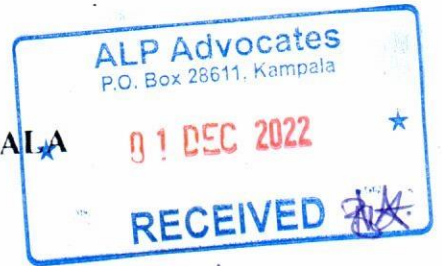


THE REPUBLIC OF UGANDA
IN THE HIGH COURT OF UGANDA AT KAMPALA
CIVIL DIVISION



MISCELLANEOUS APPLICATION NO. 0650 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

NOTICE OF MOTION

(Brought under Articles 50(2) of the Constitution of the Republic of Uganda, Judicature Act, Civil Procedure Act, Rules 5, 6,9 of the Judicature (Amicus Curiae) Rules, 2022 SI NO.54 of 2022, Civil Procedure Rules)

TAKE NOTICE that this Honourable Court will be moved on the **13th** Day of **December 2022** at **12:00** o'clock in the fore/afternoon or so soon thereafter as Counsel for the Applicants can be heard on behalf of the Applicants for orders that:

- a. The Applicants, **COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA(CIPESA), ACCESS NOW and ARTICLE 19: GLOBAL CAMPAIGN FOR FREE EXPRESSION** are granted leave to intervene as *Amici Curiae* in Miscellaneous Cause No.86 of 2022.
- b. Each party to bear its own costs.

TAKE FURTHER NOTICE that this application is supported by grounds set out in the affidavit of **WANYAMA EDRINE** on behalf of the 1st Applicant, **JOSEPH STEELE** on behalf of the 2nd Applicant and **MUGAMBI KIAI** on behalf of the 3rd Applicant which shall be read and relied upon at the hearing but briefly are that:

- i. The Applicants possess expertise and knowledge on matters concerning Digital Identity systems, digital security, right to privacy, internet freedom, biometric systems, data management, and governance and their impact on the civil and political rights, as well as social, economic, and cultural rights.
- ii. The Applicants are recognized experts regionally and internationally in the promotion and advancement of human rights, especially the right to inclusion in the arena of data protection, right to privacy, freedom of expression, surveillance, and how these intersect with the socio-economic rights.
- iii. The Applicants have interest in the determination of the Main Cause as human rights organizations promoting equity and inclusion and this constitutes fidelity to the law.
- iv. The Applicants are neutral and impartial of the dispute between the parties in the Main Cause.

- v. The submissions made by Applicants on various points of law regarding the subject matter are novel and shall aid the development of jurisprudence in Uganda.
- vi. The Applicants' submissions draw attention to relevant matters of law that are useful, focused, and principled.
- vii. The Applicants have previously submitted amicus briefs, expert opinions, legal analyses, intervenor and inter-party submissions to various international, regional and national courts, tribunals and Human Rights Commissions on points of law of key importance to human rights protection especially on the use and management of personal data and inclusion.
- viii. The Applicants are aware of the current system in Uganda that makes it mandatory for one to present a national identification number, or being part of the national identification register acquired through enrollment in the national digital identification system by Ugandans to access SAGE benefits as a form of social security, as well as public health services.
- ix. The Applicants have examined the above practices and the existing legal and policy regulatory framework and are ready and willing to provide this Honourable Court with submissions on the impact of the above practice on the right to privacy, freedom of expression, as well as the right to social security, and other rights.
- x. The Applicants had the opportunity to study the pleadings of the main Application and Affidavits in reply and note that there is need to resolve the questions around the digital national identification system in Uganda on the one hand, and 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, on the other.
- xi. These questions have not been dealt with by the pleadings before this Court and yet are important in the Court's determination of the Main

Cause and the need to balance access to SAGE with the right to privacy and freedom of expression and equity and inclusion.

xii. The Applicants' brief on international, regional, and comparative law in the field of Digital Identity systems, right to privacy, data protection, freedom of expression, and inclusion will give assistance to the Court that it would otherwise not have.

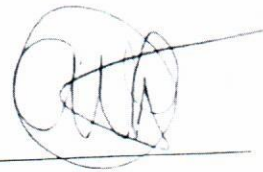
xiii. The positive benefits of the intervention of the Applicants as *Amici Curiae* outweigh any possible opposition from the parties to the main cause as has been well enunciated by the Applicants.

xiv. It is in public interest, interests of justice, the promotion and protection of human rights that the application seeking leave to intervene as *Amici Curiae* is granted.

Dated at Kampala this 4th Day of November 2022



M/s Thomas & Michael Advocates



M/s MOM Advocates

(COUNSEL FOR THE APPLICANTS)

Given under my hand and the seal of the Honourable Court this.....day
of.....2022

DEPUTY/REGISTRAR

Jointly Drawn and filed by:

M/s Thomas and Michael Advocates
Plot 127 Muteesa II Road, Ntinda
P.O. BOX 73577 Kampala
0782 285999, 0779 201692
thomasmichaeladvocates@gmail.com

AND

M/s MOM Advocates
2nd floor Ntinda Shopping Centre
Suite C08 and C09, Ntinda-Kampala

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

1ST APPLICANT'S AFFIDAVIT IN SUPPORT OF NOTICE OF MOTION

I **WANYAMA EDRINE** of C/o M/S Thomas and Michael Advocates, Plot 127 Muteesa II Road, Ntinda, P. O Box 75377, Kampala and M/s MOM Advocates 2nd floor Ntinda Shopping Centre, Suite C08 and C09, Ntinda-Kampala do hereby by solemnly make oath and state:

1. That I am an adult male Ugandan of sound mind and the Legal Officer of the 1st Applicant (**COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST AND SOUTHERN AFRICA**, Website: www.cipesa.org) hereinafter referred to as **CIPESA**.
2. That I am a duly authorised representative of the 1st Applicant swear this affidavit in that capacity in support of the application by the Applicants to be admitted as Amici Curiae in Miscellaneous Cause No 86 of 2022.
3. That I know that CIPESA is a non-for-profit organization duly registered in Uganda having been founded in 2004. CIPESA is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA focuses on decision-making that facilitates the use of ICT in support of development and poverty reduction. (*A copy of the certificate of registration is hereto attached as annexure 'WE1'*).
4. That I know that the Organisation promotes internet freedom and governance, civic participation, data governance, the digital economy, digital inclusion and digital resilience and works across the continent, informing policy-making, and stirring debate and convening productive gatherings. The Organisation works with networks, individuals and organisations (private sector, governmental, academic, civil society) across the region, and we are key members of several African and international initiatives that aim to improve the inclusiveness of the Information Society.
5. That I know that CIPESA, through research and documentation contributes 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. *(A list/summary of the research publications is hereto attached as annexure 'WE2')*

