EXECUTIVE SUMMARY:

IDENTITY IN A DIGITAL AGE: INFRASTRUCTURE FOR INCLUSIVE DEVELOPMENT

USAID
FROM THE AMERICAN PEOPLE

This report was written by the Strategy & Research team within the Center for Digital Development at USAID. The team would like to thank every organization and individual interviewed during the course of the research, and those who offered feedback and counsel along the way. Without your expertise, insight, and support, this report would not have been possible.

Cover Photo © Dominic Chavez/World Bank

Executive Summary

There may be no single factor that affects a person's ability to share in the gains of global development as much as having an official identity. Identity unlocks formal services as diverse as voting, financial account ownership, loan applications, business registration, land titling, social protection payments, and school enrollment. Robust identity systems can help protect against human trafficking or child marriage. In many ways, the roughly 1.1 billion people who lack official identity are invisible, discounted, and left behind. The need for clear understanding and informed engagement around ID technologies has never been greater.

1.1 B

In many ways, the roughly 1.1 billion people who lack official identity are invisible, discounted, and left behind.

This report offers guidance on how to address the systemic problems of today's digital ID (DID) systems, while critically assessing how emerging technologies will shape the future of DID. Today, donor investments in DID systems are often confined to sector silos. These systems are built to support specific programs, which leads to a proliferation of fragmented systems. At the same time, technology is changing at a rapid pace. Emerging trends like blockchain, advanced biometrics, and algorithmic identification will transform the DID landscape.

How the development community responds to this evolving landscape will affect whether DID is an instrument of surveillance and exploitation or empowerment and inclusion. USAID and the donor community can take steps now to support DID systems that generate mass efficiencies for development programs, and at the same time, create pathways to inclusive, sustainable digital infrastructure that will enhance development goals.

From Digital IDs to Digital Infrastructure

The first part of the report focuses on how development actors must shift from an instrumental to an infrastructural approach to DIDs. Development actors turn to DID systems for a variety of reasons – often to streamline humanitarian and social services, or to better support data-driven programming. This is what we term an 'instrumental approach,' wherein a DID system is treated as an instrument, as a means to solve a specific problem and achieve a single goal in a unique context. While this is a natural result of how donors do business, it can lead to a proliferation of isolated, single-application ID systems, thereby generating waste and significant opportunity cost.

Photo: Mohammad Al-Arief/The World Bank

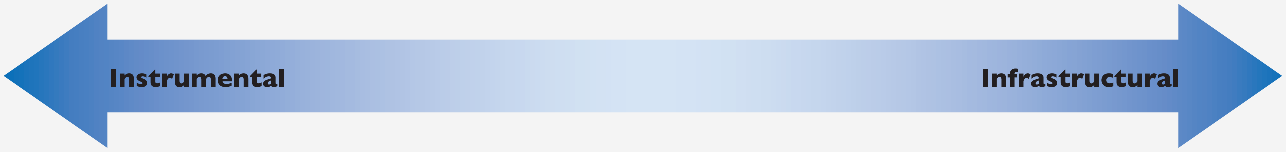
Take biometric voter registration (BVR) as an example. BVR has become a popular tool to reduce fraud and increase the transparency and legitimacy of elections. At the same time, many countries do not maintain a continuous voter roll. Instead, voter rolls are re-built from scratch and each voter is re-registered for each election. Gelb and Diofasi[1] surveyed BVR efforts in 12 African countries during 2010-2015 and found that the median cost of one-time biometric registration is $3.10 per voter. By contrast, South Africa uses a continuous voter roll with maintenance costs of about $1 per voter for each election cycle. If the 12 countries surveyed switched to the South African model, on average each would save $16 million per election. These efficiencies represent a small fraction of anticipated savings given the myriad DID systems supported across agriculture, health, education, and financial services.

This instrumental approach is not only inefficient but myopic. Designing an isolated DID system for a singular goal ignores the social, political, legal, and economic context essential for the program's success. For example, imagine a digital ID scheme is created to streamline delivery of social protection services to internally displaced persons, but registration for the ID requires collection of biometric and ethnic information. Concerns about data privacy and persecution may prove significant enough that they actually cause the groups most in need of these services not to register at all. Failure to balance political and social dynamics of ID systems can thwart the initial program goals and may negatively affect the broader system.

In total, treating DID as a means to an end rather than as a key component of a complex system results in a fragmented DID landscape. Again, BVR systems are a useful example; individual voters might have ID cards for several recent elections, each funded by a different donor and implemented by a different NGO. Multiple isolated systems serve the same population one election at a time, and data cannot be shared because of inconsistent standards or proprietary conventions. In the long run, this increases costs, overburdens users, and can exacerbate the systemic problems donors hope to solve.

[1] Gelb & Diofasi (2016). "Biometric elections in poor countries: Wasteful or a worthwhile investment?" Center for Global Development Working Paper 435.

In contrast, an infrastructural approach views DID systems as core infrastructure to support other systems and activities. Much like roads, bridges, or fiber-optic connections, they outlive the projects they were designed to support. As with physical infrastructure, a DID system's utility and compatibility with existing local systems are key to a long and productive "afterlife." Infrastructural DID systems contribute to a more cohesive and sustainable DID ecosystem by connecting or underpinning disparate systems and allowing for efficient reuse.



- Purpose limited to single project
- Design, implementation, and phase-out driven by project time frame
- Dependent on custom software, hardware, and/or data standards
- Almost always functional

- Built with long-term objective
- Designed in collaboration with local stakeholders
- Utilizes open source platforms and open standards
- Compatible with local systems when possible
- Could be repurposed or reused for other use cases with minimal additional resources
- Functional or foundational

Instrumental and infrastructural approaches should be seen as two ends of a spectrum; many DID systems have some elements of both approaches. A shift toward a more infrastructural approach will generate long-term cost-efficiencies for funders, meet the needs of diverse populations, and improve public service delivery. While a necessary short-term step, such a shift constitutes a woefully insufficient response to emerging technologies.

