****

**United Nations Special Rapporteur on Extreme Poverty and Human Rights Call for Submissions U.N. Human Rights Council report: “Social Protection: a reality check”**

17 December 2021

**Introduction**

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Special Rapporteur on Extreme Poverty and Human Rights report: “Social Protection: a reality check” to be presented to the U.N. Human Rights Council at its 50th session in June 2022.[[1]](#footnote-0) As an ECOSOC accredited organisation, Access Now routinely engages with U.N. Special Procedures in support of our mission to defend and extend the digital rights of users at risk worldwide.[[2]](#footnote-1) We also facilitate the #WhyID community of more than 250 organisations and experts from across the world working towards ensuring that digital identity programmes respect the rights of users.[[3]](#footnote-2)

This submission addresses the following question from the call for inputs: *To what extent do conditionalities attached to the granting of social protection benefits undermine social protection systems? What is the impact of such conditionalities on people who experience poverty?*

**From social inclusion to exclusion: Digital Identity as a conditionality to access social protection**

1. Social protection is essential to address poverty. One of the challenges found in the delivery of public services is that many people -- especially those who experience marginalization based on intersecting identities -- do not have a legal identity. As part of broader efforts to counter this problem, many countries worldwide, and even international bodies, continue to promote and implement digital identity systems. These systems add technology to the civil registry that are used to both give legal identity and also verify someone's identity. Proponents of digital identity systems argue that the technology will make the delivery of social services more efficient, reduce corruption by using technology to assist in clear identification and secure authentication, amongst other factors. However, as indicated in the case studies below, this is not always true. Such technology-based digital identity systems may in fact: store the inhabitants’ personal data in centralized digital databases, use a digital platform to manage the identity information, collect highly sensitive biometric data as another attribute to assign or verify a legal identity, use digital technologies to authenticate people’s identity, and more.
2. Many around the world still lack a legal identity. This is so important that the U.N. Sustainable Development Goal (SDG) 16.9 specifically calls on states to provide legal identity for all, including birth registration by 2030. In 2021, this continues to be a pending debt from states, as having a legal identity is a right we are entitled to have according to Article 6 of the Universal Declaration of Human Rights and Article 16 of the International Covenant on Civil and Political Rights.
3. Even if access to a legal identity is a human right, and should be a priority in national and international agendas, it does not mean that a lack of it should have an impact on or result in not receiving social assistance. **Social aid should be provided to people who have and do not have a legal identity** for two main reasons. First, people who do not have documentation to prove their identity usually belong to marginalized groups, and therefore already suffer from systemic forms of discrimination and poverty. People in such instances are not in a position to wait to get a legal identity first to later be eligible to receive social aid. Second, providing social aid does not only benefit the person who is receiving it, but also the community where a person lives in, therefore social aid is for all human beings no matter their legal status.
4. Nevertheless, the promoters of digital identity as a tool for better delivery of social services tend to suggest that these problems can be solved with technology. However, current issues in the delivery of social aid is the result of many problems, including structural, that cannot be magically solved with technology. In some cases, the registry of people entitled to receive aid is outdated, has errors, or is incomplete. In other cases, there is stru ctural discrimination in the country that impedes some people from being visible to the state. Moreover, there are corruption problems and technological and educational gaps. In all these situations, using digital identity technology only exacerbates ongoing problems while adding additional concerns through the processing of vast amounts of personal data.
5. In the case of **databases with errors**, any technology that will use it will give wrong outputs. For example, a digital identity system that aims to authenticate identity by using facial recognition technology can end up excluding those whose faces do not match with the template saved in the system. As evidenced by the country-specific case studies described in this submission below, this has happened and it carries with it major risks. Additionally, there is a common misheld belief that technology “does not lie.” In other words, it is less likely that someone will doubt the results given by a digital system than results obtained from analogical processes. If this is true, then paper based information will have less credibility than the outputs of the digital identity system. This can therefore become problematic for people who only have paper documents that certifies their needs and identity.
6. Furthermore, **structural social problems** can become more problematic if a digital identity system is implemented without taking measures to account for systemic issues. A common example is ethnic minorities. Minorities suffer the most as they stay invisible in the eyes of the state. In some countries making them invisible is part of the culture and history. In this sense, there are already barriers in place to be integrated into the country. For minorities, accessing a legal identity is difficult and even more so to access a social service. A digital identity system that does not take into account these problems will only care for digitizing the civil registries that already exclude minorities.
7. Digital identity systems can also create more **opacity** in the ongoing civil registry system. Proponents of digital identity systems argue that technology enables more traceability which can help fight against corruption, which is particularly important in the delivery of social aid. Nonetheless, a state that already lacks transparency in its actions is less likely to become more transparent just because technology is involved. Technology cannot help to achieve this objective if the government does not have regulations in place to mandate transparency and accountability. Moreover, even if the use of digital technologies has heavily increased in the past years, it does not mean that everyone understands how it works.
8. Finally, proponents of digital identity systems rarely consider the existing **gaps** in the country and that are more pronounced for people who experience poverty. These gaps include access to technology, including mobile phones, to a lack of digital literacy. The implementation of the digital identity system creates a problem when there are cities and villages with no electricity, no internet connection, or no electronic devices. Moreover, inhabitants who do not have access to education or do not acknowledge the benefits and dangers of the system are unable to provide informed consent to the processing of their personal data, nor to exercise their rights. This is especially important when people have to apply or are enrolled to receive social aid through a digital identity system. These programmes and digital identity systems process vast amounts of personal data including biometric data (e.g. thumbprints or iris scans) which are usually stored in centralized databases. A system designed without proper safeguards and without public scrutiny could put all that information in risk of being manipulated, hacked, stolen and more. In particular, if biometric information gets compromised, the harms are irreparable for the people as biometric information can not be easily changed. However, people who are in need have no choice but to accept the conditions proposed by governments. Meaning that there is no opportunity to freely decide and question the authorities on how their data can be processed.
9. Without proper human rights safeguards that are rigorously followed, digital identity systems can be counterproductive to the welfare of the people, violate internationally protected human rights, and undermine our cybersecurity. It is imperative that the safeguards - legal, technological, and scheme governance - be adopted holistically, and the adoption of one does not preclude the adoption of the others. If the necessary safeguards are not holistically included in digital identity systems, we recommend that they halt, be restructured where possible, or else reconsidered. In all these situations there is potential risk to exclude people who are the ones that need the most social aid. This multifaceted way of exclusion is extremely worrying.[[4]](#footnote-3)