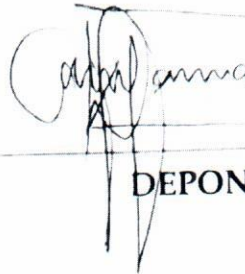
6. That I know that CIPESA is a recognized member of various African and international initiatives that aim to improve the inclusiveness of the Information Society, including the Association for Progressive Communications (APC), Global Network Initiative (GNI), Global Knowledge Partnership (GKP), IFEX, Global Encryption Coalition, World Benchmarking Alliance, and the Alliance for Affordable Internet (A4AI).
7. That I know that CIPESA has Observer status with the African Commission on Human and Peoples Rights made several contributions to the digital rights, digital inclusion, internet freedom, data protection and privacy through the various regional and international human rights mechanisms including the African Commission on Human and Peoples Rights and the Universal Periodic Review. *(A list/summary of the submissions made by CIPESA is hereto attached as annexure 'WE3')*.
8. That I know that CIPESA requests leave to appear in the present case as amicus curiae contributing its expertise and knowledge of international practice on relevant international and comparative law and jurisprudence on the use ICT to improve governance and livelihoods.
9. That I know that CIPESA has made legal analyses and submitted to government institutions such as the Parliament of Uganda on related subjects of data protection and privacy and internet freedom. *(A list of the various legal analyses is hereto attached as annexure 'WE4')*
10. That I know that CIPESA has experience in providing expertise to courts of law on issues regarding digital identity, digital inclusion, right to privacy, use

of ICT systems and their impact on human rights. CIPESA filed an affidavit in support of the petition of *Cyber Law Initiative and 5others V The Attorney General Constitutional Petition No.26 of 2018* where the gist of the case was challenging the Social Media tax and its impact on the socio and economic life of the people of Uganda. (A copy of this Affidavit is hereto attached as annexure 'WE5')


11. That I know that the Organisation has been involved in extensive stakeholder consultations and engagement on matters pertaining digital security, online security, protection of personal data, data governance, surveillance among others.
12. That I am aware that in respect to the duty to respect, protect and fulfil human rights, the obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights; obligation to protect requires States to protect individuals and groups against human rights abuses; and the obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights.
13. That I know that CIPESA is aware of the current system in Uganda that makes it mandatory for one to present a national identification number, or being part of the national identification register acquired through enrolment in the national digital identification system by Ugandans to access SAGE benefits as a form of social security, as well as public health services.
14. That CIPESA has examined the above practice and the existing legal and policy regulatory framework and is ready and willing to provide this honourable court with submissions on the impact of use of biometrics on Digital ID rights, data governance, online security, surveillance, internet freedom, right to access to information, right to privacy and freedom of information.

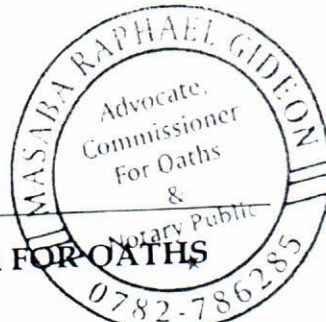
15. That I know that CIPESA has had the opportunity to study the pleadings of the main Application and Affidavits in reply and notes that there is need to resolve the questions around the data protection, digital inclusion, surveillance especially those that have been left out in the national identification system in Uganda and the sufficiency of protection measures and their impact on protection of the right to privacy even at the instance of a roll out of a good government program like SAGE. This issue has not been dealt with by the pleadings before court and yet are important in Court's determination of the Main Cause.
16. That I know that CIPESA is neutral and impartial concerning the legal matters that are before this honourable Court in the main cause.
17. That I know that the interest of CIPESA in this matter before court constitutes fidelity to the law as experts and proponents of Digital ID Systems and online security and safety and attendant rights.
18. That I know that the points of law CIPESA has submitted on are novel and will aid the development of jurisprudence of Uganda.
19. That I know that CIPESA's submissions draw attention to relevant matters of law that are useful, focused and principled.
20. That I know that CIPESA has jointly drafted, together with the 2nd and 3rd Applicants the amicus brief touching the matters deponed in this affidavit submitted to this honourable court which will give assistance to the court that it would otherwise not have.
21. That I know that it is in public interest, interests of justice, the promotion and protection of human rights that the application seeking leave to intervene as Amicus Curiae is granted.
22. That whatever is stated herein above is true and correct to the best of my knowledge belief and information save where otherwise stated.

SWORN by the said WANYAMA EDKINE at KAMPALA on this 3rd day of
November 2022


DEPONENT

BEFORE ME


A COMMISSIONER FOR OATHS



Jointly Drawn and filed by:

M/s Thomas and Michael Advocates
Plot 127 Muteesa II Road, Ntinda
P.O.BOX 73577 Kampala
0782 285999, 0779 201692
thomasmichaeladvocates@gmail.com

AND

M/s MOM Advocates
2nd floor Ntinda Shopping Centre,
Suite C08 and C09,
Ntinda-Kampala



82128


THE REPUBLIC OF UGANDA

Certificate of Incorporation

(Under section 16 (1) of the Companies Act)

I CERTIFY that COLLABORATION ON INTERNATIONAL ICT POLICY FOR EAST
..... AND SOUTHERN AFRICA (CIPESA) (BY GUARANTEE)
.....
has this day been incorporated with Limited Liability.

Dated at Kampala, this 31ST day
of JULY the year 2006


KYOMUGASHO MERCY
KENTARO
ASST. Registrar of Companies.

CIPESA RESEARCH PUBLICATIONS

1. Digital Authoritarianism And Democratic Participation In Africa Brief (Jun. 2022), https://cipesa.org/?wpfb_dl=502
2. State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance (Sep. 29, 2022), <https://cipesa.org/2022/09/state-of-internet-freedom-in-africa-2022-the-rise-of-biometric-surveillance/>
3. Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa (Aug. 16, 2022), https://cipesa.org/?wpfb_dl=492
4. Togo: Fumbling With a Digital ID While Actively Surveilling Citizens (Apr. 21, 2022), <https://cipesa.org/2022/04/togo-fumbling-with-a-digital-id-while-actively-surveilling-citizens/>
5. COVID-19 Data Governance In Kenya (Apr. 2022), https://cipesa.org/?wpfb_dl=500
6. COVID-19 And Data Rights In Uganda Report (Apr. 2022), https://cipesa.org/?wpfb_dl=493
7. Data Governance And Public Trust- Exploring The Sources Of Low Trust Levels In Public Data Controllers In Ghana Report (Apr. 2022), https://cipesa.org/?wpfb_dl=494
8. Ecosystem Approach To Digital Identification Enrolment- Assessing The Opportunities And Risks In Nigeria Report (Apr. 2022), https://cipesa.org/?wpfb_dl=498
9. Analysis of The South Sudan Cyber Crimes and Computer Misuse Provisional Order (Nov. 2021), https://cipesa.org/?wpfb_dl=480
10. Mapping and Analysis of Privacy Laws in Africa (Nov. 2021), https://cipesa.org/?wpfb_dl=479
11. State of Internet Freedom in Africa 2021 Report (Sep. 2021), https://cipesa.org/?wpfb_dl=467
12. SIM and Device Registration Could Fundamentally Interfere with Data Protection and Privacy in Lesotho (Aug. 30, 2021), <https://cipesa.org/2021/08/sim-and-device-registration-could-fundamentally-interfere-with-data-protection-and-privacy-in-lesotho/>
13. Lesotho: SIM and Device Registration Pose Major Threats to Data Protection and Privacy, (Aug. 2021), https://cipesa.org/?wpfb_dl=465
14. How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa (Jul. 19, 2021), <https://cipesa.org/2021/07/how-surveillance-collection-of-biometric-data-and-limitation-of-encryption-are-undermining-privacy-rights-in-africa-2/>
15. Data Governance Regulation In Tanzania- Gaps, Challenges And Opportunities (Apr. 2021), https://cipesa.org/?wpfb_dl=499
16. Civil Society Organisations Call For a Full Integration of Human Rights in The Deployment of Digital Identification Systems (Dec. 17, 2020), <https://cipesa.org/2020/12/civil-society-organisations-call-for-a-full-integration-of-human-rights-in-the-deployment-of-digital-identification-systems/>
17. Are Malawians Sleep-Walking into a Surveillance State? (Aug. 12, 2019), <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/>
18. The Stampede for SIM Card Registration: A Major Question for Africa (Apr. 18, 2018), <https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/>

