REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
PETITION NO. E008 OF 2021
IN THE MATTER OF: ARTICLES 1(1), 1(3)(a) & (b), (2)(1), (2) & (6), 10(1)(a), (b)&(c), 10(2)(a) & (c), 12, 22,29,38,39,53,55, 165 (3)(d) 73, & 258 OF THE CONSTITUTION OF KENYA ,2010;
AND
IN THE MATTER OF ARTICLE 258 OF THE CONSTITUTION OF KENYA, 2010
AND
IN THE MATTER OF ENFORCEMENT OF THE CONSTITUTION OF KENYA, 2010;
AND
IN THE MATTER OF DOUBLE REGISTRATION FACED BY THE MINORITY GROUPS IN KENYA.
BETWEEN
HAKI NA SHERIA INITIATIVE…..…… 1ST PETITIONER
ADAN MIRE DUBLE……2ND PETITIONER
SAHAL ABDI AMIN…….....……3RD PETITIONER
DEKA MUKTAR GURE……..……4TH PETITIONER
AND
THE HONOURABLE ATTORNEY GENERAL..…… 1ST RESPONDENT
THE CABINET SECRETARY MINISTRY OF INTERIOR & COORDINATION OF NATIONAL GOVERNMENT……2ND RESPONDENT
DIRECTOR OF NATIONAL REGISTRATION BUREAU……...3RD RESPONDENT
THE COMMISSIONER FOR REFUGEE AFFAIRS……..4TH RESPONDENT
UNHCR…….……5TH RESPONDENT

AFFIDAVIT OF LAURA LAZARO CABRERA OF PRIVACY INTERNATIONAL

I, **LAURA LAZARO CABRERA** of Privacy International, 62 Britton Street, London, EC1M 5UY, United Kingdom, make oath and state as follows: -

AFFIDAVIT OF LAURA LAZARO CABRERA OF PRIVACY INTERNATIONAL

I, LAURA LAZARO CABRERA of Privacy International, 62 Britton Street, London, EC1M 5UY, United Kingdom, make oath and state as follows:-

I. Introduction

1. I am a Legal Officer with Privacy International and am authorised to swear this affidavit on behalf of Privacy International ("PI"). PI was established in 1990 as non-profit, non-governmental organisation based in London although its work is global. PI works at the intersection of modern technologies and rights. It exposes harms and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. 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. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

2. Privacy International has worked on issues relating to identification systems since its foundation. Since playing a notable and influential role in scrutinising the proposed ID system in the UK from 2002 until 2010 – which was ultimately scrapped after the government spent over £257 million and issued 15,000 cards[1] – PI has taken its work on ID systems to the global stage. Among other work, PI has co-developed a global litigation guide for ID systems in partnership with the Harvard Law School's International Human Rights Clinic,[2] and developed its technical analysis on foundational ID systems.[3] In all of its work, Privacy International draws from the expertise of partner civil society organisations around the globe in Africa, Latin America, and Asia.

3. As a result, PI is at the center of a global network for critically engaging with identity systems, and is a source of research, educational resources, and analysis. On numerous occasions PI has been called as an expert on identity and digital identity issues by the UK government, and entities such as the Council of Europe's Committee of Convention 108, the United Nations Office of the High Commissioner for Human Rights (OHCHR) as well as the United Nations Special Rapporteurs on extreme poverty and human rights and on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

4. In April 2019, PI 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). PI's expertise was noted and recognised by the High Court of Kenya on several matters in its final judgment issued on 30 January 2020.[4]

5. I have worked as a Legal Officer at Privacy International since February 2020. I provide legal support to PI's work on identity systems, working alongside an interdisciplinary team of researchers, technologists, and policy advisors. As part of this, I have both conducted research and delivered trainings on identity systems and their implications for the right to privacy, as well as supported research conducted by our partner organisations around the world. I hold a LLM in Transnational Law from King's College London and I am a member and a scholar of Inner Temple, a professional association for barristers and one of the four Inns of Court in England and Wales. ***(Annexed herewith and marked "LLC1" and "LLC2" are copies of my Curriculum Vitae and Academic Certificates respectively)***

II. Right to privacy in the civil registration context

The concept of informational privacy

[1] Alan Travis, "ID cards scheme to be scrapped within 100 days", The Guardian, 27 May 2020. Available at: https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards
[2] Privacy International, *A Guide to Litigating ID Systems*, September 2020. Available at: https://privacyinternational.org/report/4165/guide-litigating-identity-systems-full-version
[3] Privacy International, *Digital National ID Systems: Ways, Shapes and Forms,* October 2021. Available at: https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms
[4] Nubian Rights Forum and Others v. The Hon. Attorney General, Consolidated Petitions No. 56, 58 and 59 of 2019 [hereafter "Huduma Namba judgment"], para. 876.

