comprehensive data protection legislation[61], and numerous countries are in the process of enacting such laws and instruments and frameworks have been introduced by international and regional institutions such as the African Union, the OECD and the Council of Europe. As set out above, data protection is necessary to safeguard the fundamental right to privacy by regulating the processing of personal data: providing individuals with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

62. The need for strong data protection legislation as a pre-requisite for an identification system, is reflected in the Aadhaar judgment: ""We have also impressed upon the respondents, as the discussion hereinafter would reveal, to bring out a robust data

---

WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS **,** para 241. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[60] Implementing Rules and Regulations of Republic Act No. 1105 Otherwise known as the "Philippine Identification System Act". https://psa.gov.ph/system/files/kmcd/IRR%20of%20the%20RA%2011055%20or%20PhilSys%20Law.pdf – Rule 5 Section 21

[61] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (5th Ed 2017) (January 31, 2017). (2017) 145 Privacy Laws & Business International Report, 14-26. Available at SSRN: https://ssrn.com/abstract=2992986, with more added in 2018 and early 2019.

protection regime in the form of an enactment on the basis of Justice B.N. Srikrishna (Retd.) Committee Report with necessary modifications thereto as may be deemed appropriate."[62]

63. A strong comprehensive data protection law will not cure the concerns raised in this statement, but it is an essential safeguard in the introduction of any identification system. A data protection law should provide set out principles and obligations which anyone processing personal data must comply with, together with rights for individuals and clear enforcement and redress.[63]

64. Core data protection principles found in multiple frameworks provide important safeguards to the introduction of an identification system. For example, the principle of purpose limitation in data protection requires that personal data is collected for a specific, explicit and legitimate purpose – this means that it must be clear what data will be used for and collected for one purpose must not be used for another.[64] The principle of data minimisation, for example, requires that data is limited to what is necessary to achieve that stated purpose. Further principles include transparency, fairness, accuracy, and that the data is held not longer than necessary. For example, these principles have been analysed by the EDPS in the context of identity cards in the European Union.[65] Furthermore, data projection law can enshrine rights of individuals to information about how their data is used, access their data, correct their data and more. Data protection law can also impose specific requirements in terms of the security of the data, record-keeping, to build in data

[62] WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS **,** para 241. Available from: https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf Paragraph 219 (f)

[63] Privacy International (2018), *The Keys to Data Protection*, available at: https://privacyinternational.org/report/2255/data-protection-guide-complete

[64] Article 29 Working Party (European Union group of data protection authorities before GDPR) 03/2013 on purpose limitation, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[65] EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, available at: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en_0.pdf

protection by design and default and to assess and mitigate the impact on individuals' rights.

65. I now attach and mark the following documents that I refer to and rely on in my foregoing expert evidence:

TF-1: United Nations (2014), *Principles and Recommendations for a Vital Statistics System,* Revision 3

TF-2: Privacy International (2018) *The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?*

TF-3: ID4D, World Bank (2019) *Privacy by Design: Current Practices in Estonia, India and Austria*

TF-4: Privacy International (2013) *Biometrics: Friend or Foe of Privacy?*

TF-5: United Nations High Commissioner for Human Rights (2018) *The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/29

TF-7: European Union Agency for Fundamental Rights (2018) *Fundamental rights implications of storing biometric data in identity documents and residence cards*

TF-8: LSE (2005) *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*

TF-9: Privacy International (2018) *Exclusion and identity: Life without* ID

TF-10: IDInsight (2018) *State of Aadhaar Report 2017-18*

TF-11: Whitley, Edgar (2018) *Trusted digital identity provision: GOV.UK Verify's federated approach*

TF-12: European Data Protection Supervisor, Opinions, 2010/C, C92/1, 10 April 2010

66. I make this affidavit truthfully to provide the foregoing expert evidence in relation to the Petition by the Nubian Rights Forum and for no other or improper purpose.

Sworn at London by the said

Dr. Thomas Fisher

_____

DEPONENT

This _____day of _____2019

BEFORE ME

NOTARY PUBLIC/ COMMISSIONER FOR OATHS