March 2020

privacyinternational.org

Consultation response for ID4D on the Principles on Identification for Sustainable Development: Toward the Digital Age



Consultation response for ID4D on the Principles on Identification for Sustainable Development: Toward the Digital Age

Privacy International

31st March 2020

Introduction

Privacy International welcomes the opportunity to contribute to the consultation on the Principles on Identification for Sustainable Development[1]. Valuable lessons have been learnt, particularly in the last few years, on the serious consequences of identity systems. We have seen challenges in court that have found that key provisions of these systems are incompatible with the right to privacy enshrined in constitutions. We have seen civil society organisations highlighting the serious risks of exclusion and discrimination that emerge. Valuable lessons have become clear, and PI is available to provide the information the World Bank needs to ensure these are reflected in the Principles. At the same time, developments in this space also raise questions as the relationship of the World Bank to the Principles, and how they can be used to create a future where these systems are compatible and promote human rights.

We begin with general comment on the Principles and their implementation, followed by highlighting some of the issues not addressed in the principles, before a more in-depth look at some of the concerns with individual principles.

About Privacy International

[1] https://id4d.worldbank.org/principles

Privacy International is a London-based NGO, with a network of partners around the world. PI campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

The World Bank as "owner" of the Principles

While the Principles are endorsed by 25 other organisations (including the UK's Privacy and Consumer Advisory Group (PCAG), on which Privacy International sits), the World Bank's ID4D initiative remains very much the owner and driver of the Principles. This creates a challenge, in that it remains opaque as to how the ID4D applies the principles in practice.

Other contexts are telling here. In the UK, the Privacy and Consumer Advisory Group (PCAG), the committee that provides independent advice to government on issues including identity, devised a set of Identity Assurance Principles[2]. Thus the designers of the UK's identity authentication service Verify were able to produce a mapping of what these principles meant for the different actors (the user, the government and the private sector actors) in terms of the rights and responsibilities. Crucially, Government Digital Services was also able to publish publicly the analysis of how their system applied the principles[3]. This enables anybody to see how the principles were applied, essential for establishing whether a particular system meets these principles.

We are not aware of any analysis by ID4D or the World Bank more generally that gives transparency about how these principles are applied in practice.

MAIN RECOMMENDATION 1: The World Bank must publish and make accessible to the public an analysis of how a project meets or fails to meet the Principles, when it funds a digital identity project through grants or loans, and what mitigation strategies are presented as pre-conditions as part of the assessment process; offers an analysis of a digital identity system through the ID4D's Country Analyses, or other outputs relating to digital identity.

The Principles, endorsed as they are by 25 organisations at the moment, also form a basis for much discussion on identity systems beyond the work of the Word Bank and the supporters of the Principles. However, the World Bank has not openly presented the implications of the Principles. ID4D is an organisation with multiple hats: they are a funder; an analyst; a proponent; and -through the Principles – are also placed into being in the

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

[3] https://identityassurance.blog.gov.uk/2016/11/30/applying-the-identity-assurance-principles-to-gov-uk-verify-part-1/

position of a moral leader. Given the issues raised above, it appears that they are struggling to show the moral leadership (at least publicly) that is necessary for the 'owner' of a set of principles. Thus, the question has to be asked as to whether the World Bank remains the appropriate host for the Principles. The number of organisations working in this field has increased and diversified greatly over the last few years, and it may have been necessary in the past for the World Bank to take this leadership. Now, however, there are opportunities to bring some of these discussions to open, inclusive multi-stakeholder forums/spaces in particular those led by civil society which are more closely involved in these issues, and whose mandates is to protect and promote the rights of the very people being impacted by digital identity systems.

MAIN RECOMMENDATION 2: The World Bank should commit to following the Principles across the organisation, but ownership and their curation should be spun-off to other more public, open and inclusive spaces that enable broader ongoing civil society engagement. and stronger human rights oversight.