Preparing for the Future of Digital ID

The second part of the report interrogates the new opportunities emerging to identify the unidentified. For example, new technology applications are able to uniquely identify and characterize people based on digital traces rather than demographic data, which traditional approaches rely upon. Data from mobile phone use[2], social media participation[3], and e-commerce[4] can uniquely identify people. Advances in biometrics may similarly open up new ways of identifying and authenticating people who are currently excluded from or underserved by existing ID systems. At the same time, these advances introduce new concerns related to exclusion, surveillance, data privacy, and control over data sharing and use. The report's findings, below, offer a roadmap for how development actors might understand five key trends—advances in biometrics, mobile ID, algorithmic identification, blockchain-backed ID, and user-controlled identity--such that they can lever the opportunities and mitigate the risks.

First, the utility of these technologies depend on the ability of the most marginalized to access and use the technologies. If we cannot bridge the digital divide, the use of emerging technologies risks cementing exclusion and compounding existing inequalities. People must be able to make meaningful use of the technology itself and understand its implications. This doesn't simply mean that users have access to a mobile phone or the Internet, but that they are digitally literate and understand how their personal data is being used.

[2] de Montjoye et al. (2013). "Unique in the Crowd:The privacy bounds of human mobility." Nature Scientific Reports 3, 1376.
[3] Narayanan & Shmatikov (2009). "De-anonymizing social networks." 30th IEEE Symposium on Security and Privacy.
[4] de Montjoye et al. (2015). "Unique in the shopping mall: On the reidentifiability of credit card metadata." Science 347 (6221), 536-5

Second, emerging technologies can also reinforce existing biases or create new exclusions. In algorithmic systems, for example, accuracy can suffer when algorithms are used in a context different from the one for which they were designed. This might happen when an algorithmic ID provider expands into a new, poorly understood market in which mobile phone usage patterns differ from those of the original market. Similar problems can arise with minority populations whose behavior differs from the majority. Biometrics such as facial recognition may fail when applied to diverse populations. Development actors must take care to ensure that digital ID systems are inclusive and context-appropriate.

Third, technology is no substitute for trust. Until we have more experience with new technologies, we will not know how well they function or what consequences they may have. Conducting field tests can help the development community understand how data-intensive technologies transform prior notions of trust.

Fourth, systems will only get more complex and fragmented as donors and technology companies increasingly offer alternative DID systems to traditional government offerings. This will be especially true in places where official government ID is hard to get and alternatives have more appeal. Harmonization and standardization of new ID systems should be a key goal of ID investors. But potential for surveillance abuse is rife with data-enabled ID technology. As we prioritize harmonization, we must strive for balance between greater ease of integration and the preservation of privacy and individual rights.

As ID-mediated relationships grow more diffuse and complex, trust between people and institutions will play a dominant role.

Recommendations

There are four main things donors can do to shift toward an infrastructural approach and adequately prepare for the future of DIDs.

1. **Develop guidance and a technical support framework:** When donors identify areas where our collective experience is lacking, we should prioritize building a robust body of evidence to address a lack of good practices guidance. Developing explicit resources on good practices and DID guidance could have real impact on donors' ability to shift to more sustainable infrastructural investments. A shared decisional framework could prompt early-stage consideration of such critical factors as local policy and regulatory environmental factors, or could provide guidance on weighing privacy risks against identification needs. In our research, interviewees lamented the lack of internal guidance or technical support for their DID efforts. Filling this gap should be a first step toward more impactful and effective systems.

2. **Invest in sustainable, cross-functional DID schemes:** An infrastructural investment strategy would move donors away from reliance on one-time-use DID schemes. To take a step toward such a shift, we recommend investing in DID systems that use open standards and open software platforms. Deliberate efforts should be made to partner with local government actors by default. If partnering with local partners is not appropriate, a sector-agnostic approach will still help donors prioritize and assess infrastructural components of a system. This shift in investment approach would serve multiple actors and multiple use cases and position our investments to outlive our projects.

3. **Mitigate Privacy Risks:** Digital ID creates a unique linkage of people with their personal information. As digital ID schemes proliferate and interlink with emerging technologies, we face an increased risk

that data will be stolen, misused, or leaked. We can mitigate privacy risks on multiple fronts. For example, we can advocate for data protection laws in the countries where we work or incentivize stronger adherence to laws when they are already in place. Internally, donors can prioritize the development of standardized risk-benefit assessment frameworks when we work with personal data collection, use, and sharing.

4. **Convene locally and collaborate globally:** If DID investments are to support sustainable, equitable global growth, we must work collaboratively to embrace a more unified vision of digital identity systems across sectoral and organizational silos. Working together will help us adopt, develop, and promote good practices and a principled approach to digital ID. Donors should join the conversations that are happening globally to learn from leaders in this space and mobilize around a shared vision of sustainable, equitable identity systems. At the same time, we should exercise our convening power to bring together local actors—implementing partners, local governments, civil society organizations—to mitigate system fragmentation and work toward more sustainable identity infrastructure.

Moving Forward

The future of DIDs is not predetermined. Fragmentation may persist. The gap between those who benefit from emerging technologies may grow, compounding existing inequities. Privacy breaches may overwhelm any benefit enabled by new data types. Donors like USAID have a tremendous opportunity to help ensure a future wherein digital identity is infrastructure for inclusive development and no one is left behind.

Photo: Athit Perawongmetha / World Bank