#WhyID

Access Now's comments to the World Bank consultation on the Principles on Identification for Sustainable Development

INTRODUCTION

The Principles on Identification for Sustainable Development (The Principles),[1] facilitated by the Identification for Development (ID4D) team at the World Bank, provide an important framework for the development of digital identity across the world. They are endorsed by many global and regional organisations that are active in funding, designing, developing, and deploying digital identity programmes across the world, especially in developing and less developed countries.

As an international finance institution, the World Bank created the Principles from a development perspective. Given that digital identity systems are being deployed in countries with varying levels of technological, economic, infrastructural, and governance-related development, it is important that stakeholders — and the frameworks that guide their decision-making — pay cognisance to the needs and realities of the regions, countries, and people which are behind on the development curve.

Digital identity systems pervade the lives of individuals, become gateways for important services, and in many instances become the foundation for a person's legitimacy or citizenship in a country or region. They have very real impacts on people's daily lives, particularly for those less privileged. **Digital identity systems impact human rights**.

The Principles must, at their very conceptualisation, seek to protect the human rights of the individual. At Access Now, we promote rights-respecting approaches to the design and implementation of digital identity systems. Our paper *National Digital Identity Programmes: What's next?*[2] provides 15 principles — covering data protection and privacy, governance, and cybersecurity — that serve as benchmarks for ensuring digital identity systems protect human rights.

[1] World Bank (2018). Principles on Identification for Sustainable Development: Toward the DIgital Age. http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

[2] Access Now (May 2018). National Digital Identity Programmes: What's next? https://www.accessnow.org/accessnow-digital-id-paper

Further, as a facilitator of the #WhyID Community, Access Now presented the #WhyID letter to international decision-makers last year.[3] This letter highlights the basic human rights concerns that arise from many national and humanitarian digital identity programmes, and raises questions that stakeholders must address to ensure that digital identity programmes protect human rights.

As an international organisation committed to defending and extending the digital rights of users at risk, we have examined ID4D's Principles from a human rights perspective. This comment is informed by the principles and questions raised in our policy paper and the #WhyID letter. We first provide thematic comments on the Principles and then provide specific comments for certain Principles.

THEMATIC COMMENTS

1. Do not conflate legal identity and digital identity

The Principles provide that they are intended to apply to "*the broad concept of 'legal identification' systems: those that register and identify individuals to provide government-recognized credentials (e.g. identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity.*" Further, they mention that the need for legal identity is in furtherance of the Sustainable Development Goals Target 16.9 to achieve "legal identity for all, including birth registration" by 2030.

We believe that some clarification in this regard is needed. As we mention in our policy paper on national digital identity programmes, a legal identity is usually understood as legal documentation certifying one's identity through basic data about one's personhood (such as your name and the date and place of your birth). On the other hand, digital identity adds a layer of authentication on top of the legal identity, often supported by a person's unchangeable and private biometrics (such as thumbprints or iris scans). The addition of this layer raises questions regarding the users' rights and the security of their personal information.

Requiring individuals to put their personal, unchangeable, biometric and sensitive data at great risk of privacy intrusions should be a measure of last resort for the purposes of "proving" legal identity. Legal identity can be verified in a variety of different ways, such as chip-based authentication or encryption-enabled key-based models. The risks to individuals are accentuated in communities where people have less reason to trust public authorities, including rural communities and those of marginalised people, such as refugees or other minority groups, or communities where structures and laws are not strong enough to safeguard the individuals' rights.

Key Takeaway: *Do not conflate the requirement for legal identity for all with the need for creating single central national digital identity programmes. While legal identity for all is essential, frameworks for authentication of legal identity through digital identity must protect the rights of users and promote mechanisms which provide users agency and choice.*

[3] Available at https://www.accessnow.org/whyid/

2. Do not restrain multiplicity of digital identity

As discussed above, for digital identity to be empowering in certain contexts, the technological, legal, and policy framework must be built on a foundation of user agency and choice, informed consent, the space for anonymity, and respect for privacy. A framework enabling multiple identities, which are tailored to a specific purpose and limited by data collection requirements, would enable innovative solutions which protect rights of users.