Additional Principles

Alongside the issues with specific principles highlighted below, there are three additional issues that should be included.

First, for any identity system, the purpose of the system must be clearly stated. Given the risks that exist with introducing such a system, one must not be introduced without a clear purpose behind it. Claims for a system, for example in fraud reduction, must be backed by clear, publicly available and independent evidence. This provides, for example, the lawful basis of the processing of the data for such a system. The design and nature of the system must then reflect that purpose, as well as be necessary and proportionate. Additional uses of a system, decided upon later, must also meet this test of proportionality and necessity before it can serve that new, additional purpose. Note that 'to provide an identification system' is not in itself sufficient justification; this is a tautology.

MAIN RECOMMENDATION 3: The Principles should state that every identity system must have a clearly stated purpose, with its proportionality and necessity backed by clear and publicly-available evidence. It should be explicitly noted that the purpose of creating an identification system is not itself sufficient.

Second, there should be an emphasis on the importance of a transparent and democratic process in the development of these systems. Such a system must be the product of a full and meaningful engagement with civil society and affected peoples, on both the broader topics of the desirability of the system but also on the technical nature of a specific deployment. A system must be backed by law, prior to the collection of data or its

deployment, and should have gone through democratic process, not relying on decrees or the declaration by ministers. There are few or at least limited instances where democratic process interrogate the proposals being put forward for the design and deployment of identification system. Individuals and communities are not given the opportunity to be consulted. The absence of such an inclusive, transparent legislative process means that there is no space to review, assess and amend proposals before implementation.

Through our work with the Privacy International Network we have seen identity systems pushed through by decree, diktat, or through means that allow less democratic accountability, denying the systems a democratic mandate and often a legal basis under the rule of law. They are often introduced without the firm and rigorous debate that such a major measure deserves. Few of the current existing national identification systems were established by law. For something as intrinsically personal as identity, and with identity systems so open to potential abuse, the lack of democratic debate and accountability is concerning.

For example, consider the case of the Federal Biometric Identification System for Security (SIBIOS) in Argentina, introduced in 2011 by decree 1766. By introducing it in this manner, essential debate on the issues was bypassed. With the decree only vaguely highlighting the goals and need for such a system—the "essential protection of the right to security"—it becomes impossible to both understand the need for such a system, as well as evaluate its effectiveness. As our partners from the Asociación por los Derechos Civiles (ADC) argue, "the decree seems to be based on the logic of identifying individuals effectively and easily through biometric technology, not because it is the best solution for the concrete security need, but because it is available. When the legislative debate is bypassed, one loses perspective about the safeguards that must be in place to guarantee the exercise of human rights."

In Indonesia, the e-KTP, a biometric mandatory identity card, which was launched nationwide in 2011 was never established by law, and so every year the President must issue a different presidential regulation to provide the legal framework to enable the project to proceed. And in India, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "Aadhaar Act") was passed by the Lok Sabha to establish a legislative framework for the Aadhaar scheme 5 years after it started being implemented in 2010 and by 2016 there were already 1 billion enrolees.

This opacity expands into the design and implementation phase as there is a lack of transparency of the role of the private sector, limited publicly available information on procurement processes, and so no public access to tenders or contracts of public and private partnerships. In some instances, the secrecy is institutionalised with public and

private partnership contract providing for gagging clauses whereby neither party would be able to speak about the terms of the contract. This is what is suspected happened in Kenya when the Electoral Commission failed to respond positively to the Kenyan Supreme Court's orders to grant access to its computer servers following the claims from the opposition that it systems had been compromised, and the Court decided to annul the results.

MAIN RECOMMENDATION 4: The Principles should emphasise the importance of a transparent and democratic process in the development of these systems. Such a system must be the product of a full and meaningful engagement with civil society and affected peoples, on both the broader topics of the desirability of the system but also on the technical nature of a specific deployment. A system must be backed by law, prior to the collection of data or its deployment, and should have gone through democratic process.

