



# 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.

# Table of Contents

Executive Summary .....	1
Introduction .....	2
Identity, Trust, and Power .....	3
Balancing Individual and Institutional Interest .....	4
Background: Understanding the Scope of the Problem .....	7
Digital ID Systems: How They Work .....	9
<b>PART 1</b>	
From Digital ID to Digital Infrastructure.....	15
Current Approaches to Digital ID Systems in Development.....	17
Consequences of Instrumental DID Schemes .....	22
Summary of Digital ID System Landscaping.....	41
<b>PART 2</b>	
Preparing for Futures of Digital ID .....	43
An Evolving DID Landscape.....	44
Biometric Advances.....	47
Mobile ID .....	51
Algorithmic ID.....	55
Blockchain-Backed ID .....	59
User-Controlled ID .....	63
Trend Implications .....	66
Systems-level Implications.....	70
Recommendations and Moving Forward .....	74



# 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.<sup>1</sup> 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.



## 1.1 B

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

Donors' investments in identification (ID) systems are often confined to sector silos. ID systems are built in support of a programmatic goal, not as development infrastructure critical for a digital age. This leads to inefficient use of resources and has caused international development actors to miss opportunities to make more sustainable, transformative technology investments.

Donors can take steps now to ensure our investments in digital ID (DID) serve as infrastructure for private sector investment, civic involvement, and economic empowerment. As donors work to rationalize our investments in digital ID systems, technology is changing at a rapid pace. Advanced biometrics, mobile authentication, blockchain-backed ID systems, and user-controlled ID will transform the ID landscape. Indeed, they already are. How we address these emerging trends in technology will determine whether ID is an instrument of empowerment and inclusion or surveillance, disempowerment, and exclusion.

Part 1 of this report will introduce a conceptual framework that distinguishes between two approaches to ID in development. An *instrumental approach* focuses on ID as a tool with which to accomplish the goals of a specific development project. In contrast, an *infrastructural approach* sees ID as an investment in the enabling environment for a modern economy – something with benefits that are longer-term and more diffuse. To promote sustainable progress over the long term, our recommendations will argue for long-term investments in ID infrastructure. Institutions and individuals each have key roles in the ID ecosystem, and we will discuss the tensions and opportunities inherent in trying to serve both.

Part 2 asks how the ID landscape is changing. Emerging technologies will expand the options for identifying and authenticating individuals and introduce new actors across the DID value chain. While some emerging trends may offer greater opportunity for inclusion, higher

<sup>1</sup>The widely-accepted "[Principles on Identification](#)" define identity as "a set of attributes that uniquely describes an individual or entity." Legal identity systems are "those that register and identify individuals to provide government-recognized credentials (e.g. identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity." Legal identification in this sense is unrelated to legal status in the sense of nationality or citizenship; we will use the term official identity to avoid confusion on this point.

[World Bank Group and Center for Global Development \(2017\), "Principles on Identification for Sustainable Development: Toward the Digital Age."](#)





Photo: Mohammad Al-Arief/The World Bank

confidence in authentication, or better data security, new technologies and new actors may also change the roles of traditional ID-granting institutions and their relationships with ID-holding individuals. For example, as better-connected users demand more frictionless ID-enabled services, governments and companies will need to form new partnerships in an increasingly crowded ID-services space. In addition to today's major players (mostly governments and banks), we may see more focused "identity companies" for whom ID services are their major business focus. As non-government entities become more important ID issuers, governments may see increasing competition for the provision of authoritative ID.

Based on our analysis of the current DID landscape and emerging trends, we make several recommendations for donors. First among them is to shift existing sectorally

bound investments to **more sustainable, cross-functional ID systems**. Bundling project-driven needs together with longer term infrastructure building will help ensure sustained development outcomes in the future. Second, it is essential that we **preserve privacy** by promoting data protection policies, modeling best practices in our work, and keeping abreast of emerging ID technology developments. Lastly, these are all complex, multi-stakeholder challenges that will hinge on **strong partnerships with DID pioneers** to harmonize systems and ensure that even the most vulnerable voices are heard. We must commit to working collaboratively to promote the responsible and beneficial development of identity in a digital age.