The Principles currently focus on one centralised, directly administered national identity system, which precludes the use of multiple forms of identity. These single-solution identity systems can prove coercive for users and act as a precondition for accessing services. Further, due to their ubiquity, these identity systems can enable surveillance and profiling schemes by governments and privileged private-sector actors. These digital identity systems often feed databases that connect multiple aspects of a person's life, heightening the risk of profiling. These risks are accentuated in countries with weak legislative and institutional frameworks for protecting human rights.

Mandatory enrollment requirements around a single digital identity programme further exacerbate the risk of exclusion, profiling, and surveillance. This is the case whether the enrollment requirements are explicit (e.g. when a government makes possession of a particular form of national digital ID mandatory by a specific law or edict) or coerced (e.g. when the national digital ID is required to access services from other public agencies, or when governments pressure private companies and platforms to adopt mandatory use of such IDs).

***Key Takeaway**: The Principles must not advocate for single digital identity solutions covering all users for multiple purposes. The Principles must promote the development of multiple voluntary identity frameworks in a country, which are limited by purpose.*

3. Promote prioritization of data security and preparation for system failures

The Principles do not provide guidance to ensure implementation of robust systems for avoiding catastrophic incidents, such as mass biometric data breaches or exposure of other personal information.

No system is fool-proof. When it comes to critical systems, such as national identity systems, it is imperative that measures be taken to add redundancies and contingency plans that ensure the system is defensible and in no situation would be susceptible to complete breakdown. It is important to recognize the reality of these vulnerabilities, especially in the case of biometric systems. Given that digital identity programmes are often implemented in developing countries, with underdeveloped technology and policy infrastructure, it is essential to both acknowledge the risks and require their mitigation. Instead, current suggestions within the principles such as those promoting single identity frameworks heighten those risks by creating single points of failure.

As the world fights bravely against COVID-19, with the reality of non-robust healthcare systems, the need for creating systems which are resilient to tail risks cannot be overstated. The rapid deployment and use of certain forms of data collection, databasing, and digital identity can have long-term impacts on human rights, notably the right to privacy, freedom of expression, and access to information and systems, along with a range of economic rights.

***Key Takeaway**: The Principles must account for vulnerabilities and their long-term effects, and guidance by the Principles should enable robust systems through the creation of redundancies and contingency plans.*

4. Require human rights impact assessments

While principles and guidance for digital identity programmes are essential and provide direction to various constituents in the development of digital identity systems, each system's specific context and distinct features present unique challenges to human rights that must be resolved. To ensure systems' agility and adaptability, it is essential that each system is evaluated through a human rights lens during all stages of development and deployment.

***Key Takeaway:** Human rights impact assessment, ex ante and ex post, must be added in the Principles as a definite requirement for each digital identity programme.*

5. Require inclusive and open consultations

Given the profound impact each digital identity programme has on individuals' lives, it is imperative that a principle be added requiring open, transparent processes and consultations with civil society, citizens, technologists, and all other stakeholders before and at every stage of development of a digital identity programme. Special care must be taken to include vulnerable and marginalised populations in these consultations and throughout the development and implementation process. These populations are the most affected by digital identity programmes, but all too often the least heard.

***Key Takeaway:** The Principles must require widely inclusive, transparent, and substantial consultation — especially with marginalised, at-risk, and otherwise highly impacted communities — throughout all stages of a digital identity programme's conceptualisation, development, and implementation.*

COMMENTS ON SPECIFIC PRINCIPLES

Principle 1: Ensuring universal coverage for individuals from birth to death, free from discrimination

This Principle states that each resident of a country must be provided universal and non-discriminatory legal identity from birth. In line with the Sustainable Development Goals, we agree that each individual must be provided a legal identity. However, as stated in previous sections, individuals must be given a choice in digital identity architectures through multiplicity and purpose limitation. It is not essential that one single identity be used for all purposes between a person's life and death.