Thirdly, while not a necessary part of many identity systems, the use of biometrics in these types of systems is increasingly widespread. It must be highlighted that the use of biometrics creates severe risks[4]. The Principles should reflect these risks, and explicitly states that the use of biometrics should be limited as much as possible. If biometrics is to be deployed, a system should be designed in such a way that looks to mitigate many of the risks (for example, by storing biometrics on devices rather than in a centralised database).

MAIN RECOMMENDATION 4: The Principles should highlight how the use of biometrics creates severe risks and recommend that – if biometrics are to be deployed – mitigation measures must be deployed.

Issues from the Preamble

If we are to have a document that takes a balanced approach to recognising the risks rather than just the benefits of identity systems, it must also recognise that identity systems are not only a potential enabler but also an impediment to attaining the Sustainable Development Goals. The reference to the SDGs (Footnote 1) should thus highlight how identity systems can hinder the achievement of the goals. This can include how identity systems can lead to exclusion from government social security systems, which hampers achieving a number of targets in Goal 1 on ending poverty, and Goal 2 on ending hunger[5]. Goal 4 on education cannot be achieved while education is dependent on a child or their

[4] For more details, see: https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make
[5] https://www.huffingtonpost.in/2018/09/25/aadhaar-linked-to-half-the-reported-starvation-deaths-since-2015-say-researchers_a_23539768/

parents requiring particular identity documents. The target in Goal 9.c, on the access to information and communications technology and universal access to the Internet, is hampered by the exclusionary need for SIM card registration[6]. The effect of identity requirements extends to it serving to exclude people from having decent housing (Goal 11) and rights in the workplace (Goal 8)[7].

MAIN RECOMMENDATION 5: In order to present a balanced picture, the Principles should also reflect the ways in which identity systems are a threat to development, including the Sustainable Development Goals.

Principle 1

It should be explicitly noted that the reference to 'universal coverage for individuals from birth to death' is referring to civil registration, rather than any other form of identification system. We have, unfortunately, seen the justification for schemes like biometric identity cards be based on arguments from developmental organisations on purely birth registration. The language in this section also needs updating in the light of the work of the UN Legal Identity Task Force and the UN's Legal Identity Agenda: "birth registration" is not *part* of "identity management", these are separate processes.

On the issue of non-discrimination, it is important to recognise that, while measures to ensure that any particular scheme has the barriers to enrolment and use removed, it is the case that universality will remain an aspiration rather than a reality. As such, to ensure that systems are truly non-discriminatory, then we have to also remove as far as possible the requirements for people to use a particular system or identification at all. As such it should be stated that the strongest tool against discrimination is to remove the requirements for identification at all, and where it is required to broaden the needed identification beyond one particular system.

MAIN RECOMMENDATION 6: The Principles should recommend the removal of identity requirements to reduce discrimination, or where this is not possible to broaden the needed identification beyond any one particular system.

On universality, it is essential to clarify the meaning of 'all residents'. In providing identification (whether as part of a civil registration system, or an identity system), this must explicitly include irregular migrants. Immigration status should not form a barrier. For example, in India, the Supreme Court ruled that the definition of residents did not include "illegal migrants", which leads to serious issues surrounding members of those groups or those who might be deemed to be members. As part of the measures to prevent these

[6] https://privacyinternational.org/explainer/2654/101-sim-card-registration
[7] https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

discriminations, the Principles must be explicit in stating that the scope of 'all residents' includes irregular migrants and others who are resident but without formal recognition and people with different immigration statuses.

MAIN RECOMMENDATION 7: The Principles should make it clear that any definition of 'resident' should include irregular migrants and other undocumented people, otherwise discrimination against such populations are amplified by identity systems.