**The impact of digital identity programs in the real world: country-specific case studies**

1. Below we provide more information on country-specific case studies to provide more details on how people that experience poverty could be at risk if digital identity systems are deployed without taking strong precautions, implementing human rights safeguards, and ensuring access to effective remedies.

**India - Aadhaar**

1. India has a population of 364 million people living in poverty conditions (as per 2019 UN figures), requiring social assistance. Claims around the use of technology to improve social assistance, help with better “targeting” of those in poverty has been one of the main excuses for the implementation of the Aadhaar Unique ID project. Aadhaar’s architects and other Big ID advocates have held up Aadhaar as the poster child for similar large-scale public-sector digital identity programs across the Global South.[[5]](#footnote-4) It was supposed to solve two main issues: remove corruption from welfare and enable efficient, transparent, and secure digital transactions. However, since its inception, Aadhaar has had disastrous impacts on welfare systems, many of which have been extensively documented by activists, scholars, lawyers, and academics in India.[[6]](#footnote-5) Therefore it became a barrier that has affected the life of 1.2 billion people.

1. We would like to highlight how this happens with two examples[[7]](#footnote-6):
* *A system that fails to identify the citizens:* Aadhaar collects biometrics such as face, fingerprints and iris and uses them in the enrollment process to void double registries and then to verify the identity of someone. Nevertheless, biometric technology is still not 100% accurate, nor the personal data stored. In that sense, the system tends to fail in the authentications and the deduplication purposes, meaning it cannot verify someone's identity. These people get excluded or have to take additional steps to receive their social assistance (food ratios).[[8]](#footnote-7)
* *More opacity about how the system operates:* Contrary to what has been advertised, Aadhaar is not providing transparency. Although there are two laws about access to information and food security [[9]](#footnote-8) that hold the government accountable by making its decisions accessible and transparent, the *Aadhaar Act* and project inverted this mandate. Since then, “(...) decisions about you are made by a centralized server, and you don’t even know what has gone wrong.”[[10]](#footnote-9) On top of that, the Unique Identification Authority of India refused[[11]](#footnote-10) to answer Right to Information requests on the number of Aadhaar authentication requests that had failed, claiming “national security and confidentiality” exceptions.[[12]](#footnote-11)