# Introduction

ID is far more than just a card with a name and a photograph. ID technologies sit at the interface between the power and prerogatives of institutions and the rights and needs of individuals. They can help create a basis of trust and inclusion that strengthens democracies and free market economies. They can also be used by authoritarian regimes to exclude or oppress. Rapid technological change is making the political and social context around ID systems increasingly complex. The need for clear understanding and informed engagement around ID systems and technologies has never been greater.

In recent years, development organizations have shown growing interest in ID. Sustainable Development Goal 16.9 calls for “legal identity for all, including birth registration.” In many countries, strong birth registration systems have enabled the creation of more advanced ID systems. At the same time, ID extends far beyond registration; a well-functioning ID system enables civic engagement, financial inclusion, and the exercise of legal rights.

Digital technology is increasingly used to collect, process, and store the data that ensures the integrity of ID systems. In many cases tools such as biometrics, smart cards, or public-key infrastructure are used to safeguard credentials. Compared to paper-based systems, digital ID strengthens security and can be linked to more diverse services. Where citizens’ experience of governance has been characterized by graft and abuse, automation of the citizen–state interface can help rebuild trust.<sup>2</sup> By leveraging the digital footprints of a connected population, digital ID opens new routes to inclusion for people who lack formal documentation. Many ID-related risks—including mass surveillance, data breaches, and identity theft—are also heightened by new and emerging digital ID technologies.

This report assesses the opportunities and risks of digital ID systems in development. We particularly focus on the role of project-driven ID investments and argue for a broader view of digital ID as essential development infrastructure.

## Identity, Trust, and Power

Trusting the assertion that “you are who you claim to be” is possible in small communities where everyone knows everyone else. In a “village” model of ID, your personal relationships and reputation determine whether and in what circumstance others trust you. In modern societies, many of our interpersonal interactions are nearly anonymous, and this relational basis for trust breaks down. Today, many of our relationships and transactions are digital, and our partners in business or conversation are present only virtually. When our relationships reach beyond our immediate communities, countries, or continents, proxy-based systems of establishing trust are critical. Such systems often rely on ID *tokens*—physical objects (e.g., a card) or pieces of information (e.g., a PIN or password) that are used to support identity claims.

<sup>2</sup> Gelb & Clark (2013). “[Identification for Development: The Biometrics Revolution](#),” Center for Global Development Working Paper 315.



The relationship between digital technologies, identification, and trust is complex. Some communities have preserved trust in reputation-based ID systems as digital proxies developed. In others, digital technologies have come to substitute for it. For example, GSMA's recent research on user experience of ID<sup>3</sup> finds that in Tanzania, a non-digital ID token, ward letters, tend to be highly trusted forms of ID because they are established by a personal relationship with a local official. No birth records are kept or linked to getting a ward letter, yet the ward letter is widely accepted and trusted for most services. Interestingly, a voter ID card is accepted as ID for some services where the ward letter isn't — for example, banking or enrolling in college. While a voter ID is similarly issued by a local ward with no other ID requirements, the voter ID card can support biometric authentication. For these use cases, digital technology enhanced the security of authentication, but did not change the underlying process of identity proofing at the ward level.

Pakistan also has a reputation-based ID token, the Numberdar reference, which individuals get from the local town chief. Despite being issued as a sign of trust and connection with an individual, the Numberdar reference has very limited use. Instead, the Computerized National Identity Card (CNIC), which requires registration through the national enrollment system, is the required ID for nearly all services.

Identification is ultimately about trust. An ID token can serve as a trust proxy; if a person wants to engage in a government or business transaction, she will often be asked to present ID. Her claim to be a particular person—one who is eligible to vote or likely to repay a loan or return a rental car—is bolstered by the fact that she has been recognized by a formal institution. That ID token also reduces the institution's risk by giving transaction partners a way to follow up, possibly with the help of police or collection agencies, if she proves untrustworthy. The act of being identified, in short, replaces anonymity with a proxy for trust.

