

**THE REPUBLIC OF UGANDA
IN THE HIGH COURT OF UGANDA AT KAMPALA
CIVIL DIVISION
MISCELLANEOUS APPLICATION NO..... OF 2022
(ARISING FROM MISCELLANEOUS CAUSE NO. 86 OF 2022)**

**IN THE MATTER OF AN APPLICATION FOR LEAVE TO INTERVENE AS AMICI
CURIAE BY THE APPLICANTS HEREIN ARISING FROM MISCELLANEOUS
CAUSE NO. 86 OF 2022**

BETWEEN

- 1. COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND
SOUTHERN AFRICA(CIPESA)**
- 2. ACCESS NOW**
- 3. ARTICLE 19: GLOBAL CAMPAIGN
FOR FREE EXPRESSION (ARTICLE 19) =====APPLICANTS**

AND

- 1. INITIATIVE FOR SOCIAL AND ECONOMIC RIGHTS (ISER)**
- 2. THE UNWANTED WITNESS (U) LIMITED**
- 3. HEALTHY EQUITY AND POLICY
INITIATIVE LTD =====APPLICANTS IN THE MAIN CAUSE**

AND

- 1. THE ATTORNEY GENERAL**
- 2. NATIONAL IDENTIFICATION REGISTRATION
AUTHORITY (NIRA) =====RESPONDENTS IN THE MAIN CAUSE**

JOINT AMICUS BRIEF OF ACCESS NOW, ARTICLE 19 AND CIPESA

TABLE OF CONTENTS

1. STATEMENT OF QUESTIONS TO BE ADDRESSED	1
2. TABLE OF AUTHORITIES	2
3. IDENTITY AND INTEREST OF THE AMICUS CURIAE	5
4. STATEMENTS OF EXPERTISE	6
5. ARGUMENTS	8
National digital ID programs impact human rights including the right to privacy, the right to freedom of expression, as well as intersecting economic, social, and cultural rights.	8
i) Right to Privacy	9
ii) Freedom of Expression	17
iii) The relationship between the right to privacy and impact on social, economic and cultural rights	18
6. Conclusion and Recommendations	21

1. STATEMENT OF QUESTIONS TO BE ADDRESSED

This *Amici* seek to provide the Court with additional expertise to address the following questions that have been raised in the Main Cause by the Applicants but not fully canvassed by the respective parties in Miscellaneous Cause 86 of 2022:

1. What is the impact of national digital ID programs on the right to privacy?
2. What is the impact of national digital ID programs on the right to freedom of expression?
3. What is the impact of national digital ID programs on the intersecting economic, social, and cultural rights?

2. TABLE OF AUTHORITIES

Cases

1. *Blas F. Ople v. Ruben Torres and others*, Supreme Court of the Republic of the Philippines, G.R. No. 127685 (1998). Page 13
2. *Julian J. Robinson v. The Attorney General of Jamaica*, Claim No. 2018HCV01788 (2019). Page 11
3. *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177. Page 10,12, and 16
4. *Nubian Rights Forum & Others v. Attorney General & Others*, Consolidated Petitions No. 56, 58 & 59 of 2019, High Court of Kenya at Nairobi (20 January 2020). Page 11 and 12
5. *Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Others*, Writ Petition (Civil) No.494 of 2012, Supreme Court of India (26th September 2018). Pages 9,10,14,15 and 20
6. Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005). Page 10,14,16,17 and 21

Treaties and Conventions

1. African Charter on Human and Peoples' Rights (1 June 1981). Pages 10 and 17
2. African Charter on the Rights and Welfare of the Child, (11 July 1990). Pages 10.
3. African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa (30 April 2019). Page 10
4. American Convention on Human Rights (22 November 1969). Page 10
5. American Declaration of the Rights and Duties of Man (2 May 1948). Page 10
6. Arab Charter on Human Rights (22 May 2004). Page 10
7. European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950). Page 10
8. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (18 December 1990). Page 10
9. International Covenant on Civil and Political Rights (16 December 1966). Page 9 and 17
10. Universal Declaration of Human Rights (10 December. 1948). Page 13

OTHER AUTHORITIES

1. Access Now, “#WhyID: An open letter to the leaders of international development banks, the United Nations, international aid organizations, funding agencies, and national governments,” <https://www.accessnow.org/whyid/>. Page 5
2. Access Now, “Busting the Dangerous Myths of Big ID programs: Cautionary lessons from India,” (5th October, 2021), <https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf>. Pages 20 and 21
3. Access Now, “Data Protection: Why it matters and how to protect it,” (25 January 2018), <https://www.accessnow.org/data-protection-matters-protect/>. Page 15
4. Access Now, “National Digital Identity Programmes: What’s Next?” (May 2018), <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>. Page 17 and 20
5. Anri van der Spuy, “Digital Identity in Uganda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (Towards the Evaluation of Digital ID Ecosystems in Africa: Findings from Ten Countries) [Case study],” (November 2021), Research ICT Africa, <https://researchictafrica.net/publication/digital-identity-in-uganda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/>. Page 18
6. ARTICLE 19, “Kenya: Joint Memorandum asks for Huduma Bill to fully protect rights,” (20 January 2022), <https://www.article19.org/resources/kenya-joint-memorandum-asks-for-huduma-bill-to-fully-protect-rights/>. Page 5
7. Center for Internet and Society, “Governing ID: Principles of Evaluation,” (2 March 2020), <https://cis-india.org/internet-governance/governing-id-principles-for-evaluation>. Page 16
8. Committee on Economic, Social and Cultural Rights, The Right to Social Security, General Comment No. 19: The Right to Social Security (Article 9), E/C.12/GC/19, <https://www2.ohchr.org/english/bodies/cescr/docs/cescr39/E.C.12.GC.19.pdf>. Page 21
9. Human Rights Committee, General Comment No. 28: Article 3 (The Equality of Rights Between Men and Women), (29 March 2000), CCPR/C/21/Rev.1/Add.10, <https://www.refworld.org/docid/45139c9b4.html>. Page 21
10. Human Rights Committee, General Comment No. 35: Article 9 (Liberty and Security of Person), (16 December 2014), CCPR/C/GC/35, <https://www.ohchr.org/en/calls-for-input/general-comment-no-35-article-9-liberty-and-security-person>. Page 10
11. UN General Assembly, Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (3 August 2018), <https://undocs.org/A/HRC/39/29>. Page 9 and 13