Principle 3

Principle 3 should be changed to remove the concept of a "unique" identity. The consequences of unique identities are grave: it is a key facilitator of systems used to exclude, exploit and surveil. The glorious fluidity and complexity of human identity means that, even at their best, any identity system is an incomplete reflection of that human experience; thus, leading to discrimination and exclusion for those who do not fit into a box of the single individual[8] . Unique identities remove the agency of the individual to control how government and private-sector services can link together multiple sources of data. It is a source of control over the individual: states can have an effective 'kill-switch' over the civic life of an individual. Similarly, other actors who get control over an individual's identity credential have extreme levels of control over that individual. Finally, we have seen that the way that this uniqueness has been implemented through biometric deduplication, which necessitates the creation of a biometric database with the associated risks of misuse and breaches. Allowing an individual to have a multiplicity and fluidity of identities mitigates against these severe risks to human rights. As a result, this should be included in the Principles.

MAIN RECOMMENDATION 8: The word 'unique' should be removed from the Principles, to be replaced by an understanding that unique identities create particular risks to the rights of individuals and communities. An emphasis should rather be placed on systems that allow a multiplicity of identities as a mitigation of these risks.

Principle 4

Principle 4 states: "They should also meet the needs of public agencies and private companies that use—or could use—this identity as a foundation for other services or operations." This is a statement that invites function creep - the inflation of the cases in which identification is required. In doing so, it clashes with the concept of purpose limitation. Similarly, unless 'need' is understood very narrowly, it becomes an invitation for the services and organisations involved to engage in data exploitation and making use of

[8] https://privacyinternational.org/long-read/2274/identity-discrimination-and-challenge-id

identity data for other purposes. This statement should thus be rewritten to replace the word "needs" with "legal requirements".

Principle 5

The Language around "improved functionality" should make it clear that the functionality has to be determined by the nature and needs of the system as per the original stated scope and purpose.

Principle 6

The principles should be explicit that, following from this principle, the design of a system should not include reusable unique identifiers (for example, an ID number). This is a tool for linking together disparate databases in the public and private spheres, creating a "360-degree view of the individual" that can be difficult or impossible to escape. Thus the design of a system must avoid the creation of these unique identifiers, backed by regulation to prevent the development of defacto identifiers.

MAIN RECOMMENDATION 9: The Principles should recommend that unique identifiers (whether defacto or dejure) should not be deployed.

While it is correct that the data collected, be "fit for purpose and proportional to the use case", it should be reiterated that the creation of an identity system is not itself a purpose.

The reference to "sensitive personal information" is confusing, as its use in the text and footnote do not seem to match its use under data protection law. It is, of course, important that information like ethnicity or religion not be included on ID cards or can be determined from identity numbers. But consideration should also be given to data requiring additional protection because of its 'sensitivity' within a particular context, i.e. financial information, caste.

Yet it is also the case that identity systems are themselves a tool for inferring this type of sensitive data from other data sources, as linking together many different sources of data is a key consequence of the design of many systems (in particular, those requiring a unique identity or a unique identifier).

Identity schemes are highly complex socio-technical systems, and the design requirements may change over time to embrace new opportunity, address challenges and to rectify shortcomings, and yet there is a complete lack of processes and protocols to undertake critical assessments.

There are few institutionalised instances of audits within identification programmes: is the programme solving the problem which had been identified, and which justified its creation? e.g Are fewer people excluded from accessing banking services? Are fewer stolen mobile phones sold thanks to cell phone registries? Is there less fraud in the aid sector because access is regulated through a biometric identification system? This core component of any project management system is missing. Instead, identification systems that have been called out for being controversial, inadequate, inefficient are being replicated in other countries, and so in other contexts with different factors and powers at play, without much reflection. As examples: India's Aadhaar is being exported to the Middle East; Pakistan's expertise on biometric ID is being sought in Eastern Africa; and SIM card registration systems are being deployed in countries across the world.