## Balancing Individual and Institutional Interest

States have historically played a central role in generating formal identity credentials. Centralization—of expertise, coercive force, information, and social connections—makes governments credible ID providers, but also gives them immense power over their citizens. An ID provider has power to affirm or deny a person's identity claims and to decide what content those claims must include. Access to ID registration facilities can be restricted to ensure that undesirable people remain anonymous and marginalized. Inclusion of ethnicity or religion on ID cards can be used to reify or obscure divisions and target

some groups for persecution. Conversely, the state's identifying power can also be used to foster national unity, build trust, and reconcile internal strife. Official ID literally lets citizens carry around a small piece of their government, contributing to a sense of representation and accountability.

Governments are not the only providers of ID credentials. Other institutions, including private companies, NGOs, and aid agencies, create ID systems to further their own goals. IDs from different institutions will come with different forms of legitimacy and risk, but some challenges are common. Institutions can be swayed by the allure of flashy technology commonly pushed by tech vendors, regardless of the appropriateness for the given context.<sup>4</sup> Institutions also tend to favor systems that prioritize their own desires for efficiency over the needs and experiences of ID users. A narrow focus on institutional goals often leads to sectorally siloed ID systems that are “locked in” with specific vendors. This leads, in turn, to mass inefficiencies—a single person may carry different IDs for health insurance, voting, education, or other purposes.

<sup>3</sup> GSMA (2017) “[Driving Adoption of Digital Identity for Sustainable Development: An End-user Perspective Report](#).”

<sup>4</sup> At the same time, sometimes the purchase of high-tech ID systems does more to make the institution appear modern than to add value for those who use it.



## From baby footprints to digital footprints

Present-day ID systems are epitomized by the inked footprints found on many birth certificates. Institutionally provided IDs tend to rely on standardized physical traits and biographical information like one's legal name, date of birth, and fingerprints. These characteristics, unlike reputation, can be more efficient for large-scale institutions: they require little to no familiarity with the individual, can be collected of most individuals, and remain relatively fixed over time. This means people can be identified once, recognized as a unique individual by an institution, and remain identifiable with relatively few future interactions.

Although baby footprints mark the ID systems of today, the ID systems of the future may depend instead on a digital footprint. Digital records of a person's transactions, activities, and connections are diffuse, constantly changing, and unique. Even among the world's poor, these digital footprints are constantly growing and becoming more individualized. Digital technology is enabling new ways to use a person's behavior to establish trust in their identity. This can take the form of using more advanced biometrics or mobile phones for stronger authentication, employing algorithms to authenticate identity or authorize services, or relying on distributed ledger technology to protect the integrity of information. With a growing reliance on these trends, ID systems of the future may disrupt the roles of traditional identity-granting institutions.

We are beginning to see a reprise of the “village” identity systems of the past, where reputation is now established from digital rather than in-person interactions. Digital interactions can occur faster, with many different individual and institutional actors. This means that digital identities of the future may also be more dynamic than those of today, recreated and affirmed with each digital interaction.

Digital sources of personal information are easily available and can function as highly unique identifiers. They are also “noisier” and more heterogeneous than the well-

ordered databases of traditional ID systems. Identification based on these sources will be inherently probabilistic; the level of confidence placed in any identity assertion will increase as more reputation-bolstering data are gathered. In reality, identification has always been messy and probabilistic; digital tools let us estimate the risk of mistaken identity more precisely and better optimize systems to encourage trust.

ID systems of the future could lead to more avenues for inclusion, more tailored civic representation, and more efficiency for institutions that rely on ID. But the promises inherent in these digital shifts also bring the potential for harm. Digitally enabled systems could further solidify existing exclusions or increase the potential for individual surveillance and privacy abuse. Development donor agencies often fund or build systems that will be used by other ID stakeholders. These uses could stretch beyond our original intentions—an initially benign system could be re-deployed for surveillance or suppression—or be artificially limited by the siloes we impose on our projects. We must understand how digital tools operate in their social context to avoid the unintended consequences and missed opportunities of digital development.