12. Office of the UN High Commissioner for Human Rights, International Standards: OHCHR and Privacy in the Digital Age, <https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards>. Page 16
13. UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (17 April 2013), https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. Pages 17 and 18.
14. UN General Assembly, Human Rights Council, Report of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age, (12 September 2021), <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>. Page 13.
15. UN General Assembly, Report of the Special Rapporteur on Extreme Poverty and Human Rights (11 October 2019), UN Doc. A/74/48037, <https://undocs.org/A/74/493>. Pages 20 and 21
16. UN Human Rights Committee, General Comment No. 3: The Nature of States Parties' Obligations (14 December 1990), UN Doc. E/1991/23, <https://www.refworld.org/pdfid/4538838e10.pdf>. Page 17
17. UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (28 December 2009), <https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/a-hrc-13-37.pdf>. Page 13
18. World Bank Group, "Digital ID and the Data Protection Challenge," (October 2019), <http://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf>. Page 8
19. World Bank Group, "ID4D Practitioner's Guide: Version 1.0," (October 2019), <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide>. Page 9

3. IDENTITY AND INTEREST OF THE AMICUS CURIAE

Access Now (www.accessnow.org) is an international non-profit organization that defends and extends the digital rights of people and communities at risk around the world. It was founded in 2009 and registered in the State of California, the United States of America. Through direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, the organization works through staff in more than twenty-five countries to monitor, investigate, and prevent violations of digital rights worldwide. Access Now coordinates the international “#WhyID” campaign,¹ which monitors and decries the impact that ill-considered, badly designed, and poorly implemented digital identity (digital ID) programmes can have on human lives through a global network of civil society organizations, technologists, and academic experts. An important aspect of Access Now’s litigation work involves the selective filing of amicus briefs and expert opinions before national, regional, and international courts and tribunals on points of law of key importance to human rights protection, and on which Access Now’s knowledge of international practice might assist this Honourable Court.

ARTICLE 19 is a Non-Governmental Organization registered in Kenya serving the Eastern Africa region and forms part of ARTICLE 19 global, an international non-profit organization founded in 1987 registered in England and Wales, that works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We use cutting-edge research, innovative campaigns, legal and policy analysis of national laws and submission of expert opinions through amicus briefs to national and regional courts to drive change around the world.² In this regard, we have published numerous research reports on digital rights that provide useful references for various stakeholders, leveraging on our work from our various offices across the World including North Africa, West Africa, the Middle East, Brazil, and South America, Mexico and Central America, South Asia, Europe, and Central Asia, Southeast and East Asia, United States and Canada, to draw comparisons and identify best practices. We also engage with the various international and regional human rights mechanisms on our thematic areas of focus through partnerships, collaboration and through Observer status with mechanisms such as the ACHPR. Over the last 3 years, ARTICLE 19 has been involved in extensive stakeholder consultations with the government of Kenya in the development of the regulatory framework³ to govern the

¹ Access Now, “#WhyID: An open letter to the leaders of international development banks, the United Nations, international aid organizations, funding agencies, and national governments,” <https://www.accessnow.org/whyid/>.

² ARTICLE 19, “What we do,” <https://www.article19.org/what-we-do/>.

³ ARTICLE 19, “Kenya: Joint Memorandum asks for Huduma Bill to fully protect rights,” (20 January 2022), <https://www.article19.org/resources/kenya-joint-memorandum-asks-for-huduma-bill-to-fully-protect-rights/>

implementation of Kenya’s digital ID system in a manner that ensures adequate safeguards on other rights, particularly the right to privacy. A list of ARTICLE 19’s key publications on the subject of biometric identification and privacy, is listed in the Application.

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (www.cipesa.org) works to enable African stakeholders to use ICT to improve governance and livelihoods. We promote internet freedom and governance, civic participation, data governance, the digital economy, digital inclusion and digital resilience. We do this through research and documentation contributing to the availability of information on the policy, legislative and practice environment affecting ICT in Africa; advocacy and stakeholder engagement on threats to free speech, access to information, equal access, privacy and security online and opportunities for technology to advance democratic participation, transparency and accountability in governance and protecting and promoting internet rights; and knowledge and skills development in digital rights policy engagement, digital literacy, digital security, social accountability and human rights monitoring; strategic litigation and movement building. CIPESA is a member of various African and international initiatives that aim to improve the inclusiveness of the Information Society, including the Association for Progressive Communications (APC), Global Network Initiative (GNI) , IFEX and the Alliance for Affordable Internet (A4AI). We also have Observer status with the African Commission on Human and Peoples Rights. CIPESA’s establishment⁴ in 2004 was in response to the findings of the Louder Voices Report for DFID, which cited the lack of easy, affordable and timely access to information about ICT related issues and processes as a key barrier to effective and inclusive ICT policy making in Africa. As such, our work responds to shortage of information, resources and actors consistently working at the nexus of technology, human rights and society.

4. STATEMENTS OF EXPERTISE

ACCESS NOW

Access Now has enormous experience and expertise in the field of digital rights as evidenced by the statement of expertise attached to the application with publications which we consider relevant for the present matter at hand, among others, *Digital Identity: Our five calls to action for the World Bank (2022)*, *The Jamaica NIDS digital identification program: a cautionary tale (2022)* and *Go back to the drawing board: Kenya must scrap unconstitutional Huduma Bill 2021 (2022)*.

⁴ CIPESA, “History,” <https://cipesa.org/about-us/history/>.

