OMIDYAR NETWORK

A WORLD OF POSITIVE RETURNS

Submission: UNHCR Global Virtual Summit on Digital Identity for Refugees (April 2019)
Geographic focus: Global, Africa

Good ID: Ethical design and practice for refugees and displaced populations

Background

Technology-driven changes are radically transforming the world. Nowhere is this truer than across Africa as countries 'leapfrog' straight to digital economies. Digital identity systems are increasing worldwide with 148 countries already issuing some form of digital ID (e.g., barcode, magnetic strip, smart card, token). In parallel, large international organizations - including UN and humanitarian agencies - issue millions of IDs per year in over 100 countries. An issued ID, in its most basic form, is often prerequisite to access education, information, and jobs, and increasingly required for SIM purchase and to facilitate KYC. In advanced forms, an ID on digital channels, can build authentic and verifiable information, such as a credit history, and unlock access to a broader range of products and services.

At least 500 million, or half of the African population, have no formal, issued ID or an have an ID with a single-application use case or location-tied paper-based format. An estimated 60% of African countries will launch or refresh national ID programs between 2018 and 2020, with 90% of them having a digital element. While a digital identity can be an entry point and critical enabler to services, it can result in significant risks if not designed with a human rights lens, clear value to the user, appropriate safeguards, and be 'privacy enhancing' rather than 'privacy-threatening.' Any new ID system must focus on coverage and quality.

Why it Matters?

Today, Africa hosts the world's largest migrant population, including 258 million cross-border migrants and 19+ million people that have been forcibly displaced. Many IDPs could cross-borders at any point and become refugees as is happening today in South Sudan, Uganda, and Ethiopia. The introduction of a new ID system can amplify existing conflicts or exclusion without proper design and considerations. Africa hosts the world's largest migrant population, including 258 million cross-border migrants and 19+ million forcibly displaced. Many IDPs could cross-borders and become refugees as is happening today in Cameroon, Ethiopia, Mali, South Sudan, and Uganda among others.

- The majority of the 500+ million Africans without any form of legal or issued ID, live, are in transit or displaced in countries with high levels of forced displacement and growing refugee populations.
- Simultaneously, many of these countries are rolling-out new digital identity systems without safeguards (e.g., data protection and privacy laws), a human rights lens, and unclear mandates between who is a citizen or a resident (e.g., DRC, Ethiopia, Kenya, Nigeria).
- New and protracted conflicts coupled with climate change impacts, will significantly increase the number of forcibly displaced people and extend current displacement. Each year, an average of 24 million people are displaced due to extreme climatic events, according to the Internal Displacement

Monitoring Center. By 2050, the World Bank predicts, over 143 million people across sub-Saharan Africa, South Asia, and Latin America will become 'climate refugees.'
- Displaced populations have changing identity needs at different stages of displacement (transit, arrival, settlement, return, etc.).
- Often in acute crisis or reaction to a humanitarian crisis, ID systems are designed lacking recognition of power and information asymmetries and differing incentives around consent for data protection and privacy.
- Growing concerns that once digitized, a person will no longer have the choice to identify as they choose or as needed for safety purposes (i.e., at border crossings, in hostile situations).

What is Good ID in design and practice?
Omidyar Network uses the term "Good ID" to characterize empowering forms of digital identity. *Good ID is a normative framing for any digital identity system that prioritizes individual empowerment while ensuring adequate safeguards.*

Specifically, Good ID is:
- Inclusive, offers significant personal value, and empowers individuals with privacy, security, and control.
- Builds trust with transparency, accountability, and portability.
- Seeks to address exclusion, discrimination, surveillance, and consent.

Good ID recognizes that the potential positive benefits of digital identity are not guaranteed. Obtaining a digital ID can help unlock new opportunities, it can also introduce new risks and challenges.
- How an ID system is designed, rolled out, and managed can include and protect individuals with privacy, security, and control.
- Or it can reinforce power imbalances, exclude, discriminate, and support surveillance.

Markets and technology can be forces for good, but only as part of a broader social contract.

How would I know Good ID when I see it?
Good ID is a function of both good practice and ethical technology and policy design.

PRACTICE

Transparent, accountable, sustained public engagement, and other trust-building practices lead to Good ID. In today's trust-deficient society, there are many good reasons why a digital ID issuer would want to support Good ID.

UNHCR should -
- View existing civil registry systems and new digital identity as a positive sum game
- Make and fulfill public commitments to include users in all decision-making processes and protect their human rights and interests
- Use ethical and legal frameworks, scenario-based tools (such as Ethical OS), feedback loops, and future-resilient tools to make informed decisions before and after systems are built
- Show radical transparency about the choices and decisions being made along the way, including policies, design and data sharing contracts, tenders, and protocols.
- Use open-standards and open-source technology to facilitate future evolutions of the system, without dependency on one vendor

- Commit to inoperability between UN agencies and complementary humanitarian agencies to reduce the need to re-register and authenticate
- Take accountability and provide simple and satisfactory recourse for grievances through guidelines and norms if legislation is pending or not yet in practice. Use the UN influence to push for human rights respecting safeguards to include a data protection law with internationally agreed minimum standards and enforcement authority.
- Prioritize trust and user participation as important proxies for good policies, technologies, and practices

DESIGN FEATURES

Design features in technologies and policies lead to Good ID. Omidyar Network prioritizes five features that apply to all forms of digital ID, support individual empowerment and equity, and anchor Good ID.