## Structure of the report

The report includes three main sections. First, in the Background, we provide a closer look at the current landscape of national-level digital identity systems. Next, in Part I, we present our findings from our internal research on how USAID specifically currently approaches digital identity systems. We highlight key missed opportunities and analyze what contributes to the success and failure of digital ID systems. In Part 2, we look beyond existing digital ID investments and consider how emerging technology trends are changing the digital ID ecosystem, looking into five emerging trends in digital ID: advanced biometrics, mobile authentication, algorithmic ID, blockchain-backed ID systems, and user controlled ID. We consider use cases in development, potential advantages and risks, and system level implications of each trend. We conclude with several points to consider as the digital ID landscape continues to evolve.

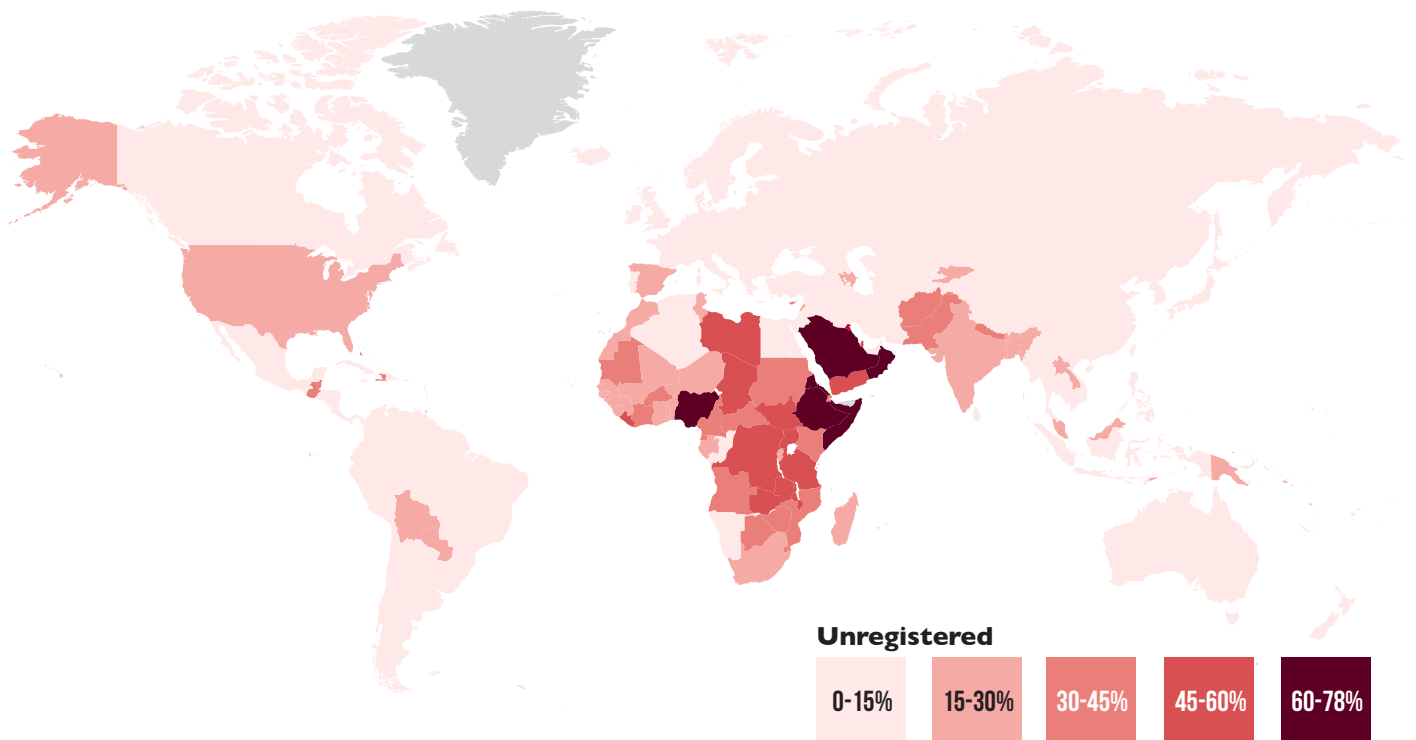


# Background

## Understanding the Scope of the Problem

Existing ID systems often fall short of the potential for sustainable inclusion in two key ways. First, despite progress in some areas of the world, many people still lack formal identification. This identification gap is most pronounced in regions that bear the highest burden of extreme poverty. Second, official ID systems that do reach their intended populations often fail to deliver on the vision of ID advocates because they are not well-integrated with service delivery or compelling use cases.

The most comprehensive dataset on official identity is currently The World Bank's Identity for Development database.<sup>5</sup> The World Bank has estimated that, globally, about 1.1 billion people lack an official identity and are not registered in a national ID system.



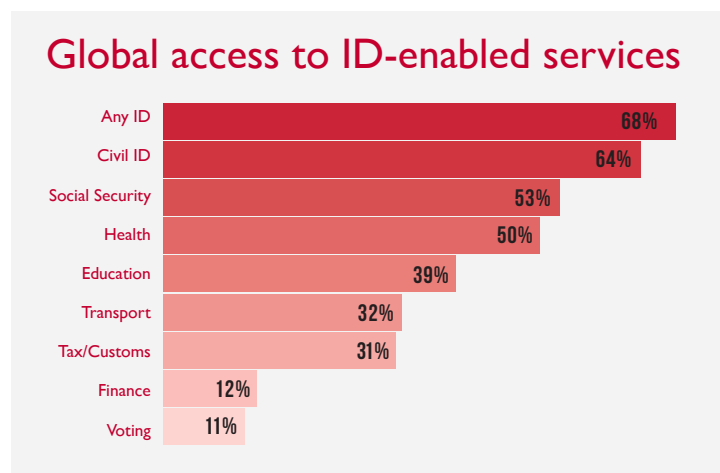
**Figure 1:** Fraction of population not included in national ID systems, according to The World Bank's 2017 ID4D report. Coverage gaps are most acute in Africa and South Asia. Estimates are based on self-reported coverage rates of national ID systems and voter registration, and household-level surveys of birth registration rates.

<sup>5</sup>Although the dataset offers information only about national ID systems, it is global in scope. There is currently no comparable database that tracks enrollment in other ID systems that may exist in country yet are not the official "national" ID. <https://data.worldbank.org/data-catalog/id4d-dataset>