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 Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

6. A key dimension of the right to privacy 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.[5] 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."[6]

7. Government identity systems ("ID systems") are, by their very nature, standardised and large-scale mechanisms by which governments process personal data. Accordingly, many of the activities which are core to the functioning of modern government-proposed ID systems – such as mandatory taking and recording of fingerprints[7] – 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 identity litigation context, understood as encompassing the right of control a person has over their personal information.[8]

8. Where provision of an ID, i.e. when one has to show proof of who they say they are, is made a requirement to access social protection services, ID systems will similarly engage economic, social and cultural rights. To the extent that it is often those who are already in precarious socio-economic conditions – such as women, the elderly, asylum-seekers, refugees and stateless persons – who are excluded from accessing ID because of legal, technical or administrative barriers,[9] questions of discrimination on the basis of sex, age, national or social origin may reasonably arise.

Biometrics as sensitive data

9. Government identity systems increasingly propose to use biometrics for identification and verification processes. Biometrics is the "measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals".[10] Examples of biometrics used in the context of ID systems include fingerprints, iris, facial photographs, vein patterns, etc. These biometrics may be

---

[5] UN HRC, *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*, 8 April 1988, para.10. Available at: https://www.refworld.org/docid/453883f922.html

[6] UN Special Rapporteur, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, 58 (16 May 2011). Available at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

[7] UN Human Rights Committee, *Views adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 3163/2018*, 24 March 2021, para. 7.2.

[8] Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters [hereafter "Aadhaar judgment"], para. 83 at 164; Huduma Namba judgment, para. 750.

[9] Privacy International, *Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations*, 29 March 2021. Available at: https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible

[10] Privacy International, *Biometrics: friend or foe of privacy?*, p.5. Available at: https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy

collected from people at the point of registration to an ID system, and may be processed for the purpose of identifying whether the biometrics of a given person is already in the system, i.e. one-to-one verification; verifying whether a presented biometric matches the record of the individual in the system to whom the biometric belongs, i.e. one-to-many verification; and they may also be used, depending on the nature of processing, across other databases, including for forensic purposes. These potential processing uses make the biometric data, and particularly any claims around uniqueness of selected biometrics, particularly sensitive. The potential for secondary processing also increases the risks associated with the processing of biometric data, and any other data in ID systems, for purposes beyond those foreseen and committed to when the ID system was specified, designed, and deployed.

10. The sensitive nature and concerns attaching to biometrics are not only well-documented,[11] but they are also echoed by data protection frameworks, as well as courts around the world. It is typical for data protection legislation to explicitly identify biometrics as a type of personal data warranting higher safeguards.[12] In parallel, courts have on multiple occasions drawn attention to the fallibility and inaccuracy of biometrics,[13] their exclusionary potential,[14] intrusive nature,[15] and permanence.[16]

11. The use of biometrics is a relevant factor in assessing the degree of interference with the right to privacy and, as result, the compliance of any existing practice with international human rights law standards. In a recent decision by the UN Human Rights Committee concerning the Mauritius' identity system, the Committee noted that the "nature and scale of the interference" arising from the mandatory processing and recording of fingerprints was such that it required "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".[17]

The special case of children

(i) Convention on the Rights of the Child

12. When assessing any human rights interference, the age of those affected can be a relevant factor. International treaty law recognises that children deserve a higher standard of protection from both public and private actors. The UN Convention on the

[11] Privacy International, *Expert Affidavit of Dr. Tom Fisher*. Available at: https://privacyinternational.org/legal-action/nubian-rights-forum-and-others-v-attorney-general-kenya
[12] Convention 108 for the protection of individuals with regard to the processing of personal data, Art. 6(1); General Data Protection Regulation, Art. 9(1); South African Protection of Personal Information Act [hereafter "POPIA"], Section 26(1)(a); Australian Privacy Act 1988, Art.6, "Sensitive information:"; Brazilian General Data Protection Regulation, Art.5(II); Colombian Data Protection Law, Art. 5; Egyptian Personal Data Protection Law, Art.1 "Sensitive Personal Data"; Kenyan Data Protection Act 2019, Art. 2, "Sensitive personal data"; Peruvian Data Protection Law, Art. 2(5).
[13] Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788 [hereafter "Robinson judgment"], para.51.
[14] Aadhaar judgment, para. 111 of dissent; Huduma Namba judgment, para. 1012.
[15] Madhewoo v. The State of Mauritius and Anor, 2015 SCJ 177 [hereafter "Madhewoo judgment"], p.23; Aadhaar judgment, paras. 125-26 of dissent; Robinson judgment, para. 55.
[16] Robinson judgment, para. 50; Huduma Namba judgment, para. 880.
[17] UN Human Rights Committee, *Views adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 3163/2018*, para. 7.6.