CIPESA List of Contributions to the African Commission on Human and Peoples Rights and the Universal Periodic Review

CIPESA Submission to the ACHPR on Ratification of the African Protocol on Disability Rights, <https://cipesa.org/wp-content/uploads/2022/05/CIPESA-Letter.pdf>

Shadow Report on Freedom of Expression Online in Rwanda, <https://cipesa.org/2017/11/shadow-report-on-freedom-of-expression-online-in-rwanda/>

Digital Rights Prioritised at The 73rd Session of The ACHPR, <https://cipesa.org/2022/10/digital-rights-prioritised-at-the-73rd-session-of-the-achpr/>

Namibia’s Digital Rights Record to be Assessed at the 38th Session of the Universal Peer Review https://cipesa.org/?wpfb_dl=436

Sierra Leone’s Digital Rights Record to be Assessed at the 38th Session of the Universal Peer Review, https://cipesa.org/?wpfb_dl=437

Universal Peer Review: Mozambique Should Guarantee Digital Rights, https://cipesa.org/?wpfb_dl=363

Ethiopia’s Digital Rights Record on the Spot at May 2019 Universal Peer Review, https://cipesa.org/?wpfb_dl=292

Submission to the 40th Session of the Universal Periodic Review – South Sudan, https://cipesa.org/?wpfb_dl=452

Submission to the 40th Session of the Universal Periodic Review – Uganda, https://cipesa.org/?wpfb_dl=451

List of CIPESA’s Legal Analyses

18 NGOs file an intervention before France’s highest court on dangers of the ‘right to be forgotten’ <https://cipesa.org/2017/04/18-ngos-file-an-intervention-before-frances-highest-court-on-dangers-of-the-right-to-be-forgotten/>

CIPESA Submits Comments On The Uganda Data Protection and Privacy Bill, 2015, https://cipesa.org/?wpfb_dl=263

Uganda: CIPESA Submits Comments on the Computer Misuse (Amendment) Bill, 2022 to Parliament, https://cipesa.org/?wpfb_dl=503

CIPESA Submits Comments to Uganda Communications Commission on Improving Access to ICT for Persons With Disabilities, https://cipesa.org/?wpfb_dl=281

Reflections on Uganda’s Draft Data Protection and Privacy Bill, 2014, https://cipesa.org/?wpfb_dl=185

MINISTRY OF JUSTICE &
CONSTITUTIONAL AFFAIRS
DIRECTORATE OF CIVIL LITIGATION
★ 19 JUL 2018 ★
RECEIVED
Sign: *[Signature]*

"WE5"



THE REPUBLIC OF UGANDA

UGANDA REVENUE AUTHORITY
RECEIVED
19 JUL 2018
Rebecca B. B. P. P.
COMMISSIONER LEGAL
SERVICES & BOARD AFFAIRS

IN THE CONSTITUTIONAL COURT OF UGANDA AT KAMPALA
CONSTITUTIONAL PETITION No. 026 OF 2018

UGANDA COMMUNICATIONS COMMISSION
RECEIVED
19 JUL 2018
Yahya
SIGN: *[Signature]*
UGANDA COMMUNICATIONS COMMISSION

- 1) CYBER LAW INITIATIVE (U) LIMITED
- 2) OPIO DANIEL BILL
- 3) BAGUMA MOSES
- 4) OKIROR EMMANUEL
- 5) SILVER KAYONDO
- 6) RAYMOND MUJUNI

.....PETITIONERS

VERSUS

COURT OF APPEAL OF UGANDA
19 JUL 2018
RECEIVED
3:32 pm
[Signature]

- 1) THE ATTORNEY GENERAL OF UGANDA
- 2) UGANDA COMMUNICATIONS COMMISSION (UCC)
- 3) UGANDA REVENUE AUTHORITY (URA)

..... RESPONDENTS

SUPPLEMENTARY AFFIDAVIT IN SUPPORT OF
THE AMENDED PETITION

I, **DR. WAIRAGALA WAKABI**, of c/o M/S Aguma Kifunga & Co. Advocates, Master Plaza, Second Floor, Room S.9 P.O. Box 1443, Kampala; M/s ORTUS LLP of 7th Floor Park Royal Building, Plot 26 Buganda Road, Kampala; do solemnly swear and state on oath as follows:

- 1. THAT I am an adult male Ugandan of sound mind; and the Executive Director of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA); and I do swear this affidavit in that capacity.

FEE'S PAID... 1,500
231794 15

MINISTRY OF JUSTICE &
CONSTITUTIONAL AFFAIRS
DIRECTORATE OF CIVIL LITIGATION
★ 19 JUL 2018 ★
4:20p
RECEIVED
Sign:



THE REPUBLIC OF UGANDA

UGANDA REVENUE AUTHORITY
RECEIVED
19 JUL 2018
Rebecca 3:30p
COMMISSIONER LEGAL
SERVICES & BOARD AFFAIRS

IN THE CONSTITUTIONAL COURT OF UGANDA AT KAMPALA
CONSTITUTIONAL PETITION No. 026 OF 2018

- 1) CYBER LAW INITIATIVE (U) LIMITED
- 2) OPIO DANIEL BILL
- 3) BAGUMA MOSES
- 4) OKIROR EMMANUEL
- 5) SILVER KAYONDO
- 6) RAYMOND MUJUNI

.....PETITIONERS

VERSUS

- 1) THE ATTORNEY GENERAL OF UGANDA
- 2) UGANDA COMMUNICATIONS COMMISSION (UCC)
- 3) UGANDA REVENUE AUTHORITY (URA)

..... RESPONDENTS

SUPPLEMENTARY AFFIDAVIT IN SUPPORT OF
THE AMENDED PETITION

I, **DR. WAIRAGALA WAKABI**, of c/o M/S Aguma Kifunga & Co. Advocates, Master Plaza, Second Floor, Room S.9 P.O. Box 1443, Kampala; M/s ORTUS LLP of 7th Floor Park Royal Building, Plot 26 Buganda Road, Kampala; do solemnly swear and state on oath as follows:

1. THAT I am an adult male Ugandan of sound mind; and the Executive Director of the Collaboration on International ICT Policy for East and Southern Africa (CIPESA); and I do swear this affidavit in that capacity.

FEES PAID.....1,500.....
.....231794

COURT OF APPEAL OF UGANDA
19 JUL 2018
RECEIVED
3:32 pm

UGANDA COMMUNICATIONS COMMISSION
19 JUL 2018
RECEIVED
3:50pm

A copy of the relevant Certificate of Incorporation is hereto attached and respectively marked "A."