ARTICLE 19

In Kenya, over the past three years, ARTICLE 19 has been involved in the consultations around data protection and the regulation of the digital ID system commonly referred to as Huduma Namba. ARTICLE 19 has been involved in extensive stakeholder consultations with the government in the development of the regulatory framework to govern the implementation of the system in a manner that ensures adequate safeguards on other rights, particularly the right to privacy.

ARTICLE 19 has also developed a comprehensive policy on the impacts of the development and deployment of biometric technologies on freedom of expression and other human rights.

As part of their larger work, ARTICLE 19 has conducted extensive research on the impact of emerging technologies on the right to privacy and the applicable human rights standards. In addition, ARTICLE 19's work on biometrics over the last decade has included analysis of the human rights implications of these systems and evidence of their design, development, and deployment in a growing number of domains. These include specific consideration of how these technologies are used for identity verification, identification, surveillance, and inference of attributes, including emotional states and those protected by law. *(See detailed statement of expertise attached to the application and affidavits in support)*

ARTICLE 19 has also extensively engaged regional and international human rights mechanisms on the enforcement of human rights and developments of human rights standards in relation to emerging technologies.

CIPESA

CIPESA has Observer status with the African Commission on Human and Peoples Rights. CIPESA's establishment has conducted research and published several articles on digital ID including *Digital authoritarianism and democratic participation in Africa Brief (2022)*, *State of Internet freedom in Africa 2022: The Rise of Biometric surveillance(2022)*, *Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localization Laws in Africa (2022)*, and *How surveillance, collection of Biometric Data and Limitation of Encryption are undermining privacy Rights in Africa. (See detailed statement attached to the application)*

Thus, the *Amici* are duly registered non-profit organizations with expertise in digital rights and particularly the digital ID systems and their impact on human lives. The *amici* are seeking to intervene in the current proceedings dealing with the digital national identification system in Uganda (Ndaga Muntu) and make submissions on the applicable standards under civil and political rights, such as the right to privacy and freedom of expression, as well as the intersecting social, economic, and cultural rights. In addition, the submission proposes recommendations on

legal safeguards that the Court may require the Respondents to provide in order to mitigate some of the negative human rights impacts.

5. ARGUMENTS

National digital ID programs impact human rights including the right to privacy, the right to freedom of expression, as well as intersecting economic, social, and cultural rights.

1. The term “identity” refers to the set of attributes that uniquely describe an individual.⁵ “Legal identification” (ID) systems collect such attributes, typically core biographic data such as a person’s name, date, and place of birth, in order to register individuals and provide credentials that one can use as proof of the legal identity.⁶ These credentials are essential to applying for governmental benefits and subsidies, verifying real estate ownership, looking for a job, opening a bank account, and qualifying for other essential services. Traditionally, these credentials have taken the form of physical documents such as birth certificates, identity cards, and passports.
2. However, as in Uganda, more countries are leveraging emerging technologies to implement digital ID programs. Such programs have two common features. First, digital ID programs entail the collection, use, and storage of biometric identifiers such as fingerprint, iris, retina, face images, ear shape, voice, DNA pattern, keystroke, or gait, to establish and verify whether an individual matches a certain profile, with some level of confidence. Second, governments are automating the processes of authentication.
3. In general, countries implement digital ID programs in pursuit of multiple interests, such as: closing gaps in identification (thereby facilitating individuals’ access to rights, services, and economic opportunities),⁷ welfare reforms (e.g. more efficient delivery of

⁵ World Bank Group, “ID4D Practitioner’s Guide: Version 1.0,” (October 2019), p. 11, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide>.

⁶ *Id.*, p. 13.

⁷ World Bank Group, “Digital ID and the Data Protection Challenge,” (October 2019), p. 1, <http://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf>.

public services, and fraud and duplication prevention),⁸ crime detection, and national security.⁹

4. However, despite these altruistic motivations, the former UN High Commissioner for Human Rights, Zeid Ra'ad Zeid Al Hussein, warned in his 2018 report on the right to privacy in the digital age about the dangers of such systems that rely on biometric data. According to Zeid, 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,” which is “extremely difficult to remedy and may seriously affect an individual’s rights.”¹⁰
5. Some of the key rights affected by digital ID systems are the rights to privacy and freedom of expression, as well as the intersecting economic, social, and cultural rights, such as the right to education and social security.

i) Right to Privacy

6. The right to privacy is codified in international law through Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which guarantee that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.”¹¹ Uganda ratified the ICCPR in 1995, creating a binding obligation to uphold the right to privacy. Article 27 of the Constitution of Uganda also expressly recognizes the right to privacy.
7. The right to privacy also protects physical privacy—preventing bodies, homes, or private property from intrusion.¹² While the ICCPR does not explicitly refer to the right to

⁸ World Bank Group, “ID4D Practitioner’s Guide: Version 1.0,” (October 2019), p. 5, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide>.

⁹ The Financial Action Task Force, “Guidance on Digital ID in Brief,” (March 2020), <https://www.fatf-gafi.org/media/fatf/documents/reports/Digital-ID-in-brief.pdf>.

¹⁰ UN General Assembly, Human Rights Council, 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, para. 14, <https://undocs.org/A/HRC/39/29>.

¹¹ UN General Assembly, International Covenant on Civil and Political Rights (16 December 1966), Article 17, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

¹² *Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Others*, Writ Petition (Civil) No.494 of 2012, Supreme Court of India (24th August 2017), https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf [hereinafter referred to as *Puttaswamy v. Union of India (Privacy-9j)*]. The Court articulated that “the

bodily integrity, the UN Human Rights Committee has affirmed that the right to privacy includes bodily integrity and autonomy.¹³

8. Various regional and national instruments and jurisprudence further affirm the connections between the human right to privacy, bodily integrity and autonomy, and biometric data. Article 4 of the African Charter on Human and Peoples' rights recognizes the inviolability of humans as well as the right to bodily integrity.¹⁴ Physical privacy is implicated by the compulsory collection of biometric data under digital ID programs. The Supreme Court of Mauritius concluded that the collection of biometric data without consent is a "search of person."¹⁵
9. At the regional level, Article 10 of the African Charter on the Rights and Welfare of the Child, also prohibits arbitrary or unlawful interference with the right to privacy of a child.¹⁶ Article 5 of the African Charter on Human and Peoples' Rights also recognizes the right to human dignity.¹⁷ Privacy has been recognised by national courts in India and Taiwan as forming an important aspect of the right to human dignity.¹⁸

body and the mind are inseparable elements of the human personality," and that privacy extends to the sanctity of the mind as well as of the body as "a private space in which the human personality can develop" (para 168).

¹³ Human Rights Committee, General Comment No. 35: Article 9 (Liberty and Security of Person), (16 December 2014), CCPR/C/GC/35, para. 3, <https://www.ohchr.org/en/calls-for-input/general-comment-no-35-article-9-liberty-and-security-person>; Human Rights Committee, General Comment No. 28: Article 3 (The Equality of Rights Between Men and Women), (29 March 2000), CCPR/C/21/Rev.1/Add.10, para. 20, <https://www.refworld.org/docid/45139c9b4.html>.

¹⁴ Organization of African Unity (OAU), African Charter on the Rights and Welfare of the Child (11 July 1990), CAB/LEG/24.9/49 (1990), Article 5.

¹⁵ *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177, p. 23. Under the program, the enrollment was mandatory for its citizens, and any failure by a citizen to comply with the provisions of the law triggered criminal sanctions. "The coercive taking of fingerprints from the fingers of a person and the extracting of its minutiae would thus clearly fall within the scope of the protection afforded to the integrity and privacy of the person." However, the Court concluded that "such interference is proportionate to the legitimate aim, i.e., prevention of identity fraud."

¹⁶ Similar rights to privacy are provided for in other conventions and instruments including: International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14; American Convention on Human Rights, Article 11; European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8; African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa, Principles 47, 40, 41, and 42; American Declaration of the Rights and Duties of Man, Article 5; Arab Charter on Human Rights, Articles 17 and 21

¹⁷ Organization of African Unity (OAU), African Charter on the Rights and Welfare of the Child, (11 July 1990), CAB/LEG/24.9/49, Article 5, https://www.achpr.org/public/Document/file/English/achpr_instr_charterchild_eng.pdf.

¹⁸ The Taiwanese Supreme Court characterized that "the core values of a free and constitutional democracy are to protect human dignity and respect the free development of personality" and the privacy should be protected "in order to protect human dignity, individuality, and the integrity of personality, as well as to protect the private sphere of personal life from intrusion and self-determination of personal information." Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005), *Puttaswamy v. Union of India* (Privacy-9j). This decision has been explicitly cited by

10. Various UN reports and resolutions have repeatedly confirmed that the right to privacy is essential to the exercise of other rights.¹⁹ According to the Office of the UN High Commissioner for Human Rights, “the right to privacy is central to the enjoyment and exercise of human rights online and offline [...], ranging from freedom of expression and freedom of association and assembly to the prohibition of discrimination and more.”²⁰
11. The right to privacy is implicated in every stage of operation of digital ID programs, from the enrollment to subsequent authentication. Digital ID programs inevitably collect, retain, store, and use both (a) biometric data taken at the time of the enrollment and (b) authentication records and relevant metadata,²¹ which will be subsequently produced and aggregated each time an individual applies for benefits and subsidies and private companies’ services that may require the authentication.²²

Biometric data

12. The collection, retention, and use of biometric data is subject to particularly strict scrutiny by courts which try to gauge whether the interference with fundamental rights is permissible within the human rights framework and whether adequate safeguards exist.²³ This is because, according to the report of the UN High Commissioner for Human Rights, biometric data is “particularly sensitive” as it is “by definition inseparably linked to a

courts in other jurisdictions, e.g., the High Court of Kenya (*Nubian Rights Forum & Others v. Attorney General & Others*, Consolidated Petitions No. 56, 58 & 59 of 2019, High Court of Kenya at Nairobi (20 January 2020), para. 748) and the Supreme Court of Judicature of Jamaica (*Julian J. Robinson v. The Attorney General of Jamaica*, Claim No. 2018HCV01788 (2019), para. 333), in support of the rulings that their digital ID programs were unconstitutional.

¹⁹ E.g., Joseph Cannataci, the former UN Special Rapporteur of the right to privacy, articulated in his 2019 report that the right to privacy is “a right that both derives from and conditions the innate dignity of the person and facilitates the exercise and enjoyment of other human rights.” Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, (Feb. 27, 2019), A/HRC/40/63, para. 52, https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_63.DOCX.

²⁰ Office of the UN High Commissioner for Human Rights, International Standards: OHCHR and Privacy in the Digital Age, <https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards>.

²¹ Metadata provides information about other data, but not its content.

²² In addition to these issues, similarly to traditional centralized ID programs, sharing of data other than biometric data, e.g., identification information or demographic information, will implicate privacy. See, *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177 paras. 361-363.

²³ See, *Nubian Rights Forum & Others v. Attorney General & Others*, Consolidated Petitions No. 56, 58 & 59 of 2019, High Court of Kenya at Nairobi (20 January 2020), para. 767. Kenyan High Court noted the harm from disclosure of DNA that may be caused not just to the data subject but other family members in terms of both identification and genetic information, as well as the risks of indiscriminate collection of genetic information and other biometric identifiers which makes such information susceptible to extraneous use, including negative profiling of individuals for ulterior motives.

particular person and that person's life.”²⁴ As such, it has the potential of being gravely abused.

13. Courts in many countries have recognized privacy violations under digital ID programs based on the potential for abuse of biometric information. For example, Kenyan High Court concluded that “the most important risks [of the centralized storage of the biometric data] are related to the misuse of the biometric data because this is data which are uniquely linked with individuals, which cannot be changed and are universal, and the effects of any abuse or misuse of the data are irreversible. The misuse can result in discrimination, profiling, surveillance of the data subjects and identity theft.”²⁵
14. Mauritius Supreme Court struck down that country's digital ID programs by finding the “overwhelming risk of abuse and misuse [of biometric information]” as “the rapid technological development in the field of information technology, there is “a serious risk that in future the private life interests bound up with biometric information may be adversely affected in novel and unpredictable ways,” therefore the storage and retention of fingerprints for an indefinite period violated privacy.”²⁶

Authentication records and other relevant data

15. A government agency responsible for digital ID programs (an ID agency) provides authentication in response to authentication requests made by various governmental agencies and private entities whose services individuals apply for. Each time individuals apply for services, authentication records are created and aggregated on both sides of an ID agency and requesting entities. Such a dossier includes details of services or transactions applied for, the identity of the requesting entity, result of each authentication, time and location of each application, time of authentication, and so on.
16. Given such an extensive information dossier, the UN High Commissioner for Human Rights expressed concerns about a potential for privacy violation, saying, “big data analytics and artificial intelligence increasingly enable States and private entities to make inferences about their physical and mental characteristics and create detailed personality profiles,” “in order to analyze, profile, assess, categorize and eventually make decisions,

²⁴ UN General Assembly, Human Rights Council, Report of the United Nations High Commissioner for Human Rights (3 August 2018), UN Doc. A/HRC/29/39, para. 14, <https://undocs.org/A/HRC/39/29>. See, also, Council of Europe, Resolution 1797 (2011), para. 1, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17968&lang=en>.

²⁵ Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors. (2020) eKLR, para. 880.

²⁶ *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177, pp. 30-31.

often automated, about them.”²⁷ The dossier of authentication records created under the digital ID programs provides states and private entities with the ability to conduct mass, indiscriminate processing and profiling, exposing people to arbitrary or unlawful surveillance.

17. Further, once an authentication records dossier is transferred and interlinked with other datasets held by governments or private entities without the consent of the ID holder, the risks of functional creep – misuse of collected data for surveillance or profiling purposes, including by law enforcement and security forces – rise even higher.
18. Multiple national courts have struck down digital ID programs based on this risk. In 1995, the Supreme Court of the Philippines concluded that the digital ID programs are not narrowly tailored (therefore unconstitutionally infringe on privacy rights) because, under these programs, all transactions with the government agency will necessarily be recorded, and “[t]he existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist.”²⁸
19. The Human Rights Committee and reports by multiple UN Special Rapporteurs, and UN High Commissioner for Human Rights have emphasized that any restriction on the right to privacy has to meet the three-part test, which requires that such restriction is provided for by law, pursuant to a legitimate aim, and is necessary and proportionate, meaning that the state needs to demonstrate that the actions in question are the least restrictive means to achieve the legitimate aim.²⁹
20. National courts are applying a similar test while evaluating digital ID programs’ effect on the right to privacy and other fundamental rights. For example, the Judicial Yuan of Taiwan required that digital ID programs must “be explicitly prescribed by statute and use less intrusive means which are substantially related to an important public interest,” due to fingerprints’ particularly high linkability with other datasets (which enables

²⁷ UN General Assembly, Human Rights Council, 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, para. 15, <https://undocs.org/A/HRC/39/29>.

²⁸ *Blas F. Ople v. Ruben Torres and others*, Supreme Court of the Republic of the Philippines, G.R. No. 127685 (1998).

²⁹ UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (28 December 2009), para.11, <https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/a-hrc-13-37.pdf>; UN General Assembly, Human Rights Council, Report of the United Nations High Commissioner for Human Rights The right to privacy in the digital age, (12 September 2021), UN Doc. A/HRC/48/3, para. 39, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>.

surveillance) as fingerprints are unique and permanent, and traces of fingerprints are left when a person touches an object.³⁰

21. The Court also concluded that “[t]he failure [...] to explicitly specify the purpose of mandatory collection and storage of fingerprint information in itself violates the constitutional protection of an individual’s information privacy” because “it is imperative for a statute to clearly specify the purpose for collection of information” because it “is the only way that individuals can know, ex ante, the purpose for the [data collection] and how the State plans to use it, in order to ascertain [the data is used] in a way that is consistent with the purpose specified by law.”³¹
22. In 2020, the Kenyan High Court struck down its digital ID program holding that “a law that affects a fundamental right or freedom should be clear and unambiguous” and “the lack of a comprehensive legislative framework when collecting personal data [...] is contrary to the principles of democratic governance and the rule of law, and thereby unjustifiable.”³²
23. In 2018, in response to claims regarding the world’s largest biometric identification program, “Aadhaar,” the Supreme Court of India struck down a part of the Aadhaar Act – Section 57, which allowed private entities to use Aadhaar number pursuant to “any contract to this effect” because any privacy violation should be backed up by law, and any “contract” cannot be treated as a law.³³
24. Courts have also struck down digital ID programs due to the lack of necessity and proportionality. In 2005, The Judicial Yuan of Taiwan reasoned that the program was not the least intrusive means to achieve a state interest, noting that “existing information, other than fingerprints, can accurately verify a person’s identity, the collection of fingerprints is not substantially related to the purpose of preventing false applications for identity cards.”³⁴ The same Court concluded that fraud prevention can be achieved by

³⁰ Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005). The Supreme Court of the Philippines struck down its digital ID programs by using a similar test: “it is the burden of government to show that A.O. No. 308 is justified by some compelling state interest and that it is narrowly drawn.” *Blas F. Ople v. Ruben Torres and others*, Supreme Court of the Republic of the Philippines, G.R. No. 127685 (1998).

³¹ Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005).

³² *Nubian Rights Forum & Others v. Attorney General & Others*, Consolidated Petitions No. 56, 58 & 59 of 2019, High Court of Kenya at Nairobi (20 January 2020), para. 921.

³³ *Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Others*, Writ Petition (Civil) No.494 of 2012, Supreme Court of India (26th September 2018), para. 447(4)(h), [hereinafter referred to as Puttaswamy v Union of India (Aadhaar)], https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf.

³⁴ Judicial Yuan Interpretation No. 603, para. 12.

combining anti-counterfeiting measures and existing information on the face of the existing identity card, such as photos.³⁵ In the Aadhaar decision of the Indian Supreme Court, referenced above, the Court also found that an identity system that resulted in the violation of the right to education could not be considered proportionate.³⁶

25. Data protection is a fundamental right that is closely related to the right to privacy.³⁷ It refers to the practices, safeguards, and binding rules put in place to protect individuals' personal information and ensure that they remain in control of it.³⁸ The UN Special Rapporteur on the right to privacy wrote in her July 2022 report that, "upholding the right to the protection of personal data, which is recognized as a right that enables the protection of other rights will ensure that the proper processing of data concerning an individual will, in turn, guarantee respect for his or her other fundamental rights."³⁹ This assertion finds support in the UN General Assembly resolution, "The Right to Privacy in the Digital Age" passed by consensus in its 75th session.⁴⁰

26. Article 5 of the European Union's General Data Protection Regulation (GDPR), which sets out key principles at the heart of data protection regimes around the world, identifies the following principles of data protection: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.⁴¹

27. Under Ugandan law, data protection is governed by the Data Protection and Privacy Act, 2019. The Ugandan digital ID system came into force in 2015 through the Registration of

³⁵ *Id.*

³⁶ *Puttaswamy v. Union of India* (Aadhaar), para 325.

³⁷ Charter of Fundamental Rights of the European Union, (26 October 2012), 2012/C 326/02, Articles 7, 8, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

³⁸ Access Now, "Data Protection: Why it matters and how to protect it" (25 January 2018), <https://www.accessnow.org/data-protection-matters-protect/>

³⁹ UN General Assembly, Report of the UN Special Rapporteur on the Right to Privacy (20 July 2022), A/77/196, para. 14, <https://undocs.org/Home/Mobile?FinalSymbol=A%2F77%2F196&Language=E&DeviceType=Desktop&LangRequested=False>

⁴⁰ UN General Assembly, Resolution on the Right to Privacy in the Digital Age (28 December 2020), A/RES/75/176, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement>: "Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association and the right to freedom of religion or belief and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale."

⁴¹ European Parliament, General Data Protection Regulation (27 April 2016), Article 5, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Persons Act, prior to the enactment of any legal framework on digital protection. The Data Protection and Privacy Act identifies similar principles to the GDPR. Ugandan data protection law, as the GDPR, also requires consent of the data subject for collecting or processing of personal data.

28. Digital ID systems, such as the one in Uganda, raise concerns about data minimisation, consent, access to information and robust security safeguards to minimize the risks to privacy arising from possible breaches of the system or unauthorized access. Being a centralized system, there is even greater consequence in case of a breach. The information required at registration under such systems is often quite extensive, which contradicts the principle of minimization.
29. Digital ID programs often permit sharing of biometric data collected under them with different governmental agencies (or even private parties), especially law enforcement agencies, for the purposes of national security, crime prevention, compliance with judicial orders, and other reasons detached from the purpose of the ID system itself.⁴² Registered persons have little agency or power to decide which information is accessed at any particular point for a particular service, and are not always informed of the access to their personal data. When access, transfer, and use of biometric information occurs without the consent of the ID holder, an individual's right to privacy is violated.⁴³ Further, such data sharing would result in the interlinking with different datasets, providing states with mass surveillance and profiling capacity.⁴⁴
30. For example, the Mauritius Court found that the state's digital ID programs violated the right to privacy as such programs made biometric information readily available to third

⁴² Center for Internet and Society, "Governing ID: Principles of Evaluation," (2 March 2020), p. 7, <https://cis-india.org/internet-governance/governing-id-principles-for-evaluation>.

The Aadhaar (Sharing of Information) Regulations 2016 placed no restrictions on the sharing or use of demographic or biometric data (except core biometric data). Section 29 (4) gives the UIDAI wide latitude to "publish, display or post publicly" Aadhaar numbers, demographic data, or photographs for purposes specified in regulations.

⁴³ See, e.g., *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177, p. 23 (finding that the collection and centralized storage of fingerprint data as part of a national identity card scheme implicated the right to privacy as codified in the Mauritian Constitution); and Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005).

⁴⁴ As an example of the privacy concern of data sharing among multiple government agencies, the Singapore government shared Covid-19 contact-tracing app with criminal law enforcement agencies, contrary to the initial purpose of the Covid-10 app. Al Jazeera, "COVID app triggers overdue debate on privacy in Singapore" (10 February 2021), <https://www.aljazeera.com/news/2021/2/10/covid-app-triggers-overdue-debate-on-privacy-in-singapore>

parties often without judicial control.⁴⁵ National digital ID programs in Estonia and Tunisia have also been raising concerns for data protection, among other issues.⁴⁶

31. Under Ugandan law, biometric data is not recognised as part of the special personal data as defined under Section 9 of the Data Protection and Privacy Act, 2019 and therefore there are no additional obligations to safeguard the handling and processing of such data.

ii) Freedom of Expression

32. Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) guarantees the right to freedom of expression.⁴⁷

33. Similarly to the right to privacy, any restriction on the right to freedom of expression has to meet the three-part test, which requires that any restriction is provided by law, is pursuant to a legitimate aim, and is necessary and proportionate to achieving that legitimate aim.⁴⁸

34. Regional instruments also codify the right to freedom of expression, including Article 9 of the African Charter on Human and Peoples' Rights.⁴⁹ Freedom of expression is also protected under Article 29 of the Ugandan Constitution.

35. As David Kaye, the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted in 2015, anonymity, is “the condition of avoiding identification,” creates a crucial “zone of privacy” that enables people to “hold opinions and exercise freedom of expression without arbitrary or unlawful interference or attacks.”⁵⁰

⁴⁵ *Madhewoo v. The State of Mauritius and Anor*, 2015 SCJ 177, p. 33.