Rights of the Child ("UN CRC") outlines that the best interests of the child shall be "a primary consideration" in all actions concerning children.[18]

13. The UN CRC specifically protects children's right to privacy.[19] The UN Committee on the Rights of the Child has commented on the risks attaching to "digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification" which "may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives".[20] The UN Committee further notes that any such interference should not only be provided for by law and serve a legitimate purpose, but also "uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child".[21]

14. The UN CRC further states that State Parties undertake to respect the right of the child to preserve his or her identity without unlawful interference.[22]

(ii) Children data protection rights

15. The UN CRC is not the only instrument to accommodate children. International data protection frameworks recognise every individual as a data subject, including children.[23] As such, children are entitled to the full array of data subject rights: access, rectification and erasure. In some cases, it is even recognised that some data subject rights have particular relevance to children. For example, the European Union's General Data Protection Regulation (EU GDPR) states that the right to erasure is relevant in particular "where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data".[24] International standard-setting bodies have taken a stronger approach. Reflecting on the rights of children in the digital environment, the UN Committee on the Rights of the Child notes that "State parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations".[25]

16. Taking into account the special needs of children, domestic data protection frameworks at large restrict or set specific conditions for the processing of children's data. Some states consider data relating to a child to amount to sensitive data;[26] others forbid the processing of children's data altogether unless their data is public.[27] Other restrictions imposed by states include parental consent below a given age,[28]

---

[18] UN Convention on the Rights of the Child [hereafter "UN CRC"], Art. 3(1).
[19] Ibid., Art. 16(1).
[20] UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN. Doc. CRC/C/GC/25/ (2 March 2021), para. 68.
[21] Ibid., para. 69.
[22] UN CRC, Art. 8(1).
[23] GDPR, Art. 4(1); Convention 108, Article 2(a).
[24] GDPR, Recital 65.
[25] UN Committee on the Rights of the Child, *General Comment No. 25*, para. 72.
[26] Ghanaian Data Protection Act 2012, Art.37(1)(a).
[27] Colombian Data Protection Law, Law 1581 of 2012.
[28] E.g. GDPR, Art. 8(1); Egyptian Personal Data Protection Law, Art. 12; Art.7; Paraguayan Data Protection Law No. 6534, Art.21(u); Ugandan Data Protection and Privacy Act 2019, Art.8.

restrictions on profiling,[29] for data protection information to be expressed in clear and plain language that a child can easily understand,[30] and special attention to be provided by supervisory authorities.[31] Domestic data protection legal frameworks in the Commonwealth have similarly incorporated specific protections for children, including by introducing default prohibitions on the processing of children's data in South Africa,[32] and draft provisions requiring children's data to be processed in a manner that protects their rights and best interests in India.[33]

(iii) International jurisprudence making the case for children's vulnerable position in the context of ID systems

17. The special needs of and protections required by children in the data protection context are reflected in international jurisprudence, and particularly in relation to the processing of biometric personal data for civil registration purposes. The consensus is that the compulsory collection of biometrics amounts to a serious interference with children's right to privacy, and accordingly warrants special caution.

18. For instance, the Kenyan High Court has highlighted the importance of asserting the protections applicable to the biometric data collected under the national identity systems particularly with regard to children, "because unlike adults, children's ability to make reasonable choices about what information to share is limited, as a result of their limited capacities, development and education, and they may thus be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[34] The Jamaican Supreme Court has gone even further, noting the unjustifiability and finality of the collection of biometric data from children. Indeed it has noted that "[i]t is one thing to register the birth of a child but quite another to take the biometric information of that child and lock that child into a system with no possibility of opting out. This is such a violation of privacy that there must be strong justification".[35]

19. Children's reduced awareness of the implications of the processing of their data, combined with the long-term consequences of sharing their biometrics even for civil registration purposes, aggravates any resulting interference with right to privacy.

III. Concerns

20. Biometric digital identity systems increasingly mediate the relationship between the individual and State – but also between the individual and international aid. Ensuring that development and humanitarian aid reaches those for whom it is intended is an ongoing priority for funders and international organisations. In the last two decades, development and humanitarian initiatives have begun to integrate digital identity management systems to support and enable programmatic goals with the primary aim

[29] E.g. GDPR, Recital 71.
[30] GDPR, Recital 58; Art. 12(1);
[31] Convention 108, Art. 15(2)(e).
[32] South African POPIA, s. 34.
[33] India Personal Data Protection Bill, Art. 16 (1).
[34] Huduma Namba judgment, para. 820.
[35] Robinson judgment, para. 48.

to ensure assistance is provided to those identified as eligible to receive aid.[36] Some of these systems have included the processing of biometrics with stated purposes including the need to verify recipients' identities to ensure those most eligible receive assistance as well as to tackle fraud and prevent misuse of humanitarian assistance.[37]

21. As it has been widely documented, these have not come without risks. With an increased realisation of the risks associated with the processing of personal data – ranging from exclusion and surveillance to data exploitation and security concerns[38] – and also the complexity of digital identity systems, some initial steps have been taken in recent years in the humanitarian sector to ensure the legal, ethical and responsible use of biometric data to ensure that refugee populations and recipients of development and humanitarian assistance are protected and their rights respected.[39]

22. The use of databases relying on biometrics is increasingly common in the management of refugee and migration flows. The European Union developed EURODAC to hold the fingerprints of all registered asylum-seekers in the EU, and there are current plans to expand the use of migration databases to all travellers.[40] The United Kingdom relies on at least three databases for immigration-related purposes – the Immigration and Asylum Biometric System, the Case Information Database and the Asylum Support System –, with many more government databases being potentially implicated in border control, and more being developed.[41] These are only two examples that PI and its partners have investigated in-depth.

