ID4AFRICA2019
18-20 June | Johannesburg | South Africa

Reflections on the ID4Africa Panel on

Appropriate Use of [Issued] Identity

ID4Afica 2019, Day 3, Plenary Session (PS6)

By Thea Anderson, Director, Omidyar Network

Panelists

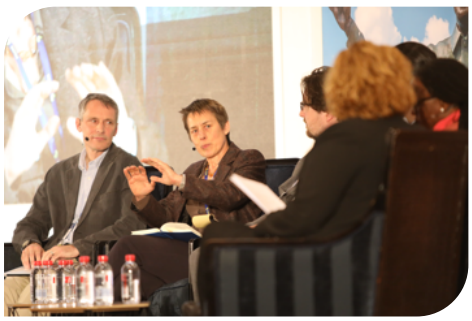
1. Teki Akuetteh Falconer, Founder & Executive Director, Africa Digital Rights' Hub, Ghana
2. Dr. Tom Fisher, Research Officer, Privacy International, UK
3. Dr. Bronwen Manby, Senior Policy Fellow, London School of Economics and Political Science, UK
4. Dr. Isaac Rutenberg, Senior Lecturer and Director, Center for Intellectual Property and Information Technology Law (CIPIT), Kenya
5. Dr. Jonathan Klaaren, Professor, University of Vit, South Africa

Moderator: Thea Anderson, Director, Omidyar Network

In the past decade, over 100 countries have initiated new identification programs often with an initial use case, such as voting or social safety nets payments. Over time, the government may expand how the ID is used, for example to pay taxes, open a bank account, or school enrollment. The expansion of use cases creates the risk of mission creep or 'function creep'. Data originally collected for one purpose, applied to a different use without consent and the ID made to be mandatory for more and more uses. This situation is increasingly common as discussed and debated by five thought leaders in the fields of identity, privacy, ethics, statelessness, and data protection on the 'Appropriate Use of Identity' panel held at ID4Africa Summit. Panel moderator, Thea Anderson, noted to accelerate the conversation Omidyar Network has launched a three-region research alliance dedicated to the questions of appropriate use of identity in Kenya, Brazil, and India to influence policymaking.

To start the discussion, each panelist shared their perspective on the question of appropriate use case and applications for issued ID. First, Teki Akuetteh Falconer, Founder & Executive Director of the Africa Digital Rights' Hub in Ghana, stressed the need for 'person-centric' ID schemes and the need to minimize mandatory ID to mitigate the potential of infringement of individuals right to privacy.

Dr. Tom Fisher, Research Officer at Privacy International, noted that ID isn't an inherent good and that "ID cards can facilitate some of the worst human rights abuses we can see." He added that unique biometric systems can make this situation even worse from a privacy perspective as "visibility" isn't always a universal positive if personal data can be used for tracking, surveillance, or profiling. He stressed the importance of taking an ecosystem approach to identity so that those without an ID are still able to access some services. He also emphasized the importance of questioning whether a use case is necessary and proportionate.



Dr. Bronwen Manby, Senior Policy Fellow at the London School of Economics, emphasized the introduction of a new ID system can be dangerous for excluded groups and that ID systems should be designed to identify and address 'atypical' cases. Governments must allow alternative forms of evidence and documentation to better reflect a country's reality and reduce the amount of statelessness. Manby stated that if ID is a human right then "if this ID requires a credential then that's

also a human right." She also questioned whether a single source of truth is a good idea and if the presentation of a national foundational ID in fact needed for many purposes.

Dr. Isaac Rutenberg, Senior Lecturer and Director at the Center for Intellectual Property and Information Technology Law in Kenya stressed for any ID, there are several fundamental rights at play - the right to an identity and the right to privacy, but the right to a secure ID is inherent in the right to an identity. He questioned the boundaries and implications of these rights. He emphasized that the data governments demand from citizens "voluntarily" gives them a valuable asset. However, rather than an exchange - using a human rights lens- , the exchange is a one-way transfer from individuals to the government.

Rutenberg warned that companies have learned how to turn the data we generate all day every day into money: "mission creep for me would be governments will be asking for more and more data from biometrics to bioinformation to activities, healthcare etc. All that information is extremely valuable and desired by the private sector". He urged countries to take data seriously and to consider the real cost to individuals going through the many hurdles to register.

