#WhyID

Open letter: protecting our identity in the digital age

To the leaders of International Development Banks, the United Nations, International Aid Organisations, Funding Agencies, and National Governments.

We are a group of civil society organisations, technologists, and experts who work on digital identity developments across the world. We have worked directly with vulnerable populations, and witnessed the impact that ill-considered, badly designed, and poorly implemented digital identity programmes can have on human lives.

+ A Basic Question: Why ID?

There is a generalised assumption that certain kinds of digital identity programmes[1] empower users, especially those in marginalised populations, by giving them legal identification and access to public services. Digital identity programmes can provide some of the same benefits to users as conventional identity and can reap the benefits of scalability of technology. However, the scalability of digital identity programmes also makes their harms scalable. It is far from being proven that most digital identity programmes have brought additional benefits to users, without placing them at risk.

Current justifications for these programmes are often theoretical, and programmes are deployed without sufficient supportive evidence of the promised benefits. On the other hand, the harms that are suffered by individuals through badly designed and implemented digital identity programmes are real and in many cases, irreparable. Unfortunately, marginalised populations suffer the greatest harm. These digital identity programmes are all too often designed and implemented without a recognition of regional and local realities and without the consultation of key stakeholders including the most vulnerable. If many developed countries have questioned and opposed similar digital identity programmes, why are they being routinely deployed in the developing world?

Human agency and choice form the foundation of human dignity. Humans being enrolled in any programme have a basic human right to understand the system and its justification and participate in designing its structure and implementation. Some basic questions on the objectives, need, and benefits of these digital identity programmes must be answered before pursuing the what, the how, the when, and the who of digital identity.

We write to raise our voice and ask this very first basic question - Why ID?

1. This letter addresses digital identity programmes backed, developed, and deployed by public sector international, regional, and national institutions and organisations.

+ Current Problems with Digital ID Programmes

Most digital identity programmes follow a **centralised and ubiquitous model**, without delivering incremental benefits to users. The central digital identity is linked to multiple other IDs and purposes for each user. This framework provides an ability to track and log everyday activities and transactions of a user.

High profile cases have demonstrated that **these programmes can create the risk of 360 degree profiling and surveillance** of users by governments and private actors with access to the databases associated with such programmes. Such an ecosystem can be hugely detrimental to the fundamental right to privacy of users. The problem is accentuated in countries with a lack of comprehensive privacy and surveillance frameworks, compromised institutional standards, and weak independent enforcement. In such countries, financial incentives become stronger for governments and private businesses to delay and dilute privacy and data protection standards, while enabling risky digital identity programmes.

Some proponents of such centralised programmes defend their deployment to achieve so-called **"single source of truth" models**. **These models, however, end up creating rather a single point of failure**, which may provide access to sensitive information of communities and even entire populations. Such centralised architectures also attract malicious actors and hence represent bad cybersecurity policy. One breach into the ecosystem could destroy the sanctity and safety of the database.

The mandatory nature of most digital identity programmes leads to exclusionary outcomes. Marginalised groups unable to enroll, due to a variety of circumstances, such as poor technology infrastructure, gaps in technology design, etc., are not able to exercise their basic rights. Enrollment in a digital identity programme must be optional. A digital identity cannot be a precondition to access basic services and rights.

Marginalised populations are being affected the most. Populations such as refugees, transgender people, and those affected by HIV are being required to register in digital identity programmes, as a pre-condition to receiving aid. It is distressing to see international institutions and organisations in charge of aid programmes requiring registration to these types of digital identity frameworks. It is essential to understand that vulnerable populations have a complete lack of negotiation power in such circumstances; consent in such circumstances is hardly valid consent and such enrollment can become coercive. It is incumbent on the aid provider to respect the rights of these populations, while providing aid.

Biometric identifiers, including fingerprints, iris scans, and facial geometry, have become increasingly popular as a means of enrolling individuals into systems and then authenticating users. Biometric data is vulnerable to hacking just like other authentication methods. However, unlike a password, **biometric indicators cannot simply be reset or changed as needed**. This poses a higher security risk, since it becomes increasingly difficult to repair the damage done by leaks or hacks of biometric data, and thus restore sanctity to biometric-based systems.

+ Key Questions and Recommendations

Considering all the issues stated above, the proliferation of digital identity programmes is deeply concerning. Human rights must form the centre of all considerations related to digital identity programmes.