23. When States develop, implement, use and maintain digital identity databases and process biometric data, the path to accountability for any alleged instances of data misuse is clearer as those processes would, or at least should, be regulated and governed by legal frameworks and policies. The accountability and governance of similar processing activities by international development and humanitarian organisations vary and in many instances remain challenging due to a variety of factors.

---

[36] Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action*, 2nd edition, May 2020, Chapter on "Digital Identity", pp 205-2113. Available at: https://www.icrc.org/en/data-protection-humanitarian-action-handbook; Privacy International, Contribution to Global Virtual Summit on digital identity, April 2019. Available at: https://privacyinternational.org/node/2994

[37] Privacy International, *Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, October 2013, pp.28-29.

[38] Privacy International, *Identity*, Topic Page. Available at: https://privacyinternational.org/topics/identity

[39] See for example: Massimo Marelli and Ben Hayes, *Facilitating innovation, ensuring protection: the ICRC Biometrics Policy*, 18 October 2019. Available at: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/; United Nations Office for the Coordination of Humanitarian Affairs (OCHA) - *Centre for Humanitarian Data, Data Responsibility Guidelines*, October 2021. Available at: https://centre.humdata.org/data-responsibility/; Oxfam, *Biometric & Foundational Identity Policy*, June 2021. Available at: https://views-voices.oxfam.org.uk/2021/06/oxfams-new-policy-on-biometrics-explores-safe-and-responsible-data-practice/

[40] Privacy International, *Travel surveillance in the EU*. Available at: https://privacyinternational.org/explainer/4119/travel-surveillance-eu

[41] Privacy International, *The UK's privatised migration surveillance regime: a rough guide for civil society*, February 2021, pp.11-14. Available at: https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf

24. Some humanitarian organisations with international status enjoy specific privileges and immunities.[42] These privileges and immunities may have value as a first line of protection for affected peoples' personal data: for example, they may protect humanitarian organisations from pressure to turn over personal data to authorities or entities who may wish to use the data for purposes different than those for which the data was collected in the first place.[43] However, as a result of those privileges and immunities, compliance of humanitarian organisations with data protection legislation can rarely be scrutinised beyond self-regulation.

25. For many international organisations, that self-regulation comes in the form of a data protection policies[44] and sometimes specific policies on the processing of biometric data.[45] However, as is often the case, such mechanisms are only as good as their enforcement, and as recent allegations reveal, the effectiveness of these internal governance and regulatory mechanisms is not without limits. One of the many examples of harms already reported about the processing of biometric data and digital identity systems in the humanitarian sector includes the recently reported example of how UNHCR collected and shared the personal data of Rohingya individuals with the Bangladesh government – which in turn shared that data with Myanmar – for the process of repatriation without undertaking a full data protection impact assessment and without the informed consent of those whose data was being shared with these third parties.[46]

State obligations in relation to third parties' conduct

26. States' obligations to protect human rights go beyond a negative obligation to refrain from participating in human rights violations and include positive obligations to protect and fulfil human rights. This much is reflected in the language of multiple human rights treaties, which impose on signatory states the obligation not just to respect human rights, but to "ensure", "secure", or alternatively "give effect" to them by adopting legislative or other necessary measures.[47] The positive obligations of the state include the obligation to take appropriate measures against private parties that threaten the enjoyment of human rights. Such obligations coexist with, and must be read in light of, the overriding obligation to take into account the best interests of the child where children are concerned.

---

[42] See, for example, Convention on the Privileges and Immunities of the United Nations, s.2.
[43] Privacy International and International Committee of the Red Cross, *Doing no Harm in the Digital Era*, October 2018, p. 27. Available at: https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf
[44] UNCHR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, May 2015. Available at: https://www.refworld.org/docid/55643c1d4.html; International Organisation for Migration, *Data Protection Manual*, 2010. Available at: https://www.iom.int/data-protection
[45] ICRC, *The Policy on the Processing of Biometric Data*, August 2019. Available at: https://www.icrc.org/en/document/icrc-biometrics-policy
[46] Human Rights Watch, *UN Shared Rohingya Data Without Informed Consent*, 15 June 2021. Available at: https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
[47] African Charter on Human and Peoples' Rights, Art. 1; International Covenant on Civil and Political Rights, Art.2; American Convention on Human Rights, Arts. 1-2; European Convention on Human Rights, Art. 1.

