Digitalizing Identity: Precautionary Thoughts on Ethiopia's "Fayda" Number

opiniojuris.org/2022/02/10/digitalizing-identity-precautionary-thoughts-on-ethiopias-fayda-number/

February 10, 2022

[Kebene Wodajo (PhD) is a senior research fellow at the Institute for Business Ethics, University of St. Gallen. Her current research project focuses on the question of justice and responsibility in cyberspace and she serves as an assistant editor of the African Journal of Business Ethics.*]*

Digital identity solutions are trending at national and global levels, supported by programs that are promoted and strongly backed by international institutions. They are aimed at realising among other things Agenda 16.9 of the UN's SDGs, namely the provision of legal identity for all, including birth certification by 2030. Proponents of the digital ID program often justify their position on the basis of improvements in access to basic services, education and national security as well as administrative facilitation. Building a properly documented legal identity is undoubtedly a positive move, but there is a difference between a written legal identification document and digital identity. The later conflates basic information and spearheads the process of using human data for authentication. These data often take the form of unchangeable biometric information such as fingerprints and iris recognition software. Experience shows that any deliberate or unintended sharing of such data can result in the undermining of fundamental rights such as privacy, freedom of expression, identity and movement as well as related socio-economic and cultural rights. Experience from India and Kenya has already demonstrated risks to privacy, exclusion and the replication of existing discrimination and inequality that comes with poorly regulated digital identification.

Discussions on digitalization focus too strongly on what can be achieved through digitalization and its promises are sometimes based on faulty constructs of techno-solutionism. Digitalization efforts, especially in the area of digital identity, need to be preceded by historical, contemporary and forward looking measures to avoid misuse. This piece reflects on these three dimensions to begin discussion on the problem by using the National digital ID program of Ethiopia as a case study.

Background to Ethiopia's National Identity Project

Ethiopia's National ID Program introduced a biometric ID system called the "Fayda Number" which is currently undergoing its trial phase. Digital identification is intended to serve as national and personal identifier to gain access to different public services. It will be regulated by an ID Authority that has yet to be established. IDs will be issued to all citizens and residents of Ethiopia in a project backed by the World Bank's Identification for Development (ID4D) program. The National Identity Project was recently joined by the Industrial Parks Development Corporation to run Ethiopia's National Identity Registration, which has so far enrolled over 20,000 citizens working at Bole Lemi Industrial Park. The project is contractually partnered with the TECH5 technology company headquartered in Geneva for the testing and evaluation of software used in this trial stage. TECH5 is one of several tech companies participating in a biometric retail payment and settlement system in India and Guinea's National ID project. The company does not have a publicly available human rights compliance and due diligence mechanism nor corporate responsibility policy. However, Ethiopia's National ID Protocol Document outlines guiding principles on privacy and minimal data collection, inclusion, authentication mechanisms and standards as well as the use of credentials, vendor neutrality and open standards based on security in design, grievance redressing and management, communications, governance, permanent independent entity, supervision and penalty procedures.

While these principles represent a good start in terms of protection, they are far from sufficient, mostly because they are stated in broad and vague language, despite the fact that the Protocol Document is designated to serve as a guiding principle for procedural decisions and adjudication until the formal establishment of an ID Authority. Core limitations for the project in its current form concern privacy. In terms of privacy and minimal data collection, the document states that:

> "Only those data necessary for establishing uniqueness will be collected. All data collected, stored in the NID database and/or published in the ID credential focuses on minimal data required to identify an individual, namely Full Name, Gender, Current Address and Date of Birth, all other data is optional…"

The Protocol also stressed that sensitive or "unnecessary" data such as religion, ethnicity or place of birth will not be collected. The principles of necessity and data minimization are important international benchmarks, and the draft Personal Data Protection Proclamation echoes these sentiments. However, the Protocol is limited in that it does not clarify which data will be considered "necessary for establishing uniqueness". This provides a leeway for arbitrary decisions and interpretations of the principle by the ID

Authority. There are also gaps in both the draft Proclamation and the Protocol on data categorized as sensitive. Both documents assert that data such as ethnicity, religion and place of birth will not be collected, since they are sensitive, but this has little practical implication. In the Ethiopian context, a person's ethnicity and religion can be inferred easily enough from their name/family name, and to some extent from their address and language preference.

The inclusion principle states that "the National Foundational ID service will be available to all citizens and non-citizens (legal residents) who can provide any type of acceptable evidence". It identifies three further principles: leaving no one behind, ensuring universal access free from discrimination and removing barriers to access. These are all valid principles, but without details that can guide users and implementers, they add little value. The requirement of any "type of acceptable evidence" is particularly vague. What kind of evidence falls within this category? The Protocol included having a witness as one type of evidence, but this hardly guides individuals. What if the person cannot find a witness, or if they do not have an identifying document for several socio-economic and political reasons, or if people are not willing to testify for them?