With mission creep rampant and hard to regulate when it comes to identification schemes, there is a need to adopt a thorough decision-making process whereby first it is decided whether the new/additional purpose(s) is compatible with the original purpose, and if it is, there is a need to assess whether the way the scheme is designed it fit for that purpose to ensure that the security, safety and integrity of the data and the infrastructure are ensured. As the instigator/owner/manager of the identification system designs the system with their own interests in mind, it is likely it will be incompatible for uses by other parties.

Principle 7

It is correct to highlight the need for sustainability and long-term thinking, and we urge that an emphasis must be placed on the importance of security. The data in identity systems, particularly but not limited to any biometric data, can be relevant for the lifetime of an individual, and even after death.

It should be noted that private sector use can be problematic or even unlawful. For example, the Indian supreme court found that "Allowing private entities to use Aadhaar numbers will lead to commercial exploitation of an individual's personal data without his/her consent and could lead to individual profiling", and thus its use was unconstitutional[9]. This should be reflected in the Principles.

The funding model also needs to be transparent. For example, making a claim that a system is to be paid for through reducing leakages in social security systems requires evidence to back up this claim (i.e, an independent analysis of the leakages in the system, and whether these are then capable of being fixed through the introduction of a particular identity scheme). This also requires the cost of a system be made transparent.

[9] https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar

Understanding the 'business model' for an ID system is essential; furthermore, that system must not be based upon the exploitation of an individual's data or the metadata surrounding the identity system[10].

MAIN RECOMMENDATION 10: The Principles should emphasise the need for transparency in the economic model of an identity system, and to ensure that this does not lead the exploitation of people's data or metadata.

Principle 8

Data protection is necessary to safeguard the fundamental right to privacy as it will serve to regulate and oversee the processing of personal data: providing individuals with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

Data protection legislation must be in place prior to rolling an identity system, and the law must also be accompanied by effective implementation and enforcement in order to adequately operationalise it.

Core data protection principles found in multiple frameworks provide important safeguards to the introduction of an identification system. For example, the principle of purpose limitation in data protection requires that personal data is collected for a specific, explicit and legitimate purpose – this means that it must be clear what data will be used for and collected for one purpose must not be used for another. The principle of data minimisation, for example, requires that data is limited to what is necessary to achieve that stated purpose. Further principles include transparency, fairness, accuracy, and that the data is held no longer than necessary. These principles have been analysed by the EDPS in the context of identity cards in the European Union.

Furthermore, data protection law provides for the right of individuals to be informed about how their data is used, to access their data, to correct their data, amongst others. Data protection law also imposes specific requirements in terms of the security of the data, record-keeping, to build in data protection by design and default and to assess and mitigate the impact on individuals' rights.

But it is not just about ensuring that a robust, effective data protection legislation be in place, but it is also about ensuring that any laws that are adopted to establish identification systems must provide for the respect and protection of the highest data protection and safeguards either by referring to existing relevant safeguards such as those

[10] https://privacyinternational.org/advocacy/3215/response-uks-call-evidence-digital-identity

enshrined in Constitutions and/or provided for in data protection legislation, and where these don't exist provisions must integrated within the laws that establish the schemes.

MAIN RECOMMENDATION 11: The Principles should emphasise that data protection legislation must be in place prior to rolling an identity system, and the law must also be accompanied by effective implementation and enforcement in order to adequately operationalise it. These must meet the highest standards.

Principle 10

Accountability and enforcement are key to the success of the protection of personal data, and so accountability should be at the core of any law regulating of the processing of personal data and the protection of the rights of individuals, and data protection rules thus need to be enforced by a regulator or authority. While international data protection regulations remain largely non-prescriptive on enforcement, in order to give effect to the fundamental right of data protection and its principles, legislation must provide for the establishment of an independent supervisory authority. A supervisory authority requires this statutory footing in order to establish clearly its mandate, powers and independence.