We therefore request the champions and supporters of such digital identity programmes to:

1. **Respond to WhyID?** The basic WhyID question has several elements that must be asked at the onset of any digital identity programme in any given region or country:
   - **Why** do we need these foundational digital identity systems? What are their benefits?
   - **Why** are such programmes deployed without sufficient evidence of the benefits that they should deliver? How do these programmes plan to reduce the risk to and safeguard the rights and data of users?
   - **Why** should it be mandatory - either explicitly or de facto - for users to enroll onto these programmes? These programmes are either mandatory through legislative mandates or through making them a precondition to essential services for users.
   - **Why** are these programmes centralised and ubiquitous? Why is one digital identity linked to multiple facets of a citizen's life?
   - **Why** are countries leapfrogging to digital identity programmes, especially in regions where conventional identity programmes have not worked? The scalability of digital identity programmes also makes their harms scalable.
   - **Why** are these digital identity programmes not following the security guidance coming out of various expert academic and technical standard setting bodies on the use of biometrics in identity systems?[1]
   - **Why** are some private sector enterprises being privileged with access and ability to access the ID systems and build their private businesses on top of them? What safeguards are being implemented to prevent the misuse of information by the private sector? What should be the role of the private sector in the identity ecosystem?

   Those who promote these programmes must first critically evaluate and answer these basic WhyID questions, along with providing evidence of such rationale. In addition to answering these questions, these actors must actively engage and consult all actors. If there is no compelling rationale, evidence-based policy plan and measures to avoid and repair harms, there should be no digital identity programme rolled out.

2. **Evaluate and, if needed, halt:** The potential impact on human rights of all existing and potential digital identity programmes must be independently evaluated. They must be checked for necessary safeguards and detailed audit reports must be made public, for scrutiny. If the necessary safeguards are not in place, the digital identity programmes must be halted.

3. **Moratorium on the collection and use of biometrics (including facial recognition) for authentication purposes:** 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 programme. The harms from the breach of biometric information is irreparable for users and the ecosystem.

2. For example, guidance by organisations such as National Institute of Standards and Technology and IEEE Standards Association.

+ Conclusion

The undersigning organisations expect international, regional, and national leaders to address the **why** before they act. Those who promote digital identity programmes must thoroughly answer these questions, and follow human rights -centric approaches to identity. Each identity programme has an inherent requirement of trust from the user. Trust can only be built on the foundation of transparency and accountability. Trust can only be built when systems are designed to promote, empower, and protect the rights of citizens across the world. And that is exactly what the main objective of all policymakers should be.

Signed,

Access Now GLOBAL
AfroLeadership CAMEROON
Article 19 GLOBAL
Article 21 Trust INDIA
Association for Progressive Communications (APC) GLOBAL
Bits of Freedom THE NETHERLANDS
Civil Liberties Union for Europe EUROPE
Derechos Digitales LATIN AMERICA
Digital Rights Foundation PAKISTAN
Electronic Frontier Finland (Effi) FINLAND
Electronic Frontier Foundation (EFF) GLOBAL
Epicenter.works - for digital rights AUSTRIA
Fight for the Future USA
Foundation for Media Alternatives PHILIPPINES
Fundación Acceso CENTRAL AMERICA
Fundación Datos Protegidos LATIN AMERICA
Fundación Huaira Anden Region, LATIN AMERICA
Gambia Cyber Security Alliance GAMBIA
Human Rights Watch (HRW) GLOBAL
HumanFirst.Tech USA
Hiperderecho PERU
Internet Freedom Foundation INDIA
Internet Policy Observatory PAKISTAN
Internet Sans Frontieres GLOBAL
IPANDETEC - Centroamérica CENTRAL AMERICA
Karisma COLOMBIA
Majal.org MENA
Manushya Foundation ASIA
Metamorphosis Foundation EUROPE
Open Culture Foundation TAIWAN
Paradigm Initiative AFRICA
Privacy International UK
SFLC.in INDIA
Spectrum MENA
Taiwan Association for Human Rights TAIWAN
Techfugees GLOBAL
TEDIC NGO PARAGUAY
Thai Netizen Network THAILAND
The IO Foundation GLOBAL
The Tor Project GLOBAL
WITNESS GLOBAL
#SeguridadDigital MEXICO
@AmarantaONG CHILE

Individuals

Amadou Ceesay, Amba Kak, Berhan Taye, Charlie Martial Ngounou, Danny Rayman Labrin, Eduardo Carrillo, Gautam Bhatia, Javiera Moreno Andrade, Kaliya Young, Koh Henry, Malavika Jayaram, Naman M. Aggarwal, Prasanna S, Ria Singh Sawhney, Sarvjeet Singh, Shireen Mitchell, Siddharth Prakash Rao, Soudeh Rad, Usha Ramanathan, and Yesha Tshering Paul.

accessnow

This letter was facilitated by Access Now, an international non-profit organization that works to extend and defend the human rights of users at risk across the globe. To join the #WhyID list and learn more about our ongoing collective work on digital identity, **please contact identity@accessnow.org**