**Kenya - Huduma Namba**

1. In 2019, the Kenya government introduced a new mandatory and biometric ID system without due regard to the potential privacy, data protection and surveillance shortfalls that could befall it.[[13]](#footnote-12) This new ID called “Huduma Namba” quickly received criticism, and human rights advocacy groups challenged its implementation in court. The court ordered a suspension and demanded the government to address exclusion risks towards some groups of people, among others, and to enact proper regulation.[[14]](#footnote-13) This was partially fulfilled with a *Data Protection Act* and the The Registration of Persons (National Integrated Identity Management System) Rules; which later were used by human rights advocates as an argument to state that the system was in place without complying with data protection regulations. This last challenge was recently addressed by the Court who had declared the roll out of the system in conflict with the Data Protection Act.[[15]](#footnote-14) Besides that, the roll out has also exacerbated problems of exclusion towards historically marginalized groups of people.
2. *A system that exacerbates ethnic discrimination:* Kenya has a long history of discrimination against minorities, specially minority groups. That is the case of the Nubians who arrived in Kenya 100 years ago. Prior to the introduction of the Huduma Namba, they were facing stringent, overzealous and intrusive processes getting identity documents as Kenyan citizenship was not granted to them automatically. This problem was even addressed by the African Commission on Human and People’s Rights who found that the process of civil registration based on ethnic identity violated the African Charter on Human and People’s Rights.[[16]](#footnote-15) Nonetheless, when the new digital system was introduced this problem was not addressed. With the rollout of Huduma Namba, Nubians will have to face another challenge: access to a digital citizenship on top of the long civil registry vetting process. Without a recognised form of ID, Nubians cannot exercise different rights such as education, have property, nor access to social aid programs. This can affect the chances to get out of poverty and condemns them to be marginalized.[[17]](#footnote-16)

**Argentina - IFE (Ingreso Familiar de Emergencia Covid)**

1. Since 1968, Argentina has had a foundational and centralized digital identity system.[[18]](#footnote-17) In 2009, the National Registry of Persons (RENAPER) of the Ministry of Interior, Public Works and Housing, has the power to “utilise digital technologies for the identification of national and foreign citizens.”[[19]](#footnote-18) Three years later, the National Identity Document (DNI) started storing biometric information on a RFID chip[[20]](#footnote-19) and some years later the RENAPER created an online platform to host the digital identity system. Through all these years, having a foundational ID document has been normalized among the population. The RENAPER even promotes it as the door to access someone’s rights.[[21]](#footnote-20) The national registry database is the base and source for multiple purposes including social services. Therefore, a person who does not have a DNI, such as migrants, does not exist. Nevertheless, this normalization has brought problems and serious accusations regarding mass surveillance practices and how it can affect people living in contexts that are not fully digitized.
2. *A system that fails due to technological and educational gaps:* Argentina has serious economic struggles which impact on how people engage with technology. According to the Instituto Nacional de Estadísticas y Censos (INDEC) of 2,8 million people who answered their survey, 1,4 are not employed and 3 work informally.[[22]](#footnote-21) These groups of people suffered the most during the COVID-19 pandemic. In response, the federal government launched a social program called IFE (Ingreso Familiar de Emergencia Covid)[[23]](#footnote-22) that seeked to provide money support to families who were not earning enough money to survive. Although the purpose is fair, the only way to apply for it was on digital platforms. If approved, the person had to open a bank account using their DNI and verify his/her identity using the digital identity system. People who did not have adequate electronic devices, good internet connection, knowledge on how to use the platform, or had doubts about doing it by themselves had problems accessing the social benefit. [[24]](#footnote-23) In Argentina, only 29.1% of people that experience poverty have a strong link and knowledge with electronic devices.[[25]](#footnote-24) These people are 16 times more likely to be digitally excluded than people living in the highest socioeconomic stratum.[[26]](#footnote-25)