In many countries with data protection laws, we are seeing that that many data protection authorities are not granted the necessary institutional and financial independence to execute its mandate effectively. This hinders trust in the implementation of the law, and fosters a lack of trust from the public.

The strength of powers invested in these authorities varies from country to country, as does their independence from government. Some jurisdictions have established more than one regulatory body for oversight regulation and enforcement, with powers depending on if the data is being processed by public or private entities, e.g. Colombia. These powers, for example, can include the ability to conduct investigations, act on complaints, and impose fines when an organisation has broken the law.

Redress for breaches of data protection law should also be available through the courts, both through individual actions and collective redress (brought by NGOs and consumer groups).

MAIN RECOMMENDATION 12: Regulators of identity systems, and the associated data protection issues, must be granted the necessary institutional and financial independence to execute their mandates effectively. There must be opportunities for collective as well as individual redress.

Conclusion

The opportunities provided by a review of the Principles must not be squandered. It provides an opportunity to reflect on lessons learned about where digital identity systems have failed to protect people and/or directly undermined people's rights to develop Principles that will lead to a better future for us all, whether we are enrolled in any particular identity system or not.

We urge the World Bank not to end the consultation process with this current process of revisions. This is just a starting point. We recommend that they adopt creative, innovative and sustainable ways to continuously consult with others in open, inclusive processes. Doing so will reaffirm their commitment not only to this revision process but also the purpose and vision of the Principles.

Summary of Main Recommendations

MAIN RECOMMENDATION 1: The World Bank must publish and make accessible to the public an analysis of how a project meets or fails to meet the Principles, when it funds a digital identity project through grants or loans, and what mitigation strategies are presented as pre-conditions as part of the assessment process; offers an analysis of a digital identity system through the ID4D's Country Analyses, or other outputs relating to digital identity.

MAIN RECOMMENDATION 2: The World Bank should commit to following the Principles across the organisation, but ownership and their curation should be spun-off to other more public, open and inclusive spaces that enable broader ongoing civil society engagement. and stronger human rights oversight.

MAIN RECOMMENDATION 3: The Principles should state that every identity system must have a clearly stated purpose, with its proportionality and necessity backed by clear and publicly-available evidence. It should be explicitly noted that the purpose of creating an identification system is not itself sufficient.

MAIN RECOMMENDATION 4: The Principles should highlight how the use of biometrics creates severe risks, and recommend that – if biometrics are to be deployed – mitigation measures must be deployed.

MAIN RECOMMENDATION 5: In order to present a balanced picture, the Principles should also reflect the ways in which identity systems are a threat to development, including the Sustainable Development Goals.

MAIN RECOMMENDATION 6: The Principles should recommend the removal of identity requirements to reduce discrimination, or where this is not possible to broaden the needed identification beyond any one particular system.

MAIN RECOMMENDATION 7: The Principles should make it clear that any definition of 'resident' should include irregular migrants and other undocumented people, otherwise discrimination against such populations are amplified by identity systems.

MAIN RECOMMENDATION 8: The word 'unique' should be removed from the Principles, to be replaced by an understanding that unique identities create particular risks to the rights of individuals and communities. An emphasis should rather be placed on systems that allow a multiplicity of identities as a mitigation of these risks.

MAIN RECOMMENDATION 9: The Principles should recommend that unique identifiers (whether defacto or dejure) should not be deployed.

MAIN RECOMMENDATION 10: The Principles should emphasise the need for transparency in the economic model of an identity system, and to ensure that this does not lead the exploitation of people's data or metadata.

MAIN RECOMMENDATION 11: The Principles should emphasise that data protection legislation must be in place prior to rolling an identity system, and the law must also be accompanied by effective implementation and enforcement in order to adequately operationalise it. These must meet the highest standards.

MAIN RECOMMENDATION 12: Regulators of identity systems, and the associated data protection issues, must be granted the necessary institutional and financial independence to execute their mandates effectively. There must be opportunities for collective as well as individual redress.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).