2. That I have extensive expertise in the areas of telecoms regulation, online rights and internet governance mechanisms in Africa and on global best practices for digital inclusion.
3. That the internet is an important enabler for public access to information and dissemination, transparency and accountability, knowledge generation, social and economic growth for the state and citizens, government interaction with citizens, civic participation in governance processes, and inclusion in the global digital society.
4. That access to the internet entails use of platforms such as WhatsApp, Messenger, Twitter, Facebook, Tumblr, LinkedIn, Skype, Over-The-Top (OTT) services, as well as the use of Virtual Private Networks (VPNs) and browsing services.
5. That access to OTT services offered by some of the aforementioned platforms is an integral part of access to the internet and an enabler of public access to information and dissemination, transparency and accountability, government interaction with citizens, civic participation in governance processes and inclusion in the global digital society.
6. That the use the internet including through social media has positively impacted on the social, political and economic status of Uganda at a national and civic level.
7. That on May 30, 2018, the Parliament of Uganda enacted the Excise Duty (Amendment) Act, 2018 whose sections **3(b)** and **6(g)** impose an excise duty of UGX 200 per day of use to access OTT services as of July 1, 2018.

8. That in compliance to the Excise Duty (Amendment) Act, 2018, telecommunication companies including MTN, Airtel and Africell on June 29, 2018 issued a joint public notice confirming that the law would take effect on July 1, 2018 and that access to a range of social media platforms and OTT services would be blocked subject to payment of OTT tax via mobile wallet, EVC or any electronic wallets.
9. That I am aggrieved by the passing of the Excise Duty (Amendment) Act, 2018 whose sections **3(b)** and **6(g)** impose excise duty of UGX 200 per user per day for access to over the top (OTT) services with effect from July 1, 2018.
10. That the passing of the Excise Duty (Amendment) Act, 2018, specifically sections 3 (b) and 6 (g) are contrary to article 29 (1) (a) on freedom of expression and article 41 on access to information of the Constitution of the Republic of Uganda, 1995.
11. That the Excise Duty (Amendment) Act, 2018, specifically sections 3 (b) and 6 (g) fall within the ambit of article 2 (2) on supremacy of the Constitution of the Republic of Uganda, 1995 and should be treated as such.
12. That the Excise Duty (Amendment) Act, 2018, specifically sections 3 (b) and 6 (g) is contrary to international human rights instruments to which Uganda is party including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the Declaration of principles of freedom of expression in Africa (2002), and the Resolution on the Situation of Freedom of Expression in Africa. These international instruments provide for the right to freedom of speech, expression, access to information and dissemination and imparting of ideas.

13. That under the international human rights instruments, by becoming party to international treaties, the government of Uganda has a duty to respect, protect and fulfill rights of the citizens by among others enacting progressive legislation including through transparent public consultation processes.
14. That I am aware that in respect to the duty to respect, protect and fulfill human rights, the: obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights; obligation to protect requires States to protect individuals and groups against human rights abuses; and the obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights.
15. That given the current poverty levels of the country with **19.7%** living below the national poverty line and **34.6%** living on USD1.90 PPP per day according to the World Bank Uganda Poverty Assessment of 2016 (available at <http://pubdocs.worldbank.org/en/381951474255092375/pdf/Uganda-Poverty-Assessment-Report-2016.pdf>), a large cross-section of the populace will face financial limitations to access the internet and social media due to the increased costs associated with the tax and will as a result have limited the enjoyment of their online fundamental human rights and basic freedoms. **An extract of the full report is hereto attached and marked "B"**
16. That according to research by the Alliance for Affordable Internet (available at <http://1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2017/02/A4AI-2017-Affordability-Report.pdf>), the OTT taxes cause the cost to connect for Uganda's poorest to jump by 10%, resulting in just 1GB of data costing them nearly 40% of their average monthly income. **An extract of the full report is hereto attached and marked "C"**

17. That given the current estimated internet penetration rate of 48.2 internet users per 100 inhabitants according to the Post, Broadcasting and Telecommunications Market & Industry Q3 Report, 2017 of the Uganda Communications Commission(available at <http://www.ucc.co.ug/wp-content/uploads/2018/02/Market-Industry-Quarterly-Report-for-the-Quarter-ending-September-2017-Final.pdf>), the introduction of the social media tax is likely to reduce internet penetration and usage. **An extract of the full report is hereto attached and marked “D”**
18. That According to the Uganda National Information Technology (IT) survey of 2017 – 2018 (available at <https://www.nita.go.ug/sites/default/files/publications/National%20IT%20Survey%20April%2010th.pdf>); at least **92%** of Uganda Ministries, Departments and Agencies (MDAs) rely on social media to engage with their constituents with Facebook, Twitter and WhatsApp ranking as the highest. In the same report **76.6%** of the respondents indicated that the cost of access to the internet was a limitation to their use of the internet. **An extract of the full report is hereto attached and marked “E”**
19. That taxing social media will hinder engagement between citizens and government Ministries, Departments and Agencies (MDAs) who have come to rely on it as an avenue for civic participation, and for which in May 2013, Cabinet directed the Ministry of Information and Communications Technology (MoICT) to ensure that every Government Ministry, Department and Agencies (MDAs) opens a Twitter and Facebook account to improve communication with the Public.
20. That the taxes on social media OTT platforms serve to promote a culture of inequality in Uganda and widen the gender digital divide – particularly for women.

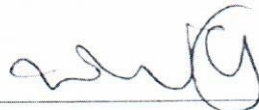
21. That increasing government criticism on social media has led to government actions which are contrary to Article 29 (1) (a) of the Constitution of the Republic of Uganda, 1995 on freedom of expression, such as social media shutdowns (as witnessed during the 2016 election period on two separate occasions), information requests for user data from global intermediaries (such as the request for information on TVO from Facebook) and the use of the Computer Misuse Act, 2011 against critics of the state as witnessed in the arrest of Dr. Stella Nyanzi.

22. That Ugandans who use social media are already paying Value Added Tax through data purchases using airtime and the introduction of an additional tax is tantamount to double taxation.

23. That I depone this affidavit in support of the reliefs sought in the petition herein; and in strong opposition to the enacted Excise Duty (Amendment) Act, 2018 whose sections 3(b) and 6(g) impose and continue to impose an excise duty of UGX 200 per user per day for access to Over-the-Top (OTT) services with effect from July 1st, 2018.

24. That I have stated herein above is true and correct to the best of my knowledge.

SIGNED by the said **DR. WAIRAGALA WAKABI** at Kampala on this 19th day of July, **2018**.



DEPONENT

BEFORE ME:



KAKEETO MAHMOOD ESO
ADVOCATE &
COMMISSIONER FOR OATHS
P. O. BOX 6236 K'LA
Email: kakeetolaw@yahoo.com

A COMMISSIONER FOR OATHS

Jointly drawn & filed by:

M/S Aguma Kifunga & Co. Advocates

Master Plaza, Second Floor, Room S9

P.O. Box 1443, Kampala

Tel: 0703831252

Email: kiizaeron@gmail.com

AND

M/s ORTUS LLP

7th Floor Park Royal Building

Plot 26 Buganda Road, Kampala.

