Digital Identity, Surveillance, and Data Protection

Aishat Salami
Ridwan Oloyede

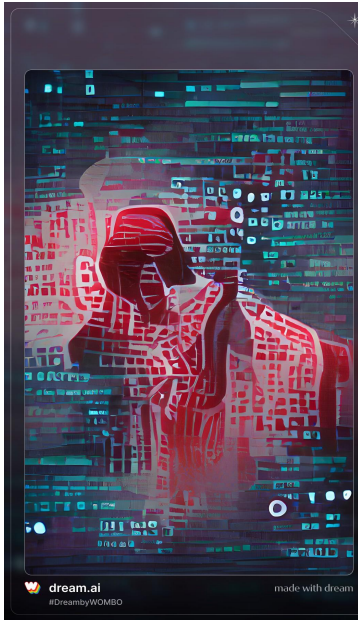
What is digital Identity?

A digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and is used for electronic transactions. It provides remote assurance that the person is who they purport to be. - (World Bank 2018)

Almost half of the 1 billion people without proof of identity live in Africa - World Bank

Some drivers for digital identity

- Social inclusion
- Financial inclusion
- National security
- Prevention of crime
- Prevention of electronic/election fraud



State of play

- A number of African countries are building or committing to building national digital identity systems, in realisation of the World Bank's Identity for Development initiative (ID4D), and the United Nations Sustainable Development Goal.
- Countries such as Botswana, Kenya, Morocco, Rwanda, Namibia have systems that are relatively advanced in terms of coverage and integration of their digital identity systems, but there are still the majority that are not as advanced
- In much of Africa, there is generally a lack of strong foundational identity systems.
- "Less than 45% of Sub-Saharan African children under the age of five have been registered in contrast to 98% in Central and Eastern Europe, 92% in Latin America and the Caribbean, and over 75% in East Asia". - (UNICEF Annual Report 2014)

TABLE 1: Common Models of Digital Identity Systems

Technology	**Estonia** **Institution**: Citizenship and Migration Board, within Ministry of Internal Affairs. **Registration**: Civil registration. **Credential**: Identity card with a photograph and a chip. **Target population**: 1.3 million people. **Use of ID based on**: Personal ID number (PIN).	**India** **Institution**: Unique Identification Authority of India, within Planning Commission of India. **Registration**: Biometrics (10 fingerprints and iris). **Credential**: No physical credential (a 12-digit unique ID number or "Aadhaar" is given). **Target population**: 1.2 billion people. **Use of ID based on**: Aadhaar number, along with demographic, biometric, or password.
Institutional Structure	**Ghana** **Institution**: National Identity Authority, within the Office of the President. **Registration**: Biometrics (fingerprints). **Credential**: National identity card ("Ghana Card"), and smartcard. **Target population**: 25 million people. **Use of ID based on**: National identity card and biometrics.	**Pakistan** **Institution**: National Database and Registration Authority (autonomous body). **Registration**: Biometrics (fingerprints). **Credential**: National identity card with a photograph, smartcard, and mobile ID. **Target population**: 180 million people. **Use of ID based on**: Smartcards, mobile phones, and biometrics.

Source: World Bank 2014

Problems inherent in Digital Identity Systems

Although digital identity aims to provide people with proof of identity and other economic, social, and political benefits; however the use and misuse of digital identity systems springs up concerns that cannot be ignored.

1. Digital ID registrations can be used as instruments of discrimination and for targeting vulnerable populations
2. Risk of Exclusion
3. Cybersecurity and privacy concerns
4. Surveillance
5. Commodification of data

Emerging issues

- Modernisation and digitisation of civil registry
- Funding for foundational biometric identity systems and border control.
- Regional collaboration on biometric identity system (ECOWAS)
- Sub-national unit adopting biometric residency registration systems
- Rise of private players in digital ID ecosystem
- Mandatory SIM registration
- Mandatory linkage of SIM registration and national identity registration
- Multiple biometric registration by government agencies
- AU Partnership for Digital Identity (2018)
- AU Draft Digital ID Framework
- EU-AU Partnership
- African Continental Free Trade Area (AfCFTA)