1. PRIVACY

Privacy is a fundamental human right.

If privacy is missing or lacking depth, an ID system will not truly empower. Protect privacy with design choices and establishing a robust governance framework. Limit the data collected, give the legal right to change how identity information is used, fully disclose how identity data will be used, and proactively notify individuals when privacy policies change. Providing end-to-end encryption of content is a grossly inadequate way of addressing privacy concerns and can lead to perverse incentives.[1]

2. INCLUSION

Inclusion is the foundation of Good ID.

Good ID makes digital ID systems accessible and fair with inclusive practices and features. *Digital identity is not derived from and does not confer citizenship and will be provided to citizens and non-citizens alike*. Anyone should have the right to utilize digital identity systems to prove who they are for all public and/or private services. Simply put, anyone who wants a digital identity should be able to get one, free from discrimination or limitation, from the country where they legally reside. At the same time, individuals should have access to alternative means of identification and choices in how they identify themselves.

To include the most people, users must have confidence in the system's privacy; adding more individuals from marginalized groups to poorly designed digital ID systems that track their location or note their ethnicity, religion, refugee status will only intensify vulnerability. *In such cases, it may be better not to have a digital identity at all.*

Good ID offers:

- Equal and fair opportunity for everyone to establish/use digital identities to authenticate
- Limits number and situations when digital ID is mandatory

[1] Read "Digital Identity and Privacy" for more ways privacy-by-design can lay the foundation for Good ID.

- Alternatives when individuals wish to participate, but not use a particular form of digital ID
- Low barriers in establishing and using identities (e.g., require minimal data to register/authenticate)
- Safeguards against discrimination (e.g., processing applications inconsistently among different ethnic groups, religions, gender identities)
- Mechanisms to manage unintended consequences (e.g. clerical/technology errors that exclude, remediation for any related harms

3. PERSONAL VALUE

Good ID is defined by high, personal value for users.

The amount of friction and vulnerabilities individuals experience increases or decreases that value. Good ID shouldn't be difficult ID.

Good ID must offer:

- Access to a range of meaningful services
- Accurate and precise records, reflecting the users' preferred level of privacy
- Convenience in use, registration, and management
- Interoperability and portability so identities work across services, sectors, and geographies while upholding security and privacy

4. USER AGENCY

Good ID is embedded with personal agency + ability for individuals to control and manage their digital identities.

Good ID must offer:

- Transparency to see who is collecting and divulging data, what data trails are forming, how others use and process their information, and for what purposes
- Mechanisms for meaningful, informed consent related to each new purpose and before any identity data is shared with another party; individuals can choose and change who uses and accesses their identity data; for how long and for what purpose; and have the ability to update and remove their data as needed
- Options for individuals to deny use of their identity, update records when identity information changes, and revoke permission even after permission has been granted
- Alternatives when individuals wish to participate, but not use a particular form of digital ID or disclose identity information beyond what is strictly necessary
- Recourse in the event of regulatory violations and user grievances supported by clear, legal frameworks

5. SECURITY

Privacy is not possible without security. Good ID makes transacting in a digital world safer by minimizing vulnerability.

Good ID must offer:

- Data integrity, including limits on the amount of data collected, how it is stored and used, and how it will be disseminated with clear roles and expectations governing the behavior of system administrators and anyone who interacts with identity data
  - Rigorous cybersecurity practices and defensible systems, strong encryption, and audits, that evolve to mitigate threats and block unintended or unauthorized access, disclosure, or manipulation
  - Safeguards from breaches, corruption, or loss of personal data embedded in technology design, operational controls, and regulations
  - Timely disclosure of breaches to all parties affected
  - Public and private frameworks that embed an audit trail, assign responsibility, and provide for recourse in the case of a security leakage or breach

This normative framing will have to evolve with new thinking, new technology, new experiences, and new societal expectations, especially as it relates to refugees and other forcibly displaced populations.

Areas to explore with UNHCR:

- Consent is critical to privacy-by-design; how will new technologies introduce alternative forms of consent for agency over data?
- How can we increase trust anchors to offer identity proofing and attestations?
- How can we to assist policymakers keep pace with the evolving digital identity landscape to shape laws and regulations that enable innovation and reduce hurdles to adoption, while safeguarding data, privacy for displaced populations or those in transit?

Please help unlock the full potential of Good ID by sharing your learning, viewpoints, projects, events, and other resources on the Good ID online platforms—www.good-id.org and @GoodID or contact tanderson@omidyar.com