While estimated rates of official identification are generally high in the Global North and in Latin America, identification gaps in Africa and South Asia are acute. An estimated 502 million people lack official identification in sub-Saharan Africa, with another 357 million in South Asia.<sup>6</sup>

The World Bank estimate suggests that roughly 1 in 6 humans lack official identification. But it is possible that


many more people—poor, rural, indigenous, female, refugee, immigrant, or marginalized populations—could be described as “under-identified.” These are people who have been enrolled in a government ID system at some point in their lives, but whose identity credentials may not empower them to exercise their rights, receive government services, or participate fully in the modern economy.



**Figure 2:** Fraction of the global population with access to ID-based services, according to the World Bank ID4D report. Globally, about 1.1 billion people are excluded from national ID systems. Among those who are included, the services linked to national IDs vary widely, with high-value services (such as voting and finance) often disconnected from the ID system.

Development requires not merely improving coverage of official ID systems, but improving adoption and effective use of the services that rely on official ID. The World Bank study estimates that although 68 percent of the world’s population is included in a national ID system<sup>7</sup>, these systems vary widely in the services they offer. Roughly three-quarters of the world’s ID holders have an ID that links to their health care system, while under half

are connected to tax payment systems. Only about 11 percent of people have a national ID that enables voting. In cases where national IDs are not linked to voting (including the Social Security Card in the United States) voter registration is handled by a separate system. This highlights the distinction between having a national ID that serves only as identity and a national ID that serves a functional purpose.