One digital identity controlled by the state, with the lack of effective governance and policy structures, would render the individual unduly under the control of the state, as well as privileged private organisations. Reliance on one single source of identity also increases the chance of mass breaches, exclusion, and discrimination within an identity system, as any error within the system would scale to a whole population. As previously mentioned, the mandatory nature of a single digital identity programme creates hurdles for access to services and amplifies the harms of exclusion, profiling, and surveillance.

***Key Takeaway**: This Principle should be amended to clarify that universality and non-discrimination are supported through enabling voluntary multiple digital identities for specific purposes. Each potential use case for a digital identity must be evaluated to understand the impact on human rights and the need for deploying digital identities for such a use case.*

Principle 3: Establishing a robust — unique, secure, and accurate — identity

In relation to the suggestion to establish a robust — unique, secure, and accurate — identity, we reiterate our concerns regarding the need for a single identity for all purposes. We agree that identity must be secure and accurate. Further, we believe that the creation of a single identity goes against the principle of robustness. A robust identity framework would be resilient to downside risks. A single digital identity framework for a nation's whole population, for all purposes, accentuates the single point of failure risk which would have massive consequences for that population. The creation of multiple authentication mechanisms along with multiple identities for different purposes provides the necessary redundancies to create a resilient identity framework.

The collection of large amounts of personal information pertaining to identities — including biometrics — often form tempting targets for criminals and other actors for malicious hacking and cyber intrusion. Highly critical personal information is carried through programme networks. Thus, properly protecting system communications, such as requests and responses for authentication, is essential for ensuring security. End-to-end encrypted communications throughout any digital identity system is of crucial importance to ensuring digital security and must be established to the greatest extent possible.

***Key Takeaway**: A single identity framework takes away from the robustness of digital identity programmes. Secure encryption standards must be applied to all information stored, processed, and transferred in an identity environment.*

Principle 4: Creating a platform that is interoperable and responsive to the needs of various users

We believe interoperability as a term is focussed on the individual. An “interoperable” identity is one where a user would be able — both as a right, and in practice — to migrate from one identity or use case to another. However, this Principle uses the term in the context of the power of the state and its departments to use identity databases for their purposes. This Principle would ensure indiscriminate data-sharing possibilities between departments of the state without regard for the individual’s rights. The term “interoperable” should not be used for this purpose.

While we believe in truly user-centred interoperable identity programmes, we also believe that the scope of identity programmes must be narrow. The purpose of each identity programme should be limited, and the amount of data collected should be minimised. Without such safeguards, and under systems where different arms of the state are able to use identity data, an identity system has the potential of “function creep.” In this situation, a programme ends up taking on functions for which it was not originally intended. This could both compromise the rights of users and create functional issues.

Further, massive data sharing within the government under a single identity system creates many opportunities for surveillance and profiling. These risks are accentuated in the case of refugees and other marginalised populations, where data sharing can lead to adverse outcomes and harms at scale.

Key Takeaway: *The term interoperable should not be used for this Principle. This principle should be amended to disallow unregulated and unrestricted data sharing between departments of government and between governments. The Principle must also stress that digital identity programmes should be limited in scope and minimise collection of data, and additional functions should not be added.*

Principle 5: Using open standards and ensuring vendor and technology neutrality

We support the use of open standards, as they enable transparency and accountability in the functioning of identity systems. However, we must promote responsible technologies, and thus it is essential that these open standards only include rights-respecting technology solutions. Open standards, by themselves, cannot help protect rights or ensure that a digital identity system is well-designed. Creating modules, which may not protect user rights, can enable the creation of bad digital identity programmes. We suggest that language be added within the Principle to clarify this. Open standards and technology neutrality must ensure that the resulting standards and technology support, promote, and protect the rights of individuals.

Further, governments, vendors, and standard setters must also take responsibility for the impact and accuracy of their systems. As further discussed below, rights and remedies must be provided to individuals to maintain accountability of governments, vendors, and standard setters. Under the UN Guiding Principles on Business and Human Rights, companies have a duty to "know and show" their respect for human rights through due diligence, developing policies to prevent adverse impacts, and remedial measures to account for harm they've caused or contributed to. Transparency is a prerequisite for such accountability. Vendors, suppliers, and standard-setting organisations must bear the responsibility for the potential impacts of their technology and policies, and work with stakeholders to prevent and mitigate any salient risks.

***Key Takeaway**: Open standards are welcome. They should be accompanied by requirements for accountability of the vendors and standard setters. The technology and standards should protect user rights and must not enable systems which violate the rights of users.*

Principle 6: Protecting user privacy and control through system design

We agree that user privacy and data protection are essential for any identity framework to be effective and non-predatory. We further believe that comprehensive data protection, while being a necessary condition, is not a sufficient condition in itself to protect all of a user's rights. We suggest that this clarification be added within the Principle, as in many cases, those interested in establishing a digital identity system have pointed to passage of a data protection regulation as being enough to broadly dismiss concerns about the system's impact on human rights.

It is essential that data protection frameworks provide a well-functioning law and regulator. The law should be accountable to citizens, and institutions responsible for the law's enforcement should be independent and capable of overseeing and regulating it. Additionally, given its critical importance, regulations should go further in the context of national digital identity systems to meet at least the minimum requirements of a globally compliant data protection law and provide identity-specific rights.

Further,in many countries the state is the largest collector of data and in charge of the digital identity programme, making surveillance reforms just as essential as data protection laws in ensuring users' rights. Access to data and information must be governed by rule of law, backed by narrow and specific legislation, and guided by the principles of necessity and proportionality. Given the role of the state in maintaining the data in a digital identity system, safeguards must be put in place to ensure that intra-government access to data does not happen without specific mandate. The role of judicial and quasi-judicial offices in obtaining such mandates should be explored and instituted.

***Key Takeaway**: Comprehensive data protection laws are necessary, but are not alone sufficient to protect individuals' rights in the context of digital identity systems. Additional safeguards must be put in place to provide all appropriate rights and remedies. States must also put robust and comprehensive surveillance reforms in place before instituting digital identity systems.*

Principle 7: Planning for financial and operational sustainability without compromising accessibility

Adding service fees to the provision of digital identity programmes can lead to predatory outcomes for users. It must be noted that many digital identity programmes are used as a means of delivering essential services. Adding service fees in this context would effectively mean charging citizens for free services they are entitled to. Further, mixing financial incentives with service delivery can cause problems, and digital identity programmes established or administered by governments should not be set up as profit-making entities but rather as public goods.

***Key Takeaway**: Service fees should not be added to public sector digital identity programmes.*

CONCLUSION

It is of utmost importance that the Principles truly respect the rights of individuals impacted by digital identity programmes, as the Principles guide the decision-making of signatory organisations. In many instances, civil society organisations have observed that signatories to the Principles have been involved in digital identity projects that do not respect human rights — or the Principles themselves.

We strongly recommend that the signatories affirm and commit to these Principles. **Each signatory of the Principles must affirm that they will be involved only with programmes that are aligned with each tenant of these Principles, and commit to restrict funding and support to programmes that do not abide by the Principles.** For the Principles to be effective, it is essential that such commitment be made, and for them to truly guide the behavior of the supporting organisations.

Finally, each organisation must be open to feedback on their projects to ensure they are in consonance with the Principles, and if any project is found wanting in this regard, the organisations must commit to rescinding their participation. **To ensure a constructive feedback loop, we suggest that each organisation institute formalised civil society participation mechanisms to (a) evaluate and analyse human rights impact of digital identity systems, (b) advise the signatory organisation on its policies on digital identity, and (c) act as a platform for civil society feedback and reporting on on-ground impact of digital identity systems.**

Thank you for the opportunity to participate in these consultations. We hope to be able to facilitate wider consultations, and also discuss our recommendations in detail. We remain available for any clarification or queries in relation to this feedback.

For more information, please contact **identity@accessnow.org** *or visit* **accessnow.org/whyid**