Regulatory framework pulse

Absence of independence

Inadequate human and financial resources

Poor implementation of law

Adoption of Digital ID program without data protection law or authority

Access to biometric database by law enforcement without safeguards

Mandatory linkage of SIM registration and identity database

Data protection	34 - Laws 26 - Autho 8 - Law X a 20 - No law

Legitimate aim for surveillance

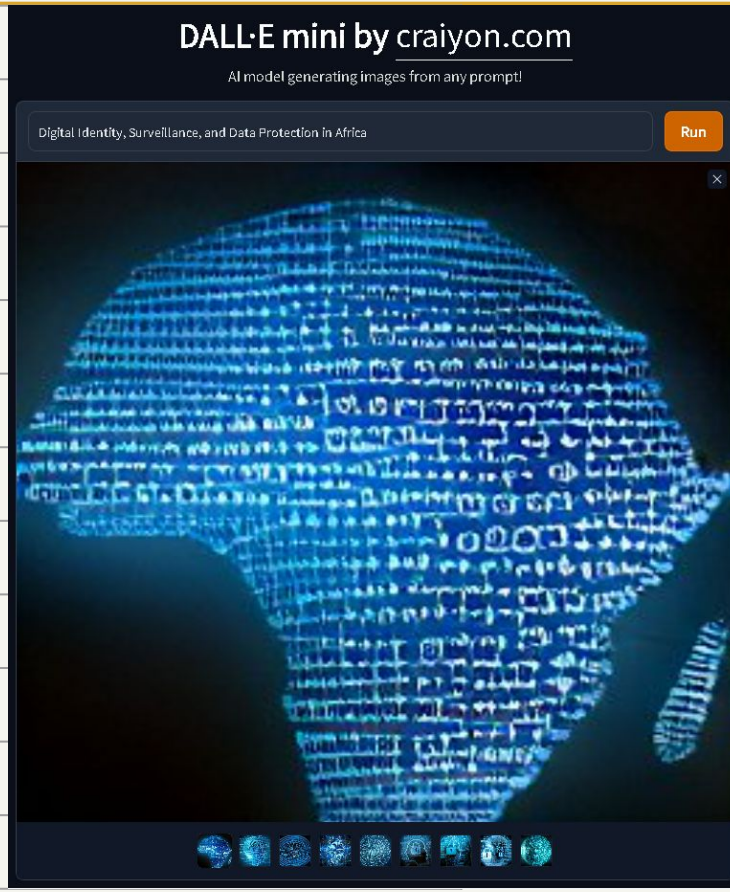
- National security
- Investigation of crimes
- Prevention of terrorism
- Protecting and safeguarding the economic wellbeing of a country
- Interest of public emergency or safety
- Giving effect to any international mutual assistance agreements

Emerging Issues

- Governments are making large investments in new surveillance technologies, passing laws that expand their legal surveillance powers, and conducting illegal surveillance of journalists, judges, and members of opposition
- Weakening or breaking of encryption
- The introduction of new laws that expand state surveillance powers
- Lack of legal precision and privacy safeguards in existing surveillance legislation
- Increased supply of new surveillance technologies that enable illegitimate surveillance.
- Absence of definition of legitimate aim and key terms
- State agencies regularly conducting surveillance outside of what is permitted in law
- Impunity for those committing illegitimate acts of surveillance.
- Insufficient capacity in civil society to hold the state fully accountable in law.
- Mandatory requirement to instal trackers on mobile telecom equipments
- Mandatory registration of SIM Cards and profiling

Surveillance laws against international human rights metrics

Surveillance laws located in a single document
Define legitimate aim
Authorisation of independent competent judicial authority
Periodic review by independent oversight body
Legality - must be contained in a law
Existence of reasonable grounds
Necessary to secure evidence
Test if surveillance measure is proportionate and limited in scope
Notify individual subject of surveillance time to appeal and request due process
Annual transparency report published publicly on requests and authorisation
Conduct Human Rights Impact Assessment before deploying tools
Conduct surveillance for the most severe crimes



Recommendations

- Enactment and implementation of data protection laws, with independent authorities to enforce the laws.
- Provision for specific regulations to be put in place, to govern the storage and use of the personal data collected.
- Formulation of inclusive policies that takes cognisance of gender disparities, and minority and marginalised groups.
- Participation of all stakeholders and wider public consultations in the development of digital identity systems.
- Need by Government to look beyond technological considerations, but also seek to remove the barriers to access and usage of digital ID.
- Enforcement of data protection safeguards and non-sharing of data with third parties.
- Provision of legal identification free from discrimination to all relevant persons in a country.
- Introduction of trust framework in identity management system.

Thanks!

Any questions ?