Finally, Dr. Jonathan Klaaren, Professor at University of Witwaterstad, WISER, South Africa pointed out the limit and social embeddedness of technology citing misuse of data by a private company hired by the South African government to administer social safety net payments to vulnerable households.

During the second portion of the session, panelists provided practical steps governments can take to ensure appropriate use of ID, including:

- There are several **critical pillars of an inclusive ID system**. This includes, transparent and independent adjudication mechanisms – courts, not administrative process - especially for nationality. Also, resources for paralegal assistance for those individuals whose applications are rejected (Manby).

- When designing an ID system, **realize that it will fail** - people will be excluded or not able to enroll. Biometrics will fail for some people. Systems will be breached. There will be fraudsters. **It is a question of failing well**. Key to the discussion has to be what happens when these failures happen, how can systems be in place to mitigate the issues - rather than relying on a picture of the world where things will always work as expected (Fisher).

- Proactive and constructive engagement with **civil society can improve the design of ID systems** (Fisher).

- Ensure a strong focus on the regulatory environment. Governments should undertake a regulatory impact analysis and **prioritize robust regulatory institutions**. Courts can play a back stop role as a regulator ensuring the right to be recognized by the law; right to a credential, if that's required to be recognized; right to citizenship (Klaaran).

- Look towards the Data Protection Authorities (DPAs) in West Africa: "They have a brilliant idea and system where some of them are requiring all government projects be submitted to the DPA… to consider the data impact" (Rutenberg)

- National ID systems are a public good and system specifications and processes should be transparent and open to public view. An ID system implemented in secret erodes trust and confidence in the government and invites speculation, rumors, and conspiracy theories. However, engagement is often superficial or token engagement if at all. (Rutenberg). Non- transparent systems will not work out in the way they were supposed to (Falconer).

- Recognize there are uses of certain technologies that are clearly deeply inappropriate in certain contexts (i.e., use of biometrics for people with HIV/AIDS). There does not have to be one single solution to all of these issues. Governments don't have to solve everything with one giant answer (or one ID). Efforts might be better placed in removing the barriers that ID that are in place recognizing barriers are often man-made. Avoid 'function creep' where ID creates its own reality in which everything requires ID (Fisher).

Key takeaways from the discussion included:

- Today, there is a significant trust deficient between ID issuers and individuals
- Public engagement is at the heart of ensuring the appropriate use of ID. Civil society must be engaged at each step to ensure the system is not discriminatory, used to exclude, invade privacy or for surveillance.
- Privacy is a human right. Call for a broader conversation on the mandatory use of issued ID and the potential to violate human rights. ID systems left unchecked can lead to exclusion. Collected data can lead to the creation of data profiles without consent which is a privacy risk.
- Significant need to identify meaningful mechanisms to (1) request consent related to each new purpose; (2) related data that may be collected; (3) explore realistic alternatives; and (4) apply human-rights lens to ensure the system includes rather than excludes.
- By not limiting mandatory use, there can be too much concentrated power by the ID issuer versus the power of the individuals. This can lead to denial of services, especially to vulnerable or persecuted groups, and increase statelessness.

- Today, ID is often imposed upon citizens, as opposed to the conventional statements that ID is a service for the citizenry. Often, people register out of fear rather than out of a belief that it's the right thing to be doing. ID issued by government or business must be narrowly scoped and serve a compelling public interest, not a private one.
- Robust safeguards need to be in place first to assure privacy, inclusion, personal value, choice and security.
- Transparent, accountable, trust-building practices are critical as any ID system must have sound governance to protect against mission creep and misuse.

Moving forward, delegates must consider the tension and trade-offs to rebalance power between ID issuers and individuals and the discussions around the appropriate use case are at the heart of the debate.

In closing, each panelist identified one thing to do today to ensure an ID has high value and remains low risk for individuals in 2030:

1. Recognize trans-national flow and build standards
2. Eradicate statelessness
3. Africa leads the decisions of new forms of ID without biometrics
4. Bring back basic ID
5. Put people's rights first and be less tech driven

---- END ----