27. The UN Human Rights Committee, reflecting on the nature of positive obligations established by the International Covenant on Civil and Political Rights, stated that such obligations "will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities".[48] Consequently, "there may be circumstances in which a failure to ensure Covenant rights […] would give rise to violations by States Parties of those rights, as a result of States Parties' permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities."[49]

28. The UN Committee on Economic, Social and Cultural Rights (UN CESCR) has similarly highlighted state obligations in relation to the conduct of private parties. While it has referred to these obligations in the context of business activities, its reasoning and approach provide a useful framing for analysing human rights interferences by third-parties at large. In a General Comment addressing this topic, the Committee noted that "State parties may be held directly responsible for the action or inaction of business entities: (a) if the entity concerned is in fact acting on that State party's instructions or is under its control or direction in carrying out the particular conduct at issue […]; (b) when a business entity is empowered under the State party's legislation to exercise elements of governmental authority […]; (c) if and to the extent that the State party acknowledges and adopts the conduct as its own".[50]

29. The UN Human Rights Committee has repeatedly recognised the positive obligations of States to protect against third-party interferences with the right to privacy. Referring to this right, the Committee has stated that in its view, "this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons".[51]

(i) Processing of third-party databases amounts to an interference with the right to privacy

30. States have positive obligations in relation to the personal data contained in databases that they have access to, irrespective of whether or not they contributed to that database. As the UN General Assembly has repeatedly affirmed, "[s]tates must respect international human rights obligations regarding the right to privacy […] when they require disclosure of personal data from third parties, including private companies."[52] Further, "[n]oting the increase in the collection of sensitive biometric

[48] UN Human Rights Committee, *General Comment 31, Nature of the General Legal Obligation on State Parties to the Covenant*, UN Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004), para. 8.
[49] Ibid.
[50] UN CESCR, *General Comment No.24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, E/C.12/GC/24 (10 August 2017). Available at: https://www.refworld.org/docid/5beaecba4.html
[51] UN HRC, *General Comment No. 16: Article 17 (Right to Privacy),* para.1; UN HRC, *General Comment 31*, para. 8.
[52] UN General Assembly Resolution on the Right to Privacy in the Digital Age (A/RES/75/176), 16 December 2020; UN General Assembly Resolution on the Right to Privacy in the Digital Age (A/RES/73/179), 17 December 2018, Preamble.

information from individuals, […] States must respect their human rights obligations […] when collecting, processing, sharing and storing biometric information".

31. This approach is confirmed by international jurisprudence. Existing human rights case-law on the privacy implications arising from the transfer of data from private to public entities is clear that any such transfers must be assessed from the standpoint of the State's positive obligations with regard to the right to privacy.[53]

32. While jurisprudence relating to government liability for the misuse of data by a third party is sparse, some guidance can be derived from the caselaw established by the European Court of Human Rights (thereafter "ECtHR"). Where personal data held by the government is misused by a third-party, the ECtHR jurisprudence has established that the State has a positive obligation to investigate alleged violations of Article 8, even in circumstances where the State is not directly at fault.[54] In any such case, the key question is "whether the national authorities took the necessary steps to ensure effective protection of the applicant's right to respect for his private life and correspondence".[55] In the ECtHR's words, "the positive obligation inherent in the effective respect of private life implies an obligation to carry out effective inquiries in order to rectify the matter to the extent possible".[56]

33. Courts as well as standard-setting bodies have highlighted the obligations incumbent upon States when the processing of children's data is involved. ECtHR jurisprudence, for example, highlights the positive obligation to give effective protection to children when their right to a private life is engaged.[57] The Council of Europe further notes that States "should ensure that the likely impact of intended data processing on the rights of the child is assessed and that the data processing is designed to prevent or minimise the risk of interference with those rights". In relation to biometric data, the Committee cautions that such processing "should in all instances only be allowed where appropriate safeguards are enshrined in law". Further, "States should implement, or require relevant stakeholders to implement, privacy-by-default settings and privacy-by-design measures, taking into account the best interests of the child", and those measures "should integrate strong safeguards for the right to privacy and data protection into devices and services".[58]

ii) Examples of States positive obligations

34. In line with common data protection obligations, existing human rights case law identifies three positive obligations that may be incumbent upon governments when handling a person's data: transparency and access, accuracy and rectification, and erasure.

[53] ECtHR, *López Ribalda and Others v. Spain*, App. No. 1874/13, Judgment, Grand Chamber, 17 October 2019.
[54] ECtHR, *Craxi v. Italy No. 2*, App. No. 25337/94, Judgment, 17 July 2003, paras. 68-76.
[55] Ibid., para. 73.
[56] Ibid., para. 74.
[57] ECtHR, *Guide on Article 8 of the European Convention on Human Rights*, 31 August 2021, para.9.
[58] Council of Europe, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, Recommendation CM/Rec(2018) 7 of the Committee of Ministers,Appendix to Recommendation CM/Rec (2018) 7, paras. 31-32, 35.