**Concluding Recommendations**

1. States
* States should not condition the provision of social assistance to the possession of a digital identity document. Forcing people to be part of a digital identity system has the potential to exacerbate current problems and could further marginalize and exclude people from getting social aid.
* It is imperative that digital identity systems, particularly those foundational systems backed by the state’s resources and legal powers, have an inclusion by design principle in its core. A decision to implement those systems should not leave anyone out of the protection of the state. States should understand that as our realities are diverse, then the solutions to our identification problems should be too.
* Digital identity systems must comply with principles of governance, data protection, privacy, and security. [[27]](#footnote-26)
* States should acknowledge the imbalance of powers between them and the population regarding the processing of personal data in digital identity systems. People living in poverty conditions should not be forced to provide sensitive data such as biometrics or be enrolled for the means of obtaining social aid. States should inform and provide alternatives to the people so their consent is free, explicit, and unequivocal.
1. Private Sector
* Conduct regular human rights due diligence assessments and reviews to identify the potential privacy, security, and discrimination risks of connecting biometric data to the receipt of social services and take steps to mitigate or prevent such risks. Ensure that the results and reporting are made public and ensure transparency.
* Conduct a data protection impact assessment prior to the deployment of products.
* Implement measures to ensure the security of the information collected on individuals.
* Ensure there are remedial processes to redress human rights harms caused or contributed by products or services.
* Forbid by contract the use of their technologies in a manner that can exclude populations, specially the ones living in poverty conditions.
1. International institutions:
* The United Nations, and the Human Rights Council in particular, should call for a moratorium on the collection and use of biometrics (including facial recognition) for authentication purposes in digital identity and social assistance programmes. Digital identity programmes should not collect or use biometrics for the authentication of users, until it can be proven that such biometric authentication is completely safe, inclusive, not liable to error, and is the only method of authentication available for the purpose of the programmes. The harm from the breach of biometric information is irreparable for users and the ecosystem.
* The United Nations, International Developing Banks, and International Aid Organizations should refrain from promoting and financing digital identity systems in countries with poor registry systems, existing social structural problems, lack of transparency rules and compliance, and with strong gaps in the access and knowledge of technology. Implementing a digital identity system where those conditions exist will only exclude communities that live in poverty. On the contrary, these institutions should advocate for identity programs that don't let anyone out.

##### **Access Now (**[**https://www.accessnow.org**](https://www.accessnow.org)**)** defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact:* ***un@accessnow.org***