Twitter: @OrtusLLP

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

2ND APPLICANT'S AFFIDAVIT IN SUPPORT OF NOTICE OF MOTION

I, **JOSEPH STEELE** of *C/o M/S Thomas and Michael Advocates, Plot 127 Muteesa II Road, Ntinda, P. O Box 75377, Kampala and M/s MOM Advocates 2nd floor Ntinda Shopping Centre, Suite C08 and C09, Ntinda-Kampala* do hereby by solemnly make oath and state:

1. That I am an adult male American of sound mind and the Chief Operating Officer of the 2nd Applicant (ACCESS NOW) duly authorized representative of the 2nd Applicant swear this affidavit in that capacity in support of the application by the Applicants to be admitted as Amici Curiae in Miscellaneous Cause No 86 of 2022.
2. That I know that ACCESS NOW is an international, non-governmental organization that defends and extends the digital rights of people and communities at risk around the world. The Organisation was founded in 2009 and is registered in the State of California, the United States of America. *(A copy of the certificate of registration is hereto attached as annexure 'JS1')*
3. That I know that 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, ACCESS NOW requests leave to appear in the present case as Amici Curiae contributing its expertise and knowledge of international practice on relevant international and comparative law and jurisprudence. *(Our profile hereto can be viewed at <https://www.accessnow.org/>)*
4. That I know that ACCESS NOW through its research, advocacy has contributed knowledge in the areas of Digital ID system and digital rights, including the right to information and privacy, through its publications, analyses, and policy briefs which have been used as resources by both governments and courts. ACCESS NOW has published over 25 publications on the subject of Digital ID systems and human rights. *(A list/summary of these publications are hereto attached as annexure 'JS2')*
5. That I know that through direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as our yearly conference on human rights in the digital age "RightsCon," the organization works in more than twenty-five countries to monitor, investigate, and prevent violations of digital rights worldwide using the expertise and the law in order to promote equity and inclusion in society and therefore, it has particular expertise to offer to this Court which we believe will be of great use in the determination

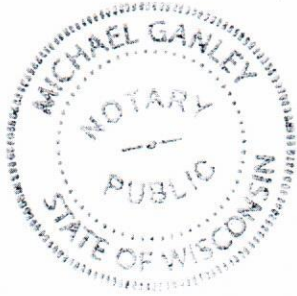
of the legal issues in the main cause. *(The details about our yearly conference RightsCon can be viewed at <https://www.rightscon.org/>)*

6. That I know that ACCESS NOW has contributed amicus briefs to several courts such as the national courts, including the United States, Cameroon, and Colombia, as well as regional courts, such as the European Court of Human Rights and the Economic Community of West African States Court of Justice (ECOWAS). *(A summary of the cases in which briefs were submitted is hereto attached as annexure 'JS3')*.
7. That I know that ACCESS NOW's amicus briefs and publications have been accepted into and relied upon by the above courts given the wealth of its expertise on the subject matter.
8. That I know that ACCESS NOW's publications have also been accepted/referred to by international bodies, tribunals, commissions, and national government institutions as a source of reliable information on digital ID, right to privacy, and freedom of expression.
9. That I know that ACCESS NOW is neutral and impartial concerning the legal matters that are before this Honourable Court in the main cause.
10. That I know that the interest of ACCESS NOW in this matter before court constitutes fidelity to the law as experts on Digital ID Systems and human rights.
11. That I know that ACCESS NOW is aware of the current system in Uganda that makes it mandatory for one to present a national identification number, or being part of the national identification register acquired through enrolment in the national digital identification system by Ugandans to access SAGE benefits as a form of social security, as well as public health services.
12. That I know that ACCESS NOW has examined the above practice and the existing legal and policy regulatory framework and is ready and willing to provide this Honourable Court with submissions on the impact of the above practices on the right to privacy, freedom of expression, as well as the right to social security and public health ,education, among other rights.

13. That I know that ACCESS NOW has had the opportunity to study the pleadings of the main Application and Affidavits in reply and notes that there is need to resolve the questions around the digital national identification system in Uganda on the one hand, and 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, on the other. These questions have not been dealt with by the pleadings before this Court and yet are important in the Court's determination of the Main Cause and the need to balance access to SAGE with the right to privacy and freedom of expression and equity and inclusion.
14. That I know that the points of law ACCESS NOW has submitted on are novel and will aid the development of jurisprudence of Uganda.
15. That I know that ACCESS NOW's submissions draw attention to relevant matters of law that are useful, focused, and principled.
16. That I know that the intervention of ACCESS NOW would draw upon a substantial body of domestic and international law and reports that will be valuable to this Honourable Court in its adjudication of this matter. *(Attached hereto is a copy of the intended Joint brief of the 2nd, 1st and 3rd Applicants as annexure 'JS4')*
17. That I know that the organization's submission on international, regional, and comparative law in the field of Digital ID Systems, right to privacy and freedom of information and inclusion will give assistance to the Court that it would otherwise not have.
18. That I know that it is in the public interest, interests of justice, the promotion and protection of human rights that the application seeking leave to intervene as Amici Curiae is granted.
19. That whatever is stated herein above is true and correct to the best of my knowledge, belief, and information save where otherwise stated.

SWORN by the said JOSEPH STEELE at Mt. Wankole, W1 (Location of
the notary public) on this 4 day of November 2022

Joseph Steele
DEPONENT



BEFORE ME

Michael Ganley

A NOTARY PUBLIC

Jointly Drawn and filed by:

M/s Thomas and Michael Advocates
Plot 127 Muteesa II Road, Ntinda
P.O. BOX 73577 Kampala
0782 285999, 0779 201692
thomasmichaeladvocates@gmail.com

AND

M/s MOM Advocates
2nd floor Ntinda Shopping Centre,
Suite C08 and C09,
Ntinda-Kampala



Secretary of State Certificate of Status

"JS1"

I, SHIRLEY N. WEBER, PH.D., California Secretary of State, hereby certify:

Entity Name: ACCESS NOW
Entity No.: 3232201
Registration Date: 07/31/2009
Entity Type: Nonprofit Corporation - CA - Public Benefit
Formed In: CALIFORNIA
Status: Active

The above referenced entity is active on the Secretary of State's records and is authorized to exercise all its powers, rights and privileges in California.

This certificate relates to the status of the entity on the Secretary of State's records as of the date of this certificate and does not reflect documents that are pending review or other events that may impact status.

No information is available from this office regarding the financial condition, status of licenses, if any, business activities or practices of the entity.



IN WITNESS WHEREOF, I execute this certificate and affix the Great Seal of the State of California this day of September 12, 2022.

SHIRLEY N. WEBER, PH.D.
Secretary of State

Certificate No.: 044237327

To verify the issuance of this Certificate, use the Certificate No. above with the Secretary of State Certification Verification Search available at bizfileOnline.sos.ca.gov.

ACCESS NOW’s list of publication on the issue of Digital ID:

1. Digital Identity: Our five calls to action for the World Bank (Sep. 28, 2022), <https://www.accessnow.org/digital-identity-world-bank/>
2. #WhyID: World Bank and dangerous digital ID systems do not mix (Sep. 7, 2022), <https://www.accessnow.org/world-bank-digital-id-systems/>
3. The Jamaica NIDS digital identification program: a cautionary tale (Aug. 3, 2022), <https://www.accessnow.org/jamaica-nids-digital-id/>
4. Biometric ID in Tunisia: a threat to privacy and data protection (Apr. 13, 2022), <https://www.accessnow.org/biometric-id-tunisia/>
5. Go back to the drawing board: Kenya must scrap unconstitutional Huduma Bill 2021 (Feb. 23, 2022), <https://www.accessnow.org/kenya-scrap-huduma-bill/>
6. Human rights organizations call for dropping the draft bill introducing biometric passports and ID cards in Tunisia (Jan. 31, 2022), <https://www.accessnow.org/draft-bill-biometric-passports-id-tunisia/>
7. We need to talk about digital ID: why the World Bank must recognize the harm in Afghanistan and beyond (Oct. 14, 2021), <https://www.accessnow.org/digital-id-world-bank/>
8. Busting Big ID’s myths (Oct. 5, 2021), <https://www.accessnow.org/busting-big-ids-myths/>
9. India’s Aadhaar proves Big ID is still a bad idea (Oct. 5, 2021), <https://www.accessnow.org/indias-aadhaar-big-id-bad/>
10. #WhyID: Organizations call on the government of Mexico to halt biometric digital ID (Sep. 23, 2021), <https://www.accessnow.org/mexico-unique-digital-id/>
11. Jamaica’s NIDS bill: human rights recommendations dismissed, still time to rectify (Jul. 30, 2021), <https://www.accessnow.org/jamaica-nids-bill-human-rights-recommendations-dismissed/>
12. Protocol for exclusion: Why COVID19 “passports” threaten human rights? (Apr. 2021), <https://www.accessnow.org/cms/assets/uploads/2021/04/Covid-Vaccine-Passports-Threaten-Human-Rights.pdf>
13. Civil society speaks out on Jamaica’s dubious new digital ID bill (Mar. 16, 2021), <https://www.accessnow.org/civil-society-response-jamaica-digital-id-bill/>
14. Statement: Tunisia’s newly proposed biometric ID and e-passport threaten privacy (Mar. 9, 2021), <https://www.accessnow.org/tunisia-biometric-id-passport-threaten-privacy/>
15. Civil society organizations call for a full integration of human rights in the deployment of digital identification systems (Dec. 17, 2020), <https://www.accessnow.org/civil-society-call-for-human-rights-in-digital-identification-systems/>
16. #WhyID: Digital health certificates are not immune from violating users’ rights (Jul. 22, 2020), <https://www.accessnow.org/whyid-digital-health-certificates-are-not-immune-from-violating-users-rights/>
17. Government responses to COVID-19 reinforce the need to ask — #WhyID? (Apr. 29, 2020), <https://www.accessnow.org/government-responses-to-covid-19-reinforce-the-need-to-ask-whyid/>
18. #WhyID: Access Now responds to World Bank Principles on Identification for Sustainable Development (Apr. 1, 2020), <https://www.accessnow.org/whyid-access-now-responds-to-world-bank-principles-on-identification-for-sustainable-development/>

19. #WhyID: Human rights groups press for critical evaluation of digital identity programs (Oct. 21, 2019), <https://www.accessnow.org/whyid-human-rights-groups-press-for-critical-evaluation-of-digital-identity-programs/>.
20. Internet access, digital ID, data protection, surveillance controls: UPR review highlights threats to digital rights (Oct. 15, 2019), <https://www.accessnow.org/internet-access-digital-id-data-protection-spyware-upr-review-highlights-threats-to-digital-rights/>.
21. India’s update to Aadhaar — a failure to fix the world’s largest biometrics-based national digital ID programme (Jun. 26, 2019), <https://www.accessnow.org/indias-update-to-aadhaar-a-failure-to-fix-the-worlds-largest-biometrics-based-national-digital-id-programme/>.
22. As Aadhaar amendment Bill lapses, Indian policymakers should rethink the digital identity project (Feb. 26, 2019), <https://www.accessnow.org/as-aadhaar-amendment-bill-lapses-indian-policymakers-should-rethink-the-digital-identity-project/>.
23. Supreme Court of India rules to restrict world’s largest digital identity framework (Aadhaar) — but debate continues (Sept. 26, 2018), <https://www.accessnow.org/supreme-court-of-india-rules-to-restrict-worlds-largest-digital-identity-framework-aadhaar-but-debate-continues/>.
24. National Digital Identity Programmes: What’s Next (May 2018), <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>
25. Digital identity programs: what could go wrong? Our contribution at UNCTAD’s E-Commerce Week (Apr. 19, 2018), <https://www.accessnow.org/digital-identity-programs-what-could-go-wrong-our-contribution-at-unctads-e-commerce-week/>.
26. Biometric ID vs. privacy: Tunisians win on privacy! But it’s not over yet (Jan. 11, 2018), <https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/>.
27. Tunisia’s “Aadhaar”? Read the draft law for a dangerous new ID, now in English (Aug. 30, 2017), <https://www.accessnow.org/tunisia-aadhaar-read-draft-law-dangerous-new-id-now-english/>.

ACCESS NOW list of cases in which briefs were submitted in national and regional courts:

1. ECOWAS Court victory: Twitter ban in Nigeria declared unlawful (Jul. 14, 2022), <https://www.accessnow.org/ecowas-court-nigeria-unlawful-twitter-ban/>.
2. Double win! Court rejects NSO’s attempts to silence victims and derail surveillance lawsuit (Nov. 9, 2021), <https://www.accessnow.org/court-rejects-nso-attempts-to-derail-surveillance-lawsuit/>.
3. Privacy win for 350,000 people in São Paulo: court blocks facial recognition cameras in metro (May 12, 2021), <https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/>.
4. Judge rules for California in net neutrality challenge, will allow state to enforce net neutrality law (Feb. 24, 2021), <https://www.accessnow.org/judge-rules-for-california-net-neutrality/>.
5. No impunity for American companies committing rights violations, says civil society to U.S. Supreme Court (Oct. 22, 2020), <https://www.accessnow.org/human-rights-violations-u-s-supreme-court/>.
6. ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal (Jun. 25, 2020), <https://www.accessnow.org/internet-shutdowns-in-togo-illegal/>.
7. Access Now joins amicus brief in defense of OTF (Jun. 24, 2020), <https://www.accessnow.org/access-now-joins-amicus-brief-in-defense-of-otf/>.
8. Collateral website blocking unlawful: European Court of Human Rights orders Russia to pay €12,000 in damages (Jun. 23, 2020), <https://www.accessnow.org/collateral-website-blocking-unlawful-russia/>.
9. Court rules the internet shutdowns in Papua and West Papua were illegal (Jun. 3, 2020), <https://www.accessnow.org/court-rules-the-internet-shutdowns-in-papua-and-west-papua-are-illegal/>.
10. Access Now files new legal intervention in Cameroon against shutdowns (Aug. 2, 2018), <https://www.accessnow.org/access-now-files-supporting-intervention-in-renewed-legal-challenge-to-internet-shutdown-in-cameroon/>.

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 an 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 People's 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.D_QCX.

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/29/39>. 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%20web.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

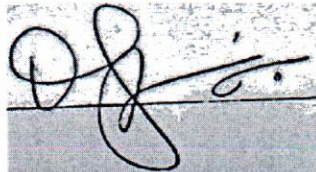
On behalf of **ACCESS NOW** by **JOSEPH STEELE**, Chief Operating Officer, Access Now

SIGNATURE



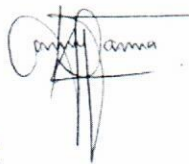
On behalf of **ARTICLE 19** by **MUGAMBI KIAI**, Regional Director, Article 19

SIGNATURE



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

SIGNATURE



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

3RD APPLICANT'S AFFIDAVIT IN SUPPORT OF NOTICE OF MOTION

I MUGAMBI KIAI of C/o M/S Thomas and Michael Advocates, Plot 127 Muteesa II Road,
Ntinda, P. O Box 75377, Kampala and M/s MOM Advocates 2nd floor Ntinda Shopping
Centre, Suite C08 and C09, Ntinda-Kampala do hereby by solemnly make oath and state:

1. That I am an adult male Kenyan of sound mind and the Regional Director Eastern Africa of the 3rd Applicant (Article 19: GLOBAL CAMPAIGN FOR FREE EXPRESSION) (hereinafter referred to as ARTICLE 19), I am the duly authorized

1

representative of the 3rd Applicant and swear this affidavit in that capacity in support of the application by the Applicants to be admitted as *Amici Curiae* in Miscellaneous Cause No 86 of 2022.