35. The rights of a data subject to access, rectify and erase their personal data, as well as the principles of transparency and accuracy, are recognised across data protection systems.[59] In the African continent, at least 10 countries recognise the full array of data subject rights.[60]

36. Transparency is a key data protection principle,[61] and access to one's personal data is a key function of transparency. In its General Comment No. 16, the UN Human Rights Committee noted that, "in order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files".[62] The Organization of American States' Special Rapporteur on Freedom of Expression, further notes that "[i]n cases where entities of the state […] obtain data improperly and/or illegally, the petitioner must have access to that information, even when classified, so that individuals have control over data that affects them.[63]

37. In case law concerning sensitive data processed by public authorities, the ECtHR has found that authorities had a positive obligation to provide those concerned with an effective and accessible procedure to allow them to have access to all relevant information necessary to understand key aspects of their lives, ranging from childhood and early development, exposure to health risks, to files created by defunct totalitarian regimes.[64]

38. Accuracy is another internationally recognised principle to consider.[65] Where data is inaccurate, the outcome of a connected decision-making process will also be inaccurate. For example, there have been documented instances wrongly denied a loan on the basis of inaccurate information which had the effect of lowering their credit score and overall damaging their consumer profile.[66] The harmful effects of inaccurate data have been recognised by human rights jurisprudence, with cases noting that inaccurate information held by the authorities may, in some circumstances,

---

[59] African Union Convention on Cyber Security and Personal Data Protection, Arts. 13, 17 and 19; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, paras.8, 12-13.
[60] Cote d'Ivoire, Ghana, Kenya, Malawi, Morocco, Nigeria, Senegal, Seychelles, South Africa, Tunisia. See Open Government Partnership and ALT Advisory, *Data Protection in Africa: A Look at OGP Member Progress*, August 2021, pp.66-67.
[61] Convention 108, Arts. 4(a), 8; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para.7; GDPR, Art. 5(1)(a).
[62] UN HRC, *General Comment No 16: Article 17 (Right to Privacy)*, para. 10.
[63] OAS Special Rapporteur for Freedom of Expression, *Report on action with respect to Habeas Data and the right of access to information in the hemisphere*, para. 36. Available at: https://www.oas.org/en/iachr/expression/showarticle.asp?artID=570&lID=1
[64] ECtHR, *Gaskin v. United Kingdom*, App. No. 10454/83, 7 July 1989, para. 49; ECtHR, *Roche v. United Kingdom*, App. No. 32555/96, 19 October 2005, para. 162; ECtHR, *Haralambie v. Romania*, App. No. 21737/03, 27 October 2009, paras. 87-89.
[65] Convention 108, Art. 4(d); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para.8; GDPR, Art. 5(1)(d).
[66] Anna Tims, "How credit score agencies have the power to make or break lives", The Guardian, 17 July 2017. Available at: https://www.theguardian.com/money/2017/jul/17/credit-score-angencies-break-lives-lenders-no-mortgage

result in such difficulties in the daily life of a data subject that it may warrant a positive obligation on States to prove the accuracy of the data which has been stored.[67]

39. It follows from the accuracy principle that, where inaccurate data is held by third parties or government entities, it should be open to the data subject to rectify it. Accordingly, the existence of onerous requirements effectively preventing individuals from rectifying their data may constitute an interference with a person's right to privacy. In a case where an individual faced insurmountable procedural barriers to rectify personal data contained in the official State register, the ECtHR ruled that the State had failed to comply with its positive obligation to secure to the complainant the effect respect for his private life.[68]

40. Rectification goes hand in hand with erasure. An individual should have the right to demand that the data controller correct, update, or modify data if it is inaccurate, erroneous, misleading or incomplete. The UN Human Rights Committee has noted, in relation to files held by public authorities to private individuals, "[i]f such files contain incorrect personal data or have been collected or processed contrary to provisions of law, every individual should have the right to request rectification or elimination".[69]

Exclusion arising from shortcomings in ID systems

(i) Challenges when access to services is made conditional on registration in ID systems

41. The potential for ID systems to have exclusionary effect was highlighted by the UN Secretary General. In a report addressed to the Human Rights Council, he notes that "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".[70] Examples of individuals being denied access to services based on their failure to produce proof of ID abound.

42. In India, while the Supreme Court has clarified that beneficiaries of the food rationing system should not be denied their entitlements based on their lack of ID or authentication failure, in practice, beneficiaries continue to be denied food rations on this basis.[71] The UN Special Rapporteur on contemporary forms of racism, reflecting on the unique position of refugees in India in light of the ubiquitous reliance on Aadhaar in order to access services, noted "[b]ecause refugees without residency

---

[67] ECtHR, *Khelili v. Switzerland*, App. No. 16188/07, 18 October 2011, paras. 64, 66-70.
[68] ECtHR, *Ciubotaru v. Moldova*, App. No. 27138/04, 27 April 2010, paras. 51-59.
[69] UN HRC, *General Comment No 16: Article 17 (Right to Privacy)*, para. 10.
[70] UN Secretary General, *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights* [hereafter "The role of new technologies for the realization of economic, social and cultural rights"], A/HRC/43/29 (4 March 2020), para.30. Available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf
[71] Privacy International, *Failures in the digitisation of India's food security programme: the exclusion of married women of Odisha*, 23 March 2021. Available at: https://privacyinternational.org/long-read/4468/failures-digitisation-indias-food-security-programme-exclusion-married-women-odisha; Sameet Panda, *Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during Covid-19*, February 2021. Available at: https://cis-india.org/raw/sameet-panda-jam-trinity-pension-pds-odisha-covid-19

permits are prohibited from holding Aadhaar cards, they are discriminated against and excluded from access to basic services and enjoyment of "rights that ensure a dignified refuge in India".[72]

43. In Uganda, overreliance on the national ID system – known as *Ndaga Muntu* – as a central tool for targeting recipients of a cash grant aimed at senior citizens has resulted in widespread exclusion: research indicated that at least 10,000 potential beneficiaries did not have an ID card, a pre-condition to receive the benefit.[73]

44. In Kenya, individuals report difficulties arising from their inability to obtain ID. In interviews procured by Haki na Sharia and Privacy International, individuals mentioned the lack of ID as an obstacle to access healthcare, birth registration for children, parental access to schools, as well as prison and court access.[74]

(ii) Exclusion need not be intentional for it to be incompatible with human rights obligations

45. When the use of ID as a pre-condition to access government services leads to exclusion, a variety of rights – ranging from civil and political rights to socio-economic rights – may be inadvertently implicated.

46. The majority in India's Supreme Court ruling on Aadhaar, India's ID system, held that Aadhaar could not be made mandatory for admission to schools because the right to education was a fundamental right of children and not a service, subsidy, or benefit under the Aadhaar Act.[75] The dissenting opinion explicitly connected access to state subsidies with the right to food.[76] That dissenting opinion went on to conclude that, if a benefit were to be denied to a person on the basis of a mismatch of biometrics, the right to dignity would be similarly implicated. According to Justice Chandrachud, "[e]xclusion based on technological errors, with no fault of the individual, is a violation of dignity".[77]

47. Turning to the case of Kenya, the UN Special Rapporteur on contemporary forms of racism considered the results of consultations with Kenyan Nubian and Somali communities, which "reported systematic difficulties securing digital identification, which then threatened their ability to access formal employment and other basic needs".[78]

---

[72] UN Special Rapporteur on contemporary forms of racism, *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, A/75/590 (10 November 2020), para. 23. Available at: https://undocs.org/A/75/590

[73] CHR&GJ, ISER and Unwanted Witness, *Chased Away and Left to Die*, June 2021, p. 41. Available at: https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf

[74] Privacy International, *When ID leaves you without identity: the case of double registration in Kenya*, 20 December 2021. Available at: https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya

[75] Aadhaar judgment, para. 332 at 401-402.

[76] Ibid., para. 254 of dissent.

[77] Ibid., para. 262 of dissent.

[78] UN Special Rapporteur on contemporary forms of racism, *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, para. 24.

48. The above examples show that exclusion from ID can implicate internationally recognised rights, including the right to social security, the right to an adequate standard of living (including adequate food), and the right to work.[79] Whether or not an ID system is compatible with these rights is a relevant consideration according to standard-setting bodies. In particular, the UN Human Rights Council has called upon States "to take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place and in full compliance with human rights law".[80]

(iii) The exclusion of population in vulnerable positions must be assessed, addressed and mitigated

49. While judicial consideration of the differentiated impacts of ID-related exclusion on specific communities is incipient, the fact that they exist has already been recognised. In Kenya, the High Court identified that there may be a segment of the population who ran the risk of exclusion, highlighting "a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS".[81]

50. The potential for exclusion has been similarly highlighted by standard-setting bodies. A report by the UN Secretary General highlighted groups commonly vulnerable to exclusion from ID systems, noting the legal and practical obstacles for the poor and disadvantaged, women, older persons, members of some occupational groups, people with disabilities, and people whose name and gender were not properly reflected in the ID system.[82]

51. Where specific groups are excluded from ID systems, concerns of discrimination may also arise. The International Covenant on Economic, Social and Cultural Rights 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".[83]

52. The imperative to pre-empt and monitor any emerging discrimination resulting from ID systems is incumbent both upon public bodies, private actors, and other third parties. The UN Secretary General has explicitly recommended "to integrate ongoing human rights due diligence and broad consultations into the process of developing and deploying comprehensive nationwide digital identification systems, in order to enable the identification and mitigation of human rights risks associated with the systems".[84]

---

[79] International Covenant on Economic, Social and Cultural Rights, Arts. 9, 11, and 6.
[80] UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/HRC/RES/42/15 (26 September 2019), para. 6(m).
[81] Huduma Namba Judgment, para. 1012.
[82] UN Secretary General, *The role of new technologies for the realization of economic, social and cultural rights*, para. 33.
[83] International Covenant on Economic, Social and Cultural Rights, Art. 2(2).
[84] UN Secretary General, *The role of new technologies for the realization of economic, social and cultural rights*, para. 51.

Effective remedies for those excluded from ID systems

(i) Effective remedies must be made available for individuals adversely affected by ID systems

53. There is a general consensus that individuals adversely affected by ID systems should have direct recourse to effective remedies emerging from jurisprudence on the validity and recognition of impact of identity systems on the enjoyment of their fundamental rights and freedoms.

54. The Indian Supreme Court in India, for example, found that a legal provision barring courts from admitting a complaint unless it had been filed by the statutory authority responsible for the ID system was unconstitutional because it barred citizens from seeking judicial remedies for data misuse.[85]

55. In a recent decision against Mauritius, the UN Human Rights Committee considered that the legislation behind its national identity card violated its citizens' privacy rights, as there were insufficient guarantees that the fingerprints and other biometric data stored on the identity card would be securely protected. The Committee noted that such guarantees were a necessary element of any effective remedies to be provided to those affected.[86]

56. A report by the UN Secretary General calls on States to "[c]reate adequate legal frameworks and mechanisms to ensure full accountability in the context of the use of new technologies, including by […] making available avenues for remedies for harm caused by new technologies".[87] The need to ensure redress is also recognised where third-party interferences with human rights are concerned. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Express notes "[t]he duty to provide effective remedies also entails an obligation to protect individuals from acts by private sector entities that cause infringements, by exercising due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities".[88] While the Rapporteur is specifically referring to the private sector, arguably the same reasoning applies to the broad range of activities carried out by third-party entities at large, regardless of their affiliation.

(ii) Minimum characteristics for remedies to be considered effective

57. The assessment of whether an ID system is compliant with the right to privacy is inextricably linked to the availability and quality of remedies that individuals may avail themselves of. Where a violation of the right to privacy is established in connection with the functioning of an ID system, an effective remedy is one which

[85] Aadhaar Judgment, para. 353 at 427.
[86] UN Human Rights Committee, *Views adopted by the Committee under article 5(4) of the Optional Protocol, concerning communication No. 3163/2018*, paras. 7.6, 9.
[87] UN Secretary General, *The role of new technologies for the realization of economic, social and cultural rights*, para. 62(h).
[88] UN Special Rapporteur on Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/41/35 (28 May 2019), para. 39.

allows the individual to obtain redress for the specific violation suffered. However, it is possible to distil the essential elements of effective remedies in the ID context from existing human rights jurisprudence. To be effective, appropriate and relevant, the remedy must be capable of directly remedying the impugned situation.

58. At a minimum, individuals who have been adversely affected by or otherwise excluded from an ID system should have access to an effective recourse to obtain redress for any harm suffered, whether it results from data misuse, design flaws or general malfunctioning of the ID system during implementation. This is consistent with recommendations that States "create opportunities for rights holders, particularly those most affected or likely to suffer adverse consequences, to effectively participate and contribute to the development process […] of new technologies"[89] and that they "further develop […] remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, and children and persons in vulnerable situations or marginalized groups".[90]

59. Specifically, there should be a mechanism available for individuals to complain about any alleged instances of data misuse and demand the situation to be rectified.[91] In a case concerning the disclosure of sensitive data, the ECtHR found that the fact that the alleged data misuse – the unauthorised disclosure of the sensitive data – was ongoing despite the existence of legal remedies, combined with the fact that the affected individual had not received compensation, amounted to a violation of the right to an effective remedy under the European Convention on Human Rights.[92]

60. Where complaint avenues are available to individuals wishing to put forward a data-related grievance, these should be reasonably responsive, adequate, and authorised to rectify the situation. The ECtHR has found, for example, that the effectiveness of remedies requires that applications by data subjects to access to their personal data be processed within a reasonable time.[93] While judicial consideration of the timeliness of the remedy has not extended to the issue of rectification, it can be reasonably concluded that a similar conclusion would be warranted given that rectification, like access, is an established data protection right.

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

62. 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 relevant information, and I confirm that they are true to the best of my knowledge, expertise and belief.

---

[89] UN Secretary General, *The role of new technologies for the realization of economic, social and cultural rights*, para. 47.
[90] UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/HRC/RES/42/15 (26 September 2019), para. 6(h).
[91] ECtHR, *Panteleyenko v. Ukraine*, App. No. 11901/02, 29 June 2006, paras. 82-84.
[92] Ibid.
[93] ECtHR, *Roche v. United Kingdom*, paras. 166-167, 169.