1. OHCHR, *Call for inputs: Thematic report to the UN Human Rights Council “Social protection: a reality check,”* available at <https://www.ohchr.org/EN/Issues/Poverty/Pages/SocialProtection-RealityCheck.aspx>, 2021. [↑](#footnote-ref-0)
2. Access Now, *About Us*, available at <https://www.accessnow.org/>, 2021. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon. [↑](#footnote-ref-1)
3. Access Now, *#WhyID,* available at <https://www.accessnow.org/whyid/>, 2021. [↑](#footnote-ref-2)
4. Access Now, *National Digital Identity Programmes: What’s Next?*, available at, <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf> at page 2, 2018. [↑](#footnote-ref-3)
5. *See, e.g.*, Unique Identification Authority of India, “Quote/Unquote,” available at https://uidai.gov.in/media-resources/media/quote-unquote.html. [↑](#footnote-ref-4)
6. Access Now, *Busting the Dangerous Myths of Big ID programs: Cautionary Lessons from India*, available online, ​​<https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf>, 2021. [↑](#footnote-ref-5)
7. We acknowledge that Aaadhaar has more problems than the ones we highlight, all of them need urgent attention and solutions. A detailed analysis on the Aadhaar Big ID system can be found in this policy paper: Access Now, *Busting the Dangerous Myths of Big ID programs: Cautionary Lessons from India*, available online, ​​<https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf>, 2021. [↑](#footnote-ref-6)
8. Reetika Khera, *Aadhaar Failures: A Tragedy of Errors*, EPW Engage, available at, <https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare>, 2019. [↑](#footnote-ref-7)
9. *The Right to Information Act* of 2005 and *the National Food Security Act* of 2006. [↑](#footnote-ref-8)
10. Rebecca Ratcliffe, *How a glitch in India's biometric welfare system can be lethal,* The Guardian, available at, <https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation>, 2019. [↑](#footnote-ref-9)
11. Anumeha Yadav, *How efficient is Aadhaar? There's no way to know since the government won't tell,* Scroll.in, April 5, 2017, available at, <https://scroll.in/article/833060/how-efficient-is-aadhaar-theres-no-way-to-know-as-the-government-wont-tell>, 2017. [↑](#footnote-ref-10)
12. Anumeha Yadav, *Under the right to information law, Aadhaar data breaches will remain a state secret,* Scroll.in, March 5, 2017, available at, <https://scroll.in/article/830589/under-the-right-to-information-law-aadhaar-data-breaches-will-remain-a-state-secret>, 2017. [↑](#footnote-ref-11)
13. Nanjala Nyabola, *National digital ID initiatives have a trust problem,* Rest of the World, 5 May 2021, available at, <https://restofworld.org/2021/kenya-digital-id/>, 2021. [↑](#footnote-ref-12)
14. Privacy International, *Kenyan Court Ruling on Huduma Namba Identity System: The Good, the Bad and the Lessons*, available at, <https://www.privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons>, 2020. [↑](#footnote-ref-13)
15. Business Daily, *High Court declares Huduma Namba illegal,* available at, <https://www.businessdailyafrica.com/bd/news/high-court-declares-huduma-namba-illegal--3582926>, 2021. [↑](#footnote-ref-14)
16. Communication 317/2006 - *The Nubian Community in Kenya vs. The Republic of Kenya,* available at, <https://www.achpr.org/public/Document/file/English/communication_317.06_eng.pdf>. [↑](#footnote-ref-15)
17. Open Society Justice Initiative, *Nubian Community in Kenya v. Kenya,* available at, <https://www.justiceinitiative.org/litigation/nubian-community-kenya-v-kenya> [↑](#footnote-ref-16)
18. Ley N. 17.671, *Ley De Identificacion, Registro y clasificacion del Potencial Humano Nacional,* available, <http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28130/texact.htm>. [↑](#footnote-ref-17)
19. Decreto 1501/2009, *Autorízación de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad*, available at <http://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/159070/norma.htm>. [↑](#footnote-ref-18)
20. Asociación por los Derechos Civiles, *The Identity We Can’t Change: How biometrics undermine our human rights,* available online, <https://adc.org.ar/wp-content/uploads/2019/11/0027-B-The-identity-we-can%C2%B4t-change-12-2017.pdf>, 2017. [↑](#footnote-ref-19)
21. Asociación por los Derechos Civiles, *Tu Yo Digital: Descubriendo las narrativas sobre identidad y biometria en América Latina: los casos de Argentina, Brasil, Colombia y México,* available at <https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf>, 2017. [↑](#footnote-ref-20)
22. Instituto Nacional de Estadísticas y Censos (INDEC), 2020, “Encuesta Permanente de Hogares. Mercado de trabajo. Tasas e indicadores socioeconómicos. Tercer trimestre de 2020,” Disponible en: https://www.indec. gob.ar/uploads/informesdeprensa/mercado\_ trabajo\_eph\_3trim20E927D146A5.pdf [↑](#footnote-ref-21)
23. Ministerio de Economia, Argentina, “Ingreso Familiar de Emergencia,” Disponible en: <https://www.argentina.gob.ar/economia/medidas-economicas-COVID19/ingresofamiliardeemergencia> [↑](#footnote-ref-22)
24. Paz Bernaldo, *Llámame por Mi Nombre: Identidad e identidad digital en Argentina,* YOTI (Your Digital Identity), available at <https://www.yoti.com/wp-content/uploads/Call_Me_by_My_Name-ES-Paz-Bernaldo.pdf> and Paz Bernaldo, *The personal cost of accessing COVID financial support in Argentina,* YOTI (Your Digital Identity), available at, <https://www.yoti.com/blog/the-personal-cost-of-accessing-covid-financial-support-in-argentina/>, 2020. [↑](#footnote-ref-23)
25. Universidad Nacional de La Plata, REVCOM. Revista científica de la red de carreras de Comunicación Social, *Tecnologías y estructura social Condiciones estructurales de inclusión digital en la población infantil de Argentina,* núm. 10, 2020, Disponible en:

<http://portal.amelica.org/ameli/jatsRepo/203/2031143008/html/index.html> [↑](#footnote-ref-24)
26. *Ibid.* <http://portal.amelica.org/ameli/jatsRepo/203/2031143008/html/index.html> [↑](#footnote-ref-25)
27. Access Now, *National Digital Identity Programmes: What’s Next?,* available at <https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>, 2018. [↑](#footnote-ref-26)