2. That I know that ARTICLE 19 is an international non-governmental organization duly registered in Kenya under the Non-Governmental Organizations Coordination Act. ARTICLE 19 forms part of ARTICLE 19 Global, an international nonprofit organization founded in 1987 and 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. *(A copy of the certificate of registration is hereto attached as annexure 'MK1')*
3. That I know that ARTICLE 19 works towards promoting and protecting freedom of expression and access to information, media freedom, and attendant rights in Eastern Africa, both offline and online and extends the digital rights of people and communities at risk around the world. The Organisation was registered in the Republic of Kenya in 2007 and works across the Eastern Africa region in seven (7) countries including Kenya, Tanzania, Uganda, Rwanda, South Sudan, Ethiopia, and Malawi.
4. That I know that ARTICLE 19 contributes to the protection and promotion of freedom of expression, right to privacy and access to information through its focus on the thematic areas of Digital Rights, Media Freedom, Civic Space, Transparency, and Protection litigation. The Organisation employs public interest litigation at various levels as an advocacy tool to promote the implementation of laws and policies and foster the growth of standard-setting jurisprudence that is informed by global best practices. ARTICLE 19 requests leave to appear in the present case as *Amicus Curiae* contributing its expertise and knowledge of international practice on relevant international and comparative law and jurisprudence. *(A link about*

who Article 19 is and what it does is herein provided;
<https://www.article19.org/what-we-do/>)

5. That I know that one of ARTICLE 19's approaches in furthering the freedom of information, right to privacy and freedom of expression include cutting-edge research and legal and policy analysis to drive change around the world. In this regard, the Organisation has published numerous research reports that provide useful references for various stakeholders, leveraging on our work across various parts of the World, through our regional offices, in 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. (*A list/summary of these publications are hereto attached as annexure 'MK2'*)
6. That I Know that ARTICLE 19 wields expertise in assessing the impacts of various technologies on human rights with a view to ensuring respect for human rights and advocating for action on emerging challenges such as the risks posed to the rights to privacy and expression, arising from mandatory collection of data, the digital divide in recognition of the risks posed to the vulnerable and marginalized groups such as the elderly, persons with disabilities in society in order to promote equity and inclusion in society and therefore, it has particular expertise to offer to this Court which we believe will be of great use in the determination of the legal issues in the main cause.
7. That I know that ARTICLE 19 has, over the past three years, in Kenya been involved in the consultations around data protection and the regulation of the digital ID system commonly referred to as "*Huduma Namba*". The Organisation 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. *(A summary of the joint submissions made by ARTICLE 19 to different government Institutions in Kenya is hereto attached as annexure 'MK3').*

8. That I know that ARTICLE 19's has submitted various briefs as an intervener and amicus by filing amicus briefs, written submissions, intervener submissions, Third Party intervention submissions in various courts and tribunals such as the Administrative Court in the United States of America, European Court of Human Rights, Constitutional Court of the Republic of Korea, Lebanon Special Tribunal, on the right to privacy and freedom of expression and these submissions have been considered by the tribunal and the courts. *(A list of brief and submissions are hereto attached as annexure 'MK4').*
9. That 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. *(A list and links to relevant reports arising from cutting-edge research on the impact of emerging biometric technologies on Human rights is hereto attached as annexure 'MK5').*
10. That ARTICLE 19 has conducted extensive legal analysis and submitted memoranda on the use of biometrics and digital rights and the right to privacy to various bodies and mechanisms such as the Kenyan Parliament, Ministry of ICT and the Office of the United Nations High Commissioner For Human Rights. *(A list of the Legal Analysis and Memoranda is also hereto attached as annexure 'MK6').*

11. That I know that ARTICLE 19 is aware of the current system in Uganda that makes it mandatory for one to present a national identification number or being part of the national identification register acquired through enrolment in the national digital identification system by Ugandans to access SAGE benefits as a form of social security, as well as public health services.
12. That ARTICLE 19 has examined the above practice and the existing legal and policy regulatory framework and is ready and willing to provide this honourable Court with submissions on the impact of the use of biometrics on the right to privacy and freedom of expression, as well as the intersecting social, economic and cultural rights.
13. That ARTICLE 19 has had the opportunity to study the pleadings of the main Application and Affidavits in reply and notes that there is need to resolve the questions around the digital national identification system in Uganda on one hand and the impact of the design of these technologies and how they impact on identity verification, identification, surveillance, and inference of attributes, including emotional states as against the international standards and state obligations on protection of the right to privacy and freedom of expression even at the instance of a roll out of a good government program like SAGE on the other. This issue has not been fully canvassed in the pleadings before court and yet are important in the Court's determination of the Main Cause.
14. That I know that ARTICLE 19 has jointly drafted, together with the 1st and 2nd Applicants the Amicus brief touching the matters deponed in this affidavit which the same has been submitted to this honourable Court which will give assistance to the court that it would otherwise not have.
15. That I know that the points of law ARTICLE 19 has submitted on are novel and will aid the development of jurisprudence of Uganda.

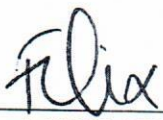
16. That I know that ARTICLE 19's submissions draw attention to relevant matters of law that are useful, focused, and principled.
17. That I know that ARTICLE 19 is neutral and impartial concerning the legal matters that are before this honourable Court in the main cause.
18. That I know that the interest of ARTICLE 19 in this matter before the honorable Court constitutes fidelity to the law as experts on Digital Identity Systems and attendant rights.
19. That I know that it is in the public interest, interests of justice, and the promotion and protection of human rights that the application seeking leave to intervene as *Amicus Curiae* is granted.
20. That whatever is stated herein above is true and correct to the best of my knowledge, belief and information save where otherwise stated.

SWORN by the said MUGAMBI KIAI at NAIROBI on this 3rd day of November 2022


DEPONENT

BEFORE ME




A NOTARY PUBLIC

6

Jointly Drawn and filed by:

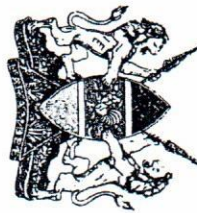
*M/s Thomas and Michael Advocates
Plot 127 Muteesa II Road, Ntinda
P.O.BOX 73577 Kampala
0782 285999, 0779 201692
thomasmichaeladvocates@gmail.com*

AND

*M/s MOM Advocates
2nd floor Ntinda Shopping Centre,
Suite C08 and C09,
Ntinda-Kampala*

"MK1"

FORM 5



REPUBLIC OF KENYA
OFFICE OF THE PRESIDENT
OP. 218/051/2007/0279/4744



(T. 1

CERTIFICATE OF REGISTRATION

I, **WYCLIFFE AWUORI MUTSUNE**, Chairman of the Non-Governmental Organizations Board, certify that the **xxx ARTICLE 19: GLOBAL CAMPAIGN FOR FREE EXPRESSION xxx** has this day been registered under section 10 of the Non-Governmental Organization Co-ordination Act as applied for.