⁴⁶ Access Now, “National Digital Identity Programmes: What’s Next?” (May 2018), <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>

⁴⁷ UN General Assembly, International Covenant on Civil and Political Rights (16 December 1966), Article 19, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

⁴⁸ UN General Assembly, Human Rights Committee, General Comment No. 34, Article 19, Freedoms of Opinion and Expression (12 September 2011), UN Doc. CCPR/C/GC/34, para. 22, <https://undocs.org/CCPR/C/GC/34>; UN General Assembly, Human Rights Committee, General Comment No. 37, Article 21, Freedoms of Opinion and Expression (17 September 2020), UN Doc. CCPR/C/GC/37, para. 40, <https://undocs.org/CCPR/C/GC/37>.

⁴⁹ African Charter on Human and Peoples' Rights, (21 October, 1986), <https://au.int/en/treaties/african-charter-human-and-peoples-rights>.

⁵⁰ UN General Assembly, Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (17 April 2013), UN Doc. A/HRC/23/40, para. 19, https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

36. However, digital ID programs, which create datasets of biometrics information and authentication records dossier, and enable interlinking these with other datasets, deprive people of anonymity, resulting in producing a population-wide chilling effect.
37. Even if states do not leverage their databases to actively monitor their citizens, the possibility or perception of surveillance “makes people cautious of what they say” and “instills fear and inhibition,” forcing individuals to “take precautions in communicating with others.”⁵¹ Due to the unique sensitivity of biometric information, namely by definition being inseparably linked to a particular person, the mere existence of these programs can lead to a broad-sweeping “chilling effect” on the exercise of freedom of expression.
38. In the case of Uganda, Section 65 of the Registration of Persons Act, provides for the use of the register for various purposes including national security as well as “any other purpose as may be determined by the Minister for Internal Affairs.” The provision has been applied in justifying access by police and security officers in fighting crime and “improving surveillance.”⁵² This creates a risk of misuse of information in the system for surveillance, producing the “chilling effect” on speech.

iii) The relationship between the right to privacy and impact on social, economic and cultural rights

39. Article 9 of the International Convention on Economic, Social and Cultural Rights (ICESCR) (ratified by Uganda in 1987) guarantees the right to social security, which encompasses the right to access and maintain benefits, whether in cash or in kind, without discrimination.⁵³ General Comment No. 19 on Article 9 of the Covenant has further clarified that the withdrawal, reduction, or suspension of benefits should be

⁵¹ Inter-American Commission on Human Rights, “Freedom of Expression and the Internet” (31 December 2013), para. 150, http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf.

⁵² Anri van der Spuy, “Digital Identity in Uganda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (Towards the Evaluation of Digital ID Ecosystems in Africa: Findings from Ten Countries) [Case study],” (November 2021), Research ICT Africa, <https://researchictafrica.net/publication/digital-identity-in-uganda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/>.

⁵³ UN General Assembly, International Covenant on Economic, Social and Cultural Rights (3 January 1976), <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>; Committee on Economic, Social and Cultural Rights, The Right to Social Security, General Comment No. 19: The Right to Social Security (Article 9), E/C.12/GC/19 para. 2, <https://www2.ohchr.org/english/bodies/cescr/docs/cescr39/E.C.12.GC.19.pdf>

circumscribed, based on grounds that are reasonable and subject to due process.⁵⁴ Article 2(1) of ICESCR requires states to take steps to the maximum of their available resources towards achieving the full realization of all economic, social, and cultural rights. General Comment No. 3 acknowledges that full realization of these rights will generally not be possible in a short period of time; however, for “any deliberately retrogressive measures, ICESCR requires the most careful consideration⁵⁵, i.e., when (i) the adoption of retrogressive measures is unavoidable; and (ii) such measures should be necessary and proportionate, in the sense that the adoption of any other policy or failure to act would be more detrimental to economic, social, and cultural rights.⁵⁶ The implications on these rights have been sufficiently canvassed by the *amici* in this case.

40. However, the *amici* seek to also stress that the violation of the right to privacy in these cases is inextricable from their impact on other social, economic, and cultural rights. The implementation of national digital ID programs often results in states’ applying retrogressive measures.

41. For instance, the Indian Supreme Court in their assessment of *privacy* observed that the socio-economic rights and civil and political rights must be seen as interrelated, and therefore, rejected the argument of the state that privacy is an elitist construct that did not reflect the aspirations of people in developing states.⁵⁷ The Court references the work of Nobel prize winning economist Amartya Sen, who established the link between the denial of civil and political liberties and the right to food in colonial India, Botswana, and Zimbabwe. On this basis, the Court observed that:

“conditions of freedom and a vibrant assertion of civil and political rights promote a constant review of the justness of socio-economic programmes and of their effectiveness in addressing deprivation and want. Scrutiny of public affairs is founded upon the existence of freedom. Hence civil and

⁵⁴ Committee on Economic, Social and Cultural Rights, The Right to Social Security, General Comment No. 19: The Right to Social Security (Article 9), E/C.12/GC/19 para. 24, <https://www2.ohchr.org/english/bodies/cescr/docs/cescr39/E.C.12.GC.19.pdf>.

⁵⁵ UN Human Rights Committee, General Comment No. 3: The Nature of States Parties’ Obligations (14 December 1990), UN Doc. E/1991/23, para. 9, <https://www.refworld.org/pdfid/4538838e10.pdf>.

⁵⁶ UN Committee on Economic, Social, and Cultural Rights, “Public Debt, Austerity Measures, and the International Covenant on Economic, Social, and Cultural Rights” (22 July 2016), UN Doc. E/C.12/2016/1, para. 4, <https://www.undocs.org/E/C.12/2016/1>.

⁵⁷ *Puttaswamy v. Union of India* (Privacy-9j), paras. 154-156.

political rights and socio-economic rights are complementary and not mutually exclusive.”⁵⁸

42. Particular to digital ID systems, in 2019, Philip Alston, the Special Rapporteur on extreme poverty and human rights, expressed concern about the use of digital ID, by saying: “any individuals, and especially those living in poverty, do not have a reliable internet connection at home, cannot afford such a connection, are not digitally skilled or confident, or are otherwise inhibited in communicating with authorities online.”⁵⁹ Such problems “impede the ability of would-be claimants to realize their human rights”⁶⁰ such as the right to social security, an adequate standard of living, mental health, and life with dignity.⁶¹
43. Reports by Access Now also pointed out that Aadhaar led to many such exclusions, also involving school children.⁶² In its final decision on Aadhaar, the Indian Supreme Court recognized these exclusions. While upholding Aadhaar as a voluntary scheme for “services,” the Court struck down the mandatory use of Aadhaar in cases where it leads to deprivation of fundamental rights such as the right to education.⁶³ Similarly, the Court recognized that government pension is also a right and, therefore, must not be subject to

⁵⁸ *Id.*

⁵⁹ UN General Assembly, Report of the Special Rapporteur on Extreme Poverty and Human Rights (11 October 2019), UN Doc. A/74/48037, paras. 11-28, 46, <https://undocs.org/A/74/493>.

⁶⁰ *Id.*

⁶¹ *Id.* para. 52. For example, In India, registration in the country’s national digital ID system, Aadhaar, is a precondition for accessing food rations and other welfare provisions. There have been many instances of “disabled and aged people facing additional difficulty” since they are “unable to physically report to an enrollment center to obtain an Aadhaar number.” As a result, they are unable to receive pension payments, meal rations, or healthcare. Even young children aren’t spared; many were never issued birth certificates and thus face difficulties in acquiring digital ID cards. Several reports suggest that such children have been “denied free meals in government schools, or even admission into schools,” creating serious concerns regarding the violation of their right to education. Furthermore, since Aadhaar machines installed in food distribution outlets require an internet connection, “poor connectivity in rural areas has also led to disruptions in food distribution schedules.” Local activists have even found that Aadhaar-related denials of food rations have led some to starve to death. *See*, National Law University Delhi, Submission to the Special Rapporteur on extreme poverty and human rights, <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>. Padmaparna Ghosh, “Aadhaar: In the World’s Biggest Biometric ID Experiment, Many Have Fallen Through the Gaps” (24 February 2018), <https://scroll.in/article/868836/aadhaar-in-the-worlds-biggest-biometric-id-experiment-many-have-fallen-through-the-gaps>. Human Rights Watch submission to Special Rapporteur on extreme poverty and human rights, p. 5, <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf>.

⁶² Access Now, “National Digital Identity Programmes: What’s Next” (21 March, 2018), <https://www.accessnow.org/national-digital-identity-programmes-whats-next/>; Access Now, “Busting the Dangerous Myths of Big ID programs: Cautionary lessons from India” (5 October, 2021), <https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf>.

⁶³ *Puttaswamy v. Union of India* (Aadhaar), para 323-235.

Aadhaar.⁶⁴ Thus, the Court refused to adopt a consent framework where it leads to exclusion from core socio-economic rights. Access Now’s report also explains that in such situations, informed consent is illusory as people have no real choice but to enroll in such programs.⁶⁵

44. In fact, enrollment in the digital ID program is usually mandatory, as is the case in Uganda, at least to receive benefits and subsidies from states. For those who seek to exercise these rights, submission of biometric information is compulsory. Even for those who do not intend to exercise these rights, albeit on a voluntary basis, enrollment is mandatory because, as the 2019 Philip Alston Report, Special Rapporteur on extreme poverty and human rights, points out, “digital by choice” policy turns into “digital-only.”⁶⁶ Early in 2005, Judicial Yuan of Taiwan decided that, although the ID cards issued under the digital ID programs are merely one of valid ID cards, digital ID cards are required in every aspect of life, for administrative procedures and private activities such as opening a bank account or being hired by a business, therefore “[whether people] are issued identity cards *directly* affects the exercise of their basic rights.”⁶⁷

45. Therefore, while informed consent must be the basis of any digital identity system, the Court must consider whether consent can be freely given in cases of derogation from core social, economic, and cultural rights.

6. Conclusion and Recommendations

46. The principles discussed in this submission relating to the fundamental rights to privacy, data protection, and freedom of expression, including in the digital space, are well-established. The context of this case – the use of the digital identity system to – is still relatively new. This brief provides the Uganda Court with an opportunity to provide clear guidance on how the existing principles apply to these new and concerning developments in state activity.

47. The *Amici* thus recommend that, at a minimum, the Court:

- a. Strongly considers whether the Ndaga Muntu digital ID system is lawful and compatible with Ugandan law and international human rights;

⁶⁴ *Id.*, para 322.

⁶⁵ Access Now, “Busting the Dangerous Myths of Big ID programs: Cautionary lessons from India” (5 October, 2021), <https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf>.

⁶⁶ UN General Assembly, Report of the Special Rapporteur on Extreme Poverty and Human Rights (11 October 2019), UN Doc. A/74/48037, para. 35, <https://undocs.org/A/74/493>.

⁶⁷ Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005).

- b. Finds that the digital ID system should not be compulsory because of the risks posed to the rights of privacy, freedom of expression, and the associated rights of Ugandans;
- c. Directs the Respondent Attorney General to ensure that the Registration of Persons Act of 2015 is reviewed to ensure consistency with the Data Protection and Privacy Act, 2019 and the Regulations therein;
- d. Directs the Respondents to ensure that the implementation of the Ndaga Muntu is in compliance with the Data Protection and Privacy Act, 2019, given the risks to data protection and privacy; and
- e. Directs the Respondents to conduct a mandatory annual audit of the digital ID System by an audit team, composed of data security and privacy experts, which is sufficiently independent from NIRA, whose report should be made public, to confirm whether the System is operated in accordance with the law.

JOINTLY SUBMITTED ON THIS 4TH day of NOVEMBER 2022

On behalf of **ACCESS NOW** by **JOSEPH STEELE**, Chief Operating Officer, Access Now



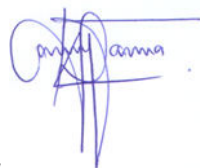
SIGNATURE

On behalf of **ARTICLE 19** by **MUGAMBI KIAI**, Regional Director, Article 19



SIGNATURE

On behalf of **CIPESA** by **WANYAMA EDRINE** Legal Officer



SIGNATURE