**India’s Aadhaar system is one of the most widely discussed ID systems in the developing world today, and this report will frequently cite it as an example of both opportunities and risks. Under the Aadhaar system, each registered individual is assigned a unique 12-digit number linked to basic demographic information and biometrics, including 10 fingerprints and iris scans. Individual identity can be authenticated by either the Aadhaar number, biometric authentication, or a one-time code sent to the registered mobile number.**

**Initially supported to establish a unique ID code for families receiving welfare services, Aadhaar is now fulfilling a mandate to identify each resident of India. Importantly, Aadhaar’s approach to inclusion is focused on residency rather than citizenship. This has allowed the Indian government to rapidly enroll a large population without becoming bogged down in determining legal citizenship for each Aadhaar enrollee. Some ID-linked services (such as voting) require more formal proof of citizenship which must be linked to the ID after enrollment.**

<sup>6</sup>These numbers depend on two key assumptions. In countries without data on national ID systems, children under the age of 15 were counted if they were included in a birth registry. Adults in these countries were presumed identified if had they registered to vote in a recent election.

<sup>7</sup>Excluding birth registries, and drawn from 2016 data.

## Digital ID Systems: How They Work

### The digital ID value chain

We describe the function of digital ID systems in terms of a “DID value chain,” which comprises three distinct phases: enrollment, authentication, and authorization. Each phase is described below and will be further explored in the value chain figures that appear throughout the report.

#### Enrollment

Enrollment typically includes several processes:

*Identity Proofing* is the process of linking records in a database to a real-world person. This requires matching the record with individual attributes that are sufficiently unique and stable to ensure that the match remains valid over time. Each system will also have a set of requirements regarding what information is required to prove one's identity. Many systems rely on “breeder documents” such as birth certificates and build upon birth registries or similar population databases. When these do not exist, a trusted person can sometimes stand in for formal papers<sup>8</sup>.

*De-duplication* ensures the uniqueness of each identity in the system. Enough must be known about each enrollee to ensure that this person is different from every other individual enrolled. This requires collecting several pieces of information, for example, name, birthdate, and mother's name. Biometrics can provide additional uniqueness in combination with biographical data, but biometrics alone cannot uniquely identify one person among hundreds of millions.

*Credential Issuing* gives new ID holders a token (e.g., a card or a unique number) with which they can assert their identity. This completes the exchange occurring between an individual and the ID-providing institution at enrollment. Individuals entrust the institution with their personal data. In return, they are given a credential that shows they have been counted by the institution.

*Accretionary ID* models allow undocumented users to establish an initial ID with little or no supporting information; supporting attestations are instead added over time. Such IDs would start with relatively little confidence that one is who they say they are—insufficient for banking KYC requirements, for example—but become more trustworthy with the addition of more information. Enrollment becomes a process of identity accretion, rather than a one-time event. At present, accretionary ID technologies are mostly in the pilot phase.

#### Authentication

Once an individual is enrolled, she can assert an ID to access a service or to transact. After she presents ID credentials, an authenticator queries the ID database to confirm that her assertion matches the information linked to the credential at enrollment. In secure authentication, two tokens are used together—one public and one private. Public tokens are analogous to a username; they can be shared with everyone. Private tokens are like a password and are used to prove legitimate ownership of a public token.

Authentication typically involves some combination of three types of credentials:

- Something you have – e.g., an ID card or registered SIM card
- Something you know – e.g., a PIN or password
- Something you are – biometrics such as face, fingerprints, or iris

The use of data during authentication differs from enrollment. When enrolling new users, each entry must be compared against the entire database to check for duplicates. When authenticating, it is only necessary to check whether a given set of credentials exists in the database. As a result, authentication typically requires less information than enrollment.

<sup>8</sup> For example, India's Aadhaar system allows an “introducer” to vouch for the identity of undocumented people. See Nyst et al. (2016): “[Digital Identity: Issue Analysis](#).” Consult Hyperion PRJ.1578.



Enