REPUBLIC OF KENYA

IN THE HIGH COURT OF KENYA AT NAIROBI

CONSTITUTIONAL AND HUMAN RIGHTS DIVISION

PETITION NO. E524 OF 2023

IN THE MATTER OF ARTICLES 1 (1) &(3)(b), 2(1), (2), (5) & (6), 6(3), 10, 12 (1), 19,

20, 21, 73(1) (a) (i), 94, 129, AND 232 (1) OF THE CONSTITUTION

AND

IN THE MATTER OF VIOLATION/THREAT TO VIOLATION OF THE RIGHTS AND

FUNDAMENTAL FREEDOMS UNDER ARTICLE 6(3), 27, 28, 31,32, 35, 43, 47, 53, 56

OF THE CONSTITUTION

AND

IN THE MATTER OF THE BIRTH AND DEATHS (AMENDMENT)

REGULATIONS,2023 (LEGAL NOTICE NO.165 OF 2023)

AND

IN THE MATTER OF THE REGISTRATION OF PERSONS (AMENDMENT)

REGULATIONS,2023 (LEGAL NOTICE NO.164 OF 2023)

AND

IN THE MATTER OF ENFORCEMENT OF THE CONSTITUTION PURSUANT TO

ARTICLE 3(1), 22 (1) & (2) (c), 23(1) & (3), 165 (3) (b) & (d) (i) & (ii) and 258(1) & 2(c).

AND

IN THE MATTER OF THE CONSTITUTION OF KENYA (PROTECTION OF RIGHTS

AND FUNDAMENTAL FREEDOMS) PRACTICE AND PROCEDURE RULES, 2013

BETWEEN

HAKI NA SHERIA INITIATIVE
……...PETITIONER

AND

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

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

DIRECTOR GENERAL OF KENYA CITIZENS AND FOREIGN NATIONALS MANAGEMENT SERVICE…….3RD RESPONDENT

THE PRINCIPAL REGISTRAR OF BIRTHS AND DEATHS……..... 4TH RESPONDENT

THE PRINCIPAL REGISTRAR OF PERSONS……. 5TH 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 Senior 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] PI has also informed the work of global institutions with development of their own principles and

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

guidelines on the use of digital identity including the Council of Europe,[2] OECD[3], and the World Bank[4]. 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 analysis.

3. I am an expert in digital systems and privacy rights. I have worked at Privacy International since February 2016. I have led 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 One Login Inclusion and Privacy Advisory Group (OLIPAG)[5], and was a member of its predecessor bodies the Privacy and Consumer Advisory Group (PCAG)[6] and the Privacy and Inclusion Advisory Forum (PIAF)[7]. I have a PhD from the Centre of African Studies at the University of Edinburgh.

4. In April 2019, I submitted an expert affidavit relating to Petition No. 56 of 2019 as consolidated with Petitions 58 & 59 of 2019 on the validity of the implementation of the National Integrated Identity Management System (NIIMS) in Kenya. My expertise was noted and recognised by the High Court of Kenya on several matters in its final judgment issued on 30 January 2020.[8]

---

[2] Council of Europe, 2023, *Guidelines on National Digital Identity,* page 6, https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html.

[3] OECD, 2023, *Recommendation of the Council on the Governance of Digital Identity*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

[4] ID4D, World Bank, 2021, *Principles on Identification for Sustainable Development: Toward the Digital Age,* https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

[5] UK Government website, *One Login Inclusion and Privacy Advisory Group,* https://www.gov.uk/government/groups/one-login-inclusion-and-privacy-advisory-group.

[6] UK Government website, *Privacy and Consumer Advisory Group,* https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group.

[7] UK Government website, *Privacy and Inclusion Advisory Forum,* https://www.gov.uk/government/groups/privacy-and-inclusion-advisory-forum.

[8] High Court of Uganda, 2019, *Nubian Rights Forum & Others v. The Hon. Attorney General*, Consolidated Petitions No. 56, 58 and 59, para. 876., http://kenyalaw.org/caselaw/cases/view/189189/.

5. In 2022, I submitted an expert affidavit in the High Court of Uganda, relating to the National Identification Registration Authority (NIRA).[9]

6. 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

7. 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.

8. 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.[10] In 2011, the UN 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 respect for the right to privacy."[11]

9. Many of the identity systems adopted by governments are, by their very nature, standardised and large-scale mechanisms by which governments process personal data. Many of the activities which can be core to the functioning of many (but not all) modern government-proposed ID systems – such as mandatory taking and recording of fingerprints[12]– constitute an interference with the right to privacy. Specifically, such measures may interfere with a person's informational privacy, a concept endorsed by Indian and Kenyan courts in the

[9] Privacy International, *ISER & Others v Attorney General of Uganda & Another,* https://privacyinternational.org/legal-action/iser-others-v-attorney-general-uganda-another.

[10] UN Human Rights Committee, 8 April 1988, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, https://www.refworld.org/legal/general/hrc/1988/en/27539.

[11] Human Rights Council, 16 May 2011, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue,* https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

[12] UN Human Rights Committee, 24 March 2021, *Views adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 3163/2018*, para. 7, https://digitallibrary.un.org/record/3970949?v=pdf.

identity litigation context, understood as encompassing the right of control a person has over their personal information.[13]

10. The implications of identity systems on the right to privacy were documented by Privacy International, supported by the International Human Rights Clinic at Harvard Law School,[14] in their analysis of legal arguments explored by national courts around the world. A "Guide to Litigating Identity Systems presents" key legal arguments challenging identity systems because of their impact on the right to privacy as well as surrounding biometric information (which includes iris and fingerprint information), an important component of most identity systems, challenging assumptions of biometric authentication's effectiveness and necessity, and regarding data protection concerns, highlighting the importance of safeguards to protect rights, and pointing to issues around the role of consent, function creep, and data sharing.[15]

11. 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. The OECD's Recommendation of the Council on the Governance of Digital Identity states, "the governance, design and implementation of digital identity systems should be rooted in democratic values and respect for human rights"[16].

12. 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."[17]

---

[13] K.S. Puttaswamy, WRIT PETITION (CIVIL) NO. 494 OF 2012**,** JUSTICE K.S. PUTTASWAMY (RETD.) AND ANOTHER versus UNION OF INDIA AND OTHERS., https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf , para 750.

[14] This guide was developed thanks to the support of the International Human Rights Clinic at Harvard Law School for their support in the research, preparation, and drafting of this guide.

[15] Annexed hereto and marked as "TF-1" is Privacy International, 2020, *A Guide to Litigating Identity Systems,* https://privacyinternational.org/learning-resources/guide-litigating-identity-systems.

[16]Annexed hereto and marked as "TF-2" is OECD, 08 June 2023, *Recommendation of the Council on the Governance of Digital Identity*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

[17] United Nations, 2014, *Principles and Recommendations for a Vital Statistics System*, Revision 3, https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf.

13. 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[18].

14. While the benefits of civil registration systems are broadly accepted, identity systems remain a deeply contested domain. The OECD states, "the deployment of digital identity systems can introduce risks, including fraud, identity theft, and cybercrime, as well as potential threats to human rights, privacy, and data protection"[19]. As outlined in this affidavit, features of identity systems raise serious concerns for human rights.

III. CONCERNS AND SAFEGUARDS

15. 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 I go into below.

16. The document "Principles on Identification for Sustainable Development: Toward the Digital Age" is a set of principles about the development and deployment of ID endorsed by over 20 organisations including the African Development Bank, ID4Africa, the UNHCR, UNDP, United Nations Economic Commission for Africa, and the World Bank Group. These principles state:

> Identification systems must be under-pinned by legitimate, comprehensive, and enforceable legal and regulatory frameworks and strong policies that promote trust in the system; ensure data protection and privacy (including cybersecurity); mitigate abuse such as unauthorized surveillance in violation of due process; are free from discrimination and promote inclusion, particularly for vulnerable or marginalized groups; and ensure accountability.[20]

17. It is essential that these mitigations are implemented at the design stage, rather than implemented later. As the World Bank's Identification for Development (ID4D) initiative

[18] Annexed hereto and marked as "TF-3" is Privacy International, 2018, *The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?,* https://privacyinternational.org/feature/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk.

[19] Annexed hereto and marked "TF-2" is OECD, 2023, *Recommendation of the Council on the Governance of Digital Identity,* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

[20] Annexed hereto and marked "TF-4" is ID4D, World Bank, 2021, *Principles on Identification for Sustainable Development: Toward the Digital Age,* https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

states: "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."[21]

18. 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.

19. However, mitigations cannot solve all problems with identity systems, and challenges remain. This statement focusses on particular concerns with identity systems relating to the use of biometrics and unique identifiers; consequences such as exclusion, data breaches, mission creep, access to and retention of data; and safeguards and mitigations, including data protection.

A. Biometrics

20. Biometrics is the "measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals".[22] Modalities can include fingerprints, iris, facial photographs, vein patterns, etc. Key features of the physical body are extracted and stored as an electronic template[23], 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?"[24]

21. 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[25],

---

[21] Annexed hereto and marked as "TF-5" is 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

[22] Privacy International, 2013, *Biometrics: Friend or Foe of Privacy?,* https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf, page 5

[23] 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.

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

[25] Annexed hereto and marked as "TF-6" is United Nations High Commissioner for Human Rights , 3 August 2018, *The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights*, https://undocs.org/A/HRC/39/29"

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 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.[26]

22. The biometric element of some ID systems is a concern highlighted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), in their Guidelines on National Digital Identity:

> The Preamble in the Explanatory report to the Protocol CETS No. 223 amending the Convention ETS No 108 for the protection of individuals with regard to automatic processing of personal data ('Convention 108+') states that 'human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects.' The increasing incorporation of biometrics into NIDS, that make people 'machine readable' carries the risk of reducing people to a mere object removed from considerations of human dignity and other adverse consequences for their human rights and fundamental freedoms.[27]

23. Furthermore, the use of biometrics is a relevant factor in assessing the degree of interference with the right to privacy and, as a result, the compliance of any existing practice with international human rights law standards. In a decision by the UN Human Rights Committee concerning Mauritius' identity system, the Committee noted:

> Moreover, given the nature and scale of the interference arising out of the mandatory processing and recording of fingerprints, the Committee finds that it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, the storage, including the duration thereof, usage, access for third parties and procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thereby providing sufficient guarantees against the risk of abuse and arbitrariness.[28]

---

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

[27] Annexed hereto and marked as "TF-7" is Council of Europe, 2023, *Guidelines on National Digital Identity,* https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html, page 6.

[28] UN Human Rights Committee, 2018, *Views adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 3163/2018,* https://digitallibrary.un.org/record/3970949?ln=es&v=pdf, para. 7.6.

24. 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[29]. In some occasions, it is privacy invasive to collect facial photographs, for example for those who wear headgear for religious reasons[30], or are part of communities who object to having their photograph taken[31]. Thus, for some, participation in a biometric system may pose physical barriers or infringe upon their privacy or other rights. Risks with exclusion are covered further in Section B below.

25. 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 biometric systems. The development and deployment of facial recognition technologies has been a particular concern of Privacy International, with the associated privacy risks.[32]

26. 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?". [33]

27. 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."[34] Thus, a biometric system is not making a

---

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

[30] 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*, https://moritzlaw.osu.edu/electionlaw/litigation/documents/LWVJ.pdf

[31] The Globe and Mail, 24 July 2009, *Supreme Court Upholds Photo Rule*s, https://www.theglobeandmail.com/news/national/supreme-court-upholds-photo-rules/article4280260/

[32] Privacy International, *Facial Recognition*, https://privacyinternational.org/learn/facial-recognition

[33] Chandrachud, *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* , https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf, para 132

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

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.

28. 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 Rights]) and with the right to protection of personal data (Article 8 of the Charter)."[35]

29. 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.[36]

30. The use of biometrics to authenticate the identities of people can bring about its own exclusions. For instance, in the case of access to healthcare, according to the UNDP, "The use of biometrics, however, can pose significant rights-related risks, since it facilitates the identification of individuals, potentially exposing them to rights violations, especially when individuals belong to stigmatized, marginalized or criminalized groups."[37] Further risks with exclusion are covered further in Section B below.

Mitigations

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

---

[35] Annexed hereto and marked as "TF-8" is European Union Agency for Fundamental Rights, 2018, *Fundamental rights implications of storing biometric data in identity documents and residence cards,* https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf, page 14

[36] European Union Agency for Fundamental Rights, 2018, *Fundamental rights implications of storing biometric data in identity documents and residence cards*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf, page 18

[37] UNDP, 2021, *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes*, https://www.undp.org/sites/g/files/zskgke326/files/2021-07/UNDP-Guidance-on-the-rights-based-and-ethical-use-of-digital-technologies-in-HIV-and-health-programmes-2-EN.pdf

32. The United Nations High Commissioner of Human Rights recommends that States "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".[38]

33. 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".[39]

34. 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.

    a. The Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("Convention 108 +").[40] Article 6 provides that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law.

    b. The EU General Data Protection Regulation ("GDPR").[41] Article 9 prohibits the processing of biometric data for the purpose of uniquely identifying a natural person subject to limited exceptions.

35. It is a recommendation by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) that data controllers for National identity Systems (NIDS) should:

> help ensuring fairness and preventing exclusion when NIDS lawfully require the processing of biometric data for authentication purposes; alternative means of inclusion should be provided for

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

[39] United Nations General Assembly, 21 January 2019, *Resolution adopted by the General Assembly on 17 December 2018 [on the report of the Third Committee (A/73/589/Add.2)],* https://www.concernedhistorians.org/content_files/file/to/ungares129.pdf

[40] Council of Europe, 18 May 2018, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data,* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf

[41] European Parliament and Council, 27 April 2016, *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, https://eur-lex.europa.eu/eli/reg/2016/679/oj

> those individuals who are unable to provide biometrics or whose biometrics are unreadable or whose biometrics become unreadable.[42]

36. 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 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 smartcard"[43]. 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[44]. 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

37. 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.[45]

38. The Secretary General of the United Nations has drawn attention in particular to the risks of exclusion in his report on the role of new technologies for the realisation of economic, social and cultural rights:

> One major concern linked to comprehensive digital identification systems is that these systems can themselves be sources of exclusion, contrary to their purpose. Costly or difficult registration requirements, for example, may prevent poor and disadvantaged populations from fully participating in an identity system. Women in some regions face legal or customary barriers to obtaining official identification. A lack of Internet connectivity, needed for online authentication, also can contribute to exclusion. Older persons and members of some occupational groups

[42] Council of Europe, 2023, *Guidelines on National Digital Identity,* page 6, available from https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html

[43] Annexed hereto and marked as "TF-9" is LSE, 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf, page 255.

[44] House of Commons Library, 2010, *Biometric passports parliamentary briefing*, https://www.statewatch.org/news/2010/jun/uk-biometric-passports-hoc-briefing.pdf

[45] See: Chapter on "Impact of identity systems on rights other than privacy" in: Privacy International, 2020, *A Guide to Litigating Identity Systems,* https://privacyinternational.org/learning-resources/guide-litigating-identity-systems

> performing mostly manual labour may have difficulties providing fingerprints that are clear enough for the purposes of the identify systems. Services that require authentication at the point of delivery create problems for older persons or persons with disabilities who may not be able to travel. Difficulties also arise when the name and gender in identity documentation are not properly reflected in the identity system, exposing people with non-binary gender identity to particular risks. Lastly, exclusion can also result from a particular group being given identity documents that are different from those of others.[46]

39. The Secretary General of the United Nations concluded: "not being able to prove one's identity can severely inhibit, and even effectively block, access to essential services, including housing, social security, banking, health care and telecommunications."[47]

40. When ID is made a requirement to access public services, it becomes relevant to the fulfilment of a State's obligations in relation to economic, social and cultural rights under the International Covenant for Economic, Social and Cultural Rights (ICESCR). When a State Party to the ICESCR (such as Kenya) takes action which furthers or impedes access to social protection, the right to social security (Article 9) is engaged. This right has multiple dimensions which, among others, encompass notions of availability and accessibility.[48] States must ensure that the rights are effectively respected, protected and fulfilled.

41. Where specific groups cannot effectively access ID systems, concerns of discrimination arise. Article 2 of the ICESCR imposes an obligation on State parties to guarantee the rights contained therein "without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

42. The World Bank ID4D's Principles on Identification for Sustainable Development also include the *Inclusion by Design Principle*:

> Identification systems should prioritize the needs and address the concerns of marginalized and vulnerable groups who are most at risk of being excluded and who are the most in need of the protections and benefits identification can provide. This requires working with communities to proactively identify legal, procedural, social, and economic barriers faced by particular groups, risks and impacts specific to these groups, and adopting appropriate technologies and mitigation

---

[46] Annexed hereto and marked as "TF-10" is UN Secretary-General, 2020, *Report on the role of new technologies for the realization of economic, social and cultural rights*, https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural, para 33.

[47] UN Secretary-General, 2020, *Report on the role of new technologies for the realization of economic, social and cultural rights*, https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural, para 30.

[48] Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health*, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=E%2fC.12%2f2000%2f4&Lang=en, para 12.

measures to ensure that new or updated identification systems do not reinforce or deepen existing inequalities.[49]

43. This Honourable Court recognised in the *NRF Case at Paragraph 1012 and 1044,* 30 January 2020, found that "a segment of population" was at risk of exclusion in the introduction of NIIMS and *Huduma Namba*.[50]

44. 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. This research found that migrants 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.[51]

45. An example of groups that may have access to ID documents but can face major obstacles in making use of these documents, is intersex, non-binary and transgender persons. In 2021, PI conducted research on trans people, i.e. people who do not identify with the gender marker they were assigned at birth. As this research on trans people in the Philippines, Argentina and France reveals, this is a group that faces particular issues because their ID documents do not reflect how they present their gender identity. As a result of this, they face difficulties accessing social services, in particular healthcare.[52]

46. In guidance provided by the United Nations Development Program (UNDP) on the use of digital technologies in the healthcare setting, they note: "For people without an officially recognized legal identity (ID) document, accessing basic services, including HIV and health

---

[49] ID4D, World Bank, 2021, *Principles on Identification for Sustainable Development: Toward the Digital Age,* https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[50] The High Court of Kenya at Nairobi, 30 January 2020, *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR ,* Paragraph 1012 and 1044.

[51] Annexed hereto and marked as "TF-11" is Privacy International, 2018, *Exclusion and identity: Life without* ID, https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

[52] Annexed hereto and marked as "TF-12" is Privacy International, 2021, *My ID, My Identity? The impact of ID systems on transgender people in Argentina, France and the Philippines*, https://privacyinternational.org/long-read/4372/my-id-my-identity-impact-id-systems-transgender-people-argentina-france-and

service, can be a major barrier."[53] In particular, the risk of exclusion is present for groups that are already marginalised: "They also pose the risk of excluding already marginalized populations, such as people living with HIV and key populations in criminalized settings, if proper safeguards are not in place to mitigate these risks."[54]

47. Research indicates that the issue of exclusion is closely linked to that of trust, a crucial element of any identity system. Designing a system that is inclusive has benefits not only for those at risk of exclusion, but for other citizens too. In an in-depth piece of research by the UK Department for Science, Innovation and Technology (DSIT) into the development of digital identity services in the UK, members of the public who were participants concluded:

> They call for the public voice to be centred as the primary stakeholder of digital identity services. They describe people should be involved in all aspects of the design, delivery and ongoing decision making on digital identity services. This includes involving people who have experienced barriers to verifying their identity such as prison leavers, asylum seekers and people who do not have a fixed address in the design of digital identity services. If those who have been most excluded from society are included in this process it will be considered more trustworthy. [55]

48. Research in Argentina by Chudnovsky and Peeters into Argentina's National Identity Document (Documento Nacional de Identidad, or "DNI") reveals the challenges and administrative burdens in place for many in obtaining this essential ID document. These are classed as learning costs (a lack of information, or misinformation, about the application procedure); psychological costs (for example, issues of shame and inadequacy around working with bureaucrats); and compliance costs (the costs of time and money, for example, in travelling to get the necessary documents).[56]

49. Exclusion from the DNI creates, in the words of Chudnovsky and Peeters, a "cascade of exclusion", as the exclusion from the ID system also leads to exclusion from social security and benefits. In particular, they highlight the case of the Universal Child Allowance (Asignacion Universal por Hijo (AUH)), a payment given to people who are not in formal

---

[53] United Nations Development Programme, 12 July 2021, *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes,* https://www.undp.org/publications/guidance-rights-based-and-ethical-use-digital-technologies-hiv-and-health-programmes

[54] Idem.

[55] Annexed hereto and marked as "TF-13" is DSIT, 2024, *Public dialogue on trust in digital identity services: a findings report,* https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report

[56] Annexed hereto and marked as "TF-14" is Chudnovsky and Peters, 2021, *A cascade of exclusion: administrative burdens and access to citizenship in the case of Argentina's National Identity Document,* International Review of Administrative Sciences, Volume 88, issue 4., https://journals.sagepub.com/doi/abs/10.1177/0020852320984541

employment and have a child under 18, resident in Argentina, for which both the eligible parent and child are required to hold a DNI. In this case, exclusion from the national ID scheme also involves exclusion from social protection.

50. In Pakistan, the national ID – the Computerised National Identity Card (CNIC) – was held, in 2017, by 96 million out of a population of 210 million citizens. Holding a CNIC is a requirement to access Pakistan's largest social security scheme, the Benazir Income Support Programme (BISP). One of the largest social security schemes in the world, this provides cash transfers to around 4.7 million households in Pakistan. Alongside the eligibility criteria, receiving these funds requires a Computerised National Identity Card (CNIC), Pakistan's national ID card.[57]

51. The challenges of instituting ID as a compulsory requirement to receive benefits were highlighted in research conducted for the UK's Department for International Development. The researchers found: "Possession of a CNIC is required to verify IDs and is essential. It is, however, also an access barrier to the most vulnerable who are more likely not to have a CNIC". Particularly when considering the use of BISP in the case of responses to shock or disaster relief, the research found: "CNIC possession is likely to remain a core eligibility criterion to access any type of disaster relief but, at least at the moment, this criterion is likely to exclude those who need support the most…The biggest hurdle to rapidly accessing relief is the CNIC."[58]

C. Unique identifiers

52. 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'[59] 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.

53. 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 (LSE)

[57] Seyfert and Ahmad, 2020, *Options for making Pakistan's flagship national cash transfer programme shock-responsive* available from https://www.opml.co.uk/files/Publications/A2241-maintains/making-bisp-shock-responsive-14062021.pdf?noredirect=1

[58] *Ibid.*

[59] "Seeding" is the term used to refer to organisations using Aadhaar numbers in their own databases, enabling them to uniquely identify those on the databases.

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 the universal electronic identifiers that would inescapably be disclosed when individuals interact with service providers."[60]

54. 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."[61]

55. 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."[62]

56. Justice Sykes of the Jamaican Supreme Court references the danger of power afforded to the state by the linking of data across state databases under the Jamaican identity system. Justice Sykes quotes scholar Nancy Liu and states when:

> unique identification just from biometric data is combined with a unique identification number is seeded into multiple databases and the use of the unique number is tracked the 'biometric data not only allow individuals to be tracked, but create the potential for the collection of an individual's information and its incorporation into a comprehensive profile by linking various databases together.'[63]

57. This set of concerns is echoed in the OECD's Recommendation of the Council on the Governance of Digital Identity. It is advised that identity systems are designed to "Prevent

---

[60] LSE, 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, https://eprints.lse.ac.uk/684/1/identityreport.pdf, page 259.

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

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

[63] Skyes, Robinson, 2019, *Opinion of Justice Sykes, Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788*

the aggregation of datasets between services or the retention of unnecessary personal data trails being left when users use digital identity solutions to access different services".[64]

Mitigations

58. 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 now-abandoned Verify.gov system enabled a citizen to verify their identity online, for example when accessing government services. This did not involve a single, unique identity number for individuals to authenticate their identities[65], but rather made use of third-party identity providers that gave varying levels of assurance that an individual is who that they claim to be. Verify.gov has been superseded by more recent developments in f digital ID systems in the UK, including the development of systems aimed at the private and public sector, have followed the same set of Principles that governed Verify.gov.[66]

59. 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."[67] The World Bank's ID4D also discussed these as being an essential part of having 'privacy by design' in the Aadhaar system[68].

---

[64] OECD, 2023, *Recommendation of the Council on the Governance of Digital Identity*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

[65] Whitley, Edgar, 2018, *Trusted digital identity provision: GOV.UK Verify's federated approach*, http://eprints.lse.ac.uk/90577/1/Whitley_Trusted%20digital%20ID_2018.pdf

[66] Annexed hereto and marked as "TF-15" is OLIPAG, 2024, *Identity assurance principles for building identity services in government,* https://www.gov.uk/government/publications/identity-assurance-principles-for-identity-services-in-government/identity-assurance-principles-for-building-identity-services-in-government

[67] Ministry of Electronics and Information Technology Unique Identification Authority of India, 01 May 2018, *Circular No. 04 of 2018*, https://dbtbharat.gov.in/data/aadhaar-uidai/Implementation%20of%20VID,%20UID%20token%20and%20Limited%20eKYC%20%E2%80%93%20Announcement%20of%20New%20API%20(Circular%204%20of%202018).pdf

[68] 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,* https://documents1.worldbank.org/curated/en/546691543847931842/pdf/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.pdf

60. Virtual ID is a temporary, revocable 16-digit number that an individual can use instead of their Aadhaar number. Tokenisation, on the other hand, 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 that is stored rather than the individual's Aadhaar number. Such measures are by no means complete solutions to the issues associated with the unique ID number of Aadhaar; implementation was pushed back a number of times[69] and developers were required to make changes to both their frontend clients and their backend applications to make use of the new systems[70]. As a result, the technical mitigations – deemed 'essential' – are better placed during the initial design and roll-out of a system, rather than introduced later.

61. 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"[71]. 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.[72]

62. The design of the Estonian system involves a platform known as X-Road, that allows institutions to exchange data[73]. 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.[74]

---

[69] 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),* https://uidai.gov.in/images/resource/Compendium_Feb_2019_11032019.pdf

[70] *Ibid.,* page 135.

[71] PDPC, 2018, *Advisory Guidelines on The Personal Data Protection Act For Nric And Other National Identification Numbers,* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf

[72] *Ibid.*

[73] 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

[74] 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

63. Another example of alternative forms of ID being accepted in interactions with the government comes from Canada. In Canadian federal elections, voters at the polling station have to prove their identity and address. This can be through a government-issued ID document containing the voter's name, address and photograph; or through two additional methods. First, the voter can provide two pieces of evidence from a long list of sources than include various proofs of identity government, private sector, financial sector, utilities and educational institutions. Many of these do not have a photograph, but must include the voters' name. Finally, a vouching system is in place, where another person who knows the voter can vouch in writing for their identity.[75]

D. Data breaches and security

64. 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 points about the more people, and the more sensitive those data points, the higher the risk.

65. 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[76].

66. 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[77]. This included the fingerprint biometric data of 5.6 million US government employees.[78]

67. 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

---

[75] Annexed hereto and marked as "TF-16" is Elections Canada (n.d.), *ID to vote,* https://www.elections.ca/content.aspx?section=vot&dir=ids&document=index&lang=e

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

[77]Washington Post, 12 June 2015, *Chinese hack of federal personnel files included security-clearance database* 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

[78] Washington Post, 23 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

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.[79]

68. 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) 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.[80]

    a) 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[81]. In January 2018, it was reported that access to the 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[82].

    b) In October 2023, it was reported that the data from Aadhaar and passport records of 815 million Indian citizens were found for sale on the dark web.[83]

E. Function creep

69. 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'.

---

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

[80]The Tribune, 4 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; 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/

[81] CIS, 2018, *(Updated) Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information,* 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

[82] The Tribune, 4 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;*

[83] The Economic Times, *Aadhaar data leak, Personal data of 81.5 crore Indians on sale on dark web: report*, https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

70. In 2004, the European Asylum Dactyloscopy Database ("EURODAC") was established to facilitate the application of the Dublin Regulation, which determines the EU Member State responsible for examining an asylum application.[84] In 2009, EU Member States proceeded to decide that EURODAC data should be made accessible for law enforcement purposes in order to fight terrorism. This purpose was never intended, as noted by the European Data Protection Supervisor ("EDPS") in its Opinion on the matter.[85] The EDPS's opinion also raised that the use of EURODAC for law enforcement purposes, and specifically for terrorism, means that a particularly 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."[86]

71. 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[87], 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.[88]

72. Limiting the use of the SSN became a key recommendation of the President's Identity Theft Task Force. The Social Security Administration in the US advises treating social security numbers as confidential information, and to avoid giving it out unnecessarily.[89]

---

[84] For more information: https://data.europa.eu/data/datasets/eurodac-statistics?locale=en

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

[86] *Ibid.*

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

[88] 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.

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

73. In the case of Aadhaar in India, the Supreme Court ruled to roll back on the emerging new uses of Aadhaar beyond the original purpose of delivering of subsidies. The Court mandated 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 imposed limitations on the use by the private sector.[90]

74. In the Republic of Ireland, the Public Services Card (PSC) is a biometric identity document that is needed for people to claim social benefits in Ireland. In June 2020, the Special Rapporteur on Extreme Poverty and Human Rights wrote to the Irish government about the PSC. He argued that:

> I am concerned that one of the results of this unwieldy process, spread out over more than two decades, and of the lack of flexibility and consultation that has been one of its hallmarks, is that low-income individuals and otherwise marginalised communities, must now contend with formidable barriers to accessing their human right to social protection in Ireland.[91]

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

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

76. These requirements have been examined in a large body of case law, in particular from the European Court of Human Rights[92] and the Court of Justice of the EU[93], which have placed limits on the collection, interception, access and retention of data. In the case of *S. & Marper v UK,* the European Court of Human Rights found there had been a violation of Article 8 of the European Convention on Human Rights, which also guarantees the right to respect for private life. The Court noted that the blanket and indiscriminate nature of the powers of

---

[90] Puttaswamy K.S., *WRIT PETITION (CIVIL) NO. 494 OF 2012, Justice K.S. Puttaswamy (Retd.) And Another Versus Union Of India And Others,* https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf, para 241, Paragraph 285, Paragraph 432, Paragraph 322 (c), Paragraph 219 (e) and Paragraph 241.

[91] Annexed hereto and marked "TF-17" is Alston, Philip, 2020, *Letter from the Special Rapporteur on Extreme Poverty and Human Rights,* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25176

[92] 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)

[93] 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).

retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences 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.[94]

77. 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. For example:

a) In India, Section 33(2) of the Aadhaar Act[95] 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 Indian Supreme Court in its Aadhaar judgment[96].

b) The Philippines has similar restrictions. 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.[97]

---

[94] European Court of Human Rights, 4 December 2008, *S. and Marper v. The United Kingdom*, App, para 103

[95] Ministry of Law and Justice, 26 March 2016, The *Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act*, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

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

[97] Philipine statistics Authority, *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

G. Effective Application of Data Protection law

78. As of May 2023, over 164 countries around the world, including Kenya, have enacted comprehensive data protection legislation[98], and numerous countries are in the process of enacting such laws. Instruments and frameworks have also been introduced by international and regional institutions such as the African Union, the OECD and the Council of Europe.

79. 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.

80. 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 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."[99]

81. Having a strong comprehensive data protection law alone is not sufficient, it must be effectively implemented and enforced in order to serve as an effective safeguard in the introduction of any identification system. Data protection law should provide principles and obligations which entities processing personal data must comply with, together with rights for individuals and clear enforcement and redress.[100]

82. In addition to key data protection principles and obligations and rights of data subject discussed elsewhere in this document, I would like to emphasise the importance of data protection impact assessments.

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

---

[98] Greenleaf, Graham, 10 May 2023, Global Tables of Data Privacy Laws and Bills (8th Ed 2023), 145 Privacy Laws & Business International Report, https://ssrn.com/abstract=4405514

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

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

TF-1 Privacy International (2020) *"A Guide to Litigating Identity Systems",* available from https://privacyinternational.org/learning-resources/guide-litigating-identity-systems

TF-2 OECD (2023) *Recommendation of the Council on the Governance of Digital Identity*" https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

TF-3 "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

TF-5 "ID4D, World Bank (2021) *Principles on Identification for Sustainable Development: Toward the Digital Age:"* page 18. Also available from:

TF-5 "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

TF-6 "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"

TF-7 Council of Europe (2023) *Guidelines on National Digital Identity,* available from https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html

TF-8 "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"

TF-9 "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"

TF-10 "UN Secretary-General (2020) Report on the role of new technologies for the realization of economic, social and cultural rights para 33, available from https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural

TF-11 "Privacy International (2018) *Exclusion and identity: Life without* ID Available from: https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id"

TF-12 Privacy International (2021) *My ID, My Identity? The impact of ID systems on transgender people in Argentina, France and the Philippines* Available from https://privacyinternational.org/long-read/4372/my-id-my-identity-impact-id-systems-transgender-people-argentina-france-and

TF-13 DSIT (2024) *Public dialogue on trust in digital identity services: a findings report* available from https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report

TF-14 Chudnovsky and Peters (2021) "A cascade of exclusion: administrative burdens and access to citizenship in the case of Argentina's National Identity Document" in International Review of Administrative Sciences, Volume 88, issue 4. https://journals.sagepub.com/doi/abs/10.1177/0020852320984541

TF-15 OLIPAG (2024) *Identity assurance principles for building identity services in government* available from https://www.gov.uk/government/publications/identity-assurance-principles-for-identity-services-in-government/identity-assurance-principles-for-building-identity-services-in-government

TF-16 Elections Canada (n.d.) *ID to vote* available from https://www.elections.ca/content.aspx?section=vot&dir=ids&document=index&lang=e

TF-17 Alston, Philip (2020) *Letter from the Special Rapporteur on Extreme Poverty and Human Rights* available from

https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25176

84. I make this affidavit truthfully to provide the foregoing expert evidence in relation to the Petition by Haki na Sheria and for no other or improper purpose.

Sworn at London by the said
Dr. Thomas Fisher

} _____
DEPONENT

This _____day of _____2024

BEFORE ME }

NOTARY PUBLIC/ COMMISSIONER FOR OATHS