59

W.A. MUTSUNE
Chairman of the Board

Dated **27TH SEPTEMBER, 2007**

GPK (L)

ARTICLE 19 list of Publications

1. *When bodies Become Data: Biometric Technologies and Freedom of Expression* (2021) that highlights the applicable human rights standards in the implementation of Biometric technologies <https://www.article19.org/wp-content/uploads/2021/04/A19-Biometric-technologies-and-FoE-Policy-2021.pdf>
2. *Who buys and controls the CCTV? Myanmar slippery slope to mass surveillance* (2022), which analyzes the impact of surveillance and biometric identification on human rights <https://www.article19.org/wp-content/uploads/2022/08/A19-Smart-Cities-Aug22.pdf>
3. *Privacy and Freedom of Expression in the age of artificial intelligence* (2018), which analyzes the impact of AI on the right to privacy and free expression and recommends safeguards to ensure these rights are realized. <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>
4. *The Global Principles on Freedom of Expression and Privacy*(2017), <https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf>
5. *Emotional Entanglement: China’s emotion recognition market and its impact on human rights* (2021), which analyzes the use of these technologies to deliver social services and their impact on human rights <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>
6. *Governance with Teeth: How human rights can strengthen FAT and ethics initiative on artificial intelligence* (2019) https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf

ARTICLE 19 List of submissions to different government institutions

1. Joint Memorandum asks for Huduma Bill to fully protect rights (2022)
<https://www.article19.org/resources/kenya-joint-memorandum-asks-for-huduma-bill-to-fully-protect-rights/>
2. ARTICLE 19 Eastern Africa memorandum to the Ministry of ICT in Kenya on the draft Data Protection Regulations 2021 (2021) <https://www.article19.org/wp-content/uploads/2021/07/ARTICLE-19-Eastern-Africa-Memorandum-Draft-Data-Protection-Regulations-11.05.2021.pdf>
3. Kenya: Protect the data protection framework (2019)(<https://www.article19.org/resources/kenya-protect-the-data-protection-framework/>)
4. Submission to the Office of Science and Technology Policy on Human rights approach to Private and Public use of biometric technologies(2022)
<https://www.article19.org/wp-content/uploads/2022/01/OSTP-biometrics-consultation.pdf>

ARTICLE 19 List of Briefs, submissions, interparty submissions submitted to various courts

1. Written submission by ARTICLE 19 and Privacy International in Patrick Beyer and Jonas Beyer v Germany, (European Court of Human Rights) Application No. 5001/12 that elaborates upon the right to anonymity and freedom of expression in the context of evaluating data retention requirements under the German Federal Telecommunications Act
https://privacyinternational.org/sites/default/files/201810/2016.09.05_PI_and_A19_Intervention.pdf
2. Third Party intervention submissions by ARTICLE 19 in the Constitutional Court of the Republic of Korea Application Number 2016Heonma388 in consideration of the freedom of expression and privacy to discuss the compliance of articles 83 (3) and 83 (4) of the Telecommunications Business Act with the International standards on Privacy and Free expression <https://www.article19.org/wp-content/uploads/2018/02/Korea-amicus-Brief-ARTICLE-19.pdf> that following our intervention, led the court to reaching a decision that safeguard human rights in particular right to privacy <https://www.article19.org/resources/south-korea-data-sharing-unconstitutional/>
3. Amicus Brief by ARTICLE 19 in the case against AL Jadeed [CO.] S.A.L./ NEW T.V. S.A.L. (N.T.V.) KARMA MOHAMED TAHSIN AL KHAYA in the Special Tribunal for Lebanon Case Number STL-14-05/T/CJ
<https://www.article19.org/data/files/medialibrary/37927/A19-KKhayat-amicus-FINAL.pdf>
4. Intervener submissions by ARTICLE 19 on the Appeal between The Queen (On the Application of Guardian News and Media Limited) and City of Westminster Magistrate Court and The Government of the United States of America ADMINISTRATIVE COURT CO/7737/10, CO/7272/10
<https://www.article19.org/data/files/medialibrary/3011/A19---GNM-Appeal--26-1-12-FINAL.pdf>

ARTICLE 19 list of Publications including Cutting-edge research on the impact of emerging biometric technologies on Human rights (Reports)

1. *When bodies Become Data: Biometric Technologies and Freedom of Expression* (2021) that highlights the applicable human rights standards in the implementation of Biometric technologies <https://www.article19.org/wp-content/uploads/2021/04/A19-Biometric-technologies-and-FoE-Policy-2021.pdf>
2. *Who buys and controls the CCTV? Myanmar slippery slope to mass surveillance* (2022), which analyzes the impact of surveillance and biometric identification on human rights <https://www.article19.org/wp-content/uploads/2022/08/A19-Smart-Cities-Aug22.pdf>
3. *Privacy and Freedom of Expression in the age of artificial intelligence* (2018), which analyzes the impact of AI on the right to privacy and free expression and recommends safeguards to ensure these rights are realized. <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>
4. *The Global Principles on Freedom of Expression and Privacy*(2017), <https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf>
5. *Emotional Entanglement: China’s emotion recognition market and its impact on human rights* (2021), which analyzes the use of these technologies to deliver social services and their impact on human rights <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>
6. *Governance with Teeth: How human rights can strengthen FAT and ethics initiative on artificial intelligence* (2019) <https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth A19 April 2019.pdf>

ARTICLE 19 list of Legal Analysis and Memoranda

1. Digital Identification must protect human rights (2021)
<https://www.article19.org/resources/consortium-calls-for-reforms-implementation-of-kenyas-digital-id/>
2. Joint Memorandum asks for Huduma Bill to fully protect rights (2022)
<https://www.article19.org/resources/kenya-joint-memorandum-asks-for-huduma-bill-to-fully-protect-rights/>
3. Submission by ARTICLE 19 to the UN OHCHR in response to the call for inputs to a report on the “right to privacy in the digital age” (2018)
<https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Article19.pdf>
4. ARTICLE 19 Eastern Africa memorandum to the Ministry of ICT in Kenya on the draft Data Protection Regulations 2021 (2021) <https://www.article19.org/wp-content/uploads/2021/07/ARTICLE-19-Eastern-Africa-Memorandum-Draft-Data-Protection-Regulations-11.05.2021.pdf>
5. Kenya: Protect the data protection framework (2019) (<https://www.article19.org/resources/kenya-protect-the-data-protection-framework/>)
6. Submission to the Office of Science and Technology Policy on Human rights approach to Private and Public use of biometric technologies(2022)
<https://www.article19.org/wp-content/uploads/2022/01/OSTP-biometrics-consultation.pdf>

The Applicants shall adduce evidence at the hearing that they possess knowledge and expertise in matters concerning Digital Identity systems, right to privacy, civil and political rights among others, that their submissions on points of law are novel and will aid the court in arriving at a proper conclusion hence it is in the interests of justice and proper determination of the main cause that the applicants be admitted as amici.

LIST OF DOCUMENTS

- a) Annexures to the affidavits of Joseph Steele, Wanyama Edrine and Mugambi Kiai
- b) Any other with leave of the court

LIST OF AUTHORITIES

- a) As indicated in the formal brief
- b) Others with leave of the court.

DATED at Kampala this 4th day of November 2022

[Signature] [Signature]

M/s Thomas & Michael Advocates

M/s MOM Advocates

(COUNSEL FOR THE APPLICANTS)

Jointly Drawn and filed by:

M/s Thomas and Michael Advocates AND

M/s MOM Advocates

Plot 127 Muteesa II Road, Ntinda

2nd floor Ntinda Shopping Centre

P.O.BOX 73577 Kampala

Suite C08 and C09, Ntinda-Kampala

0782 285999, 0779 201692

thomasmichaeladvocates@gmail.com