In terms of access to the service, it is unclear what procedural, institutional or legal mechanisms are in place to remove access barriers – whatever these barriers may be. One basic question should be to ask in what language will the service be available? All information on the website regarding the principles, use and registration for ID are in English, with a few things mentioned in Amharic. Ethiopia is a country comprising over 80 ethnic groups with different languages and children study at primary school in their mother tongue and at high school in English. Meanwhile, it is an internationally and constitutionally protected right that people should be able to access public services in a language they understand.

Precautionary notes to respond to this and other matters can be reflected in three dimensions: retrogressive, current and preventive.

Retrogressive Examination

Data and data driven technologies replicate past power relationships and inequalities, so if we seek to mitigate the influence of past inequalities through contemporary data driven technologies, we must begin by focusing on ways of addressing these inequalities. Injustices take different forms based on gender, ethnicity, socio-economic status and sometimes the intersection of all those factors. Ethiopia is a home to diverse ethnic groups with deeply divided and contested historical, political and economic narratives. The country has always been identified by an asymmetric socio-economic and political relationship between different ethnic and religious groups, and these inequalities are institutionalized through long-term policies and legislation. It is essential for digital ID to be designed and rolled out in a manner that neither replicates existing asymmetries nor aggravates contestations. For example, what language will be used, to whom will data be accessible and who runs the risk of exclusion? Legal and institutional mechanisms such

as procedural constraints on government agencies that have any form of access to personal data are vitally important, as is an independent oversight body that represents every group.

Contemporary Inquiry

Who develops the technology, and who collects, controls, processes and uses the data? What type of services and activities are linked to the digital ID program, and what legal and institutional protection is in place to protect the integrity of the system? These aspects are strongly linked to the retrogressive dimension. Ethiopia has a long history of digital repression and state surveillance, so why should we trust the government as custodian of our data? The current conflict situation shows that people are being ethnically profiled, targeted and surveilled – and we should therefore be worried about the centralization of peoples' data in the hands of the government, as it will enable further targeting and repression. Should we allow government misuse to be controlled through legislative and institutional mechanisms, and if so, does Ethiopia possess such legal and institutional infrastructure? Ethiopia currently has no data protection laws, although a draft law is under discussion. Even when the law finally arrives, enforceability will be another challenge. In institutional terms, the draft personal data protection law will establish a council, which will be accountable to the House of Peoples Representative, which is the legislative wing of the state. But the integrity and independence of the HoPR is questionable, and represents a factor that Ethiopia is still grappling with.

An anticipated response to the risk of ethnic profiling is that the information that will be collected is ethnically blind, which means that ethnicity will not be fed into the data. The draft personal data protection law specifies this under Article18 (3), and also specifies the exclusion of information related to person's religion in Article 18 (4). However, as mentioned above, this does not solve the problem of ethnic or religious profiling because peoples' ethnic identity and in some cases religion can be inferred from proxy information that is included in the dataset, such as their given name, family name and address. The solution for ethnically based profiling and targeting needs much deeper evaluation.

Ethiopia must go beyond the politically charged debate surrounding ethnicity, in which some people claim that ethnicity should be eradicated while others insist on retaining it as a central organizing factor. Both claims have limitations. Firstly, one cannot simply do away with ethnicity because that would be a breach of a person's fundamental right to identity. People have the right and freedom to identify themselves using factors that make the most sense to them based on their historical, socio-economic and cultural experience. Secondly, such claims are fallacious in both historical and contemporary terms. Past marginalization and injustices took place based on peoples' ethnic identity, which then took root in the institutional and policy structure of today's Ethiopia. This ultimately diverted the socio-economic policy preferences and political leaning of its citizens, affecting their demands. Ethnicity as an element of identity and a factor of political and policy decisions cannot simply be ignored, as it has been a part of Ethiopia for so long that many historical injustices committed in the name of ethnic identity cannot simply be negated through the removal of ethnicity from people's IDs. On the other hand, it is also

misguided to think of ethnicity as the only central factor of identity and outlook. Policy and political decisions are intertwined with dozens of other factors, including internal and external socio-economic and political aspects of life. There is no alternative but to find the right balance, but that alternative must look beyond easy answers such as the removal of ethnicity from the dataset.

Forward Looking (Preventative)

What are the pros and cons that we can anticipate from the rollout of the digital ID program? We can study and identify these factors through good practice and experience sharing, as well as mapping potential risk areas and function creeps. We must then design a combined social, legal and technological tool as a collective, building from the bottom up in a community-based setting that would enable the system to respond to these risks or failures. In case of breach of rights, judicial review processes must be in place, and legal experts, lawyers and judges who preside over such cases must have sufficient training and knowledge of the technical issues related to data, data driven technologies and their adverse implications for human rights. As mentioned above, it is important to put procedural constraints on the ID authority and other government agencies linked with the service. We must establish an oversight body, design a mechanism for the input and scrutiny of external groups such as grassroots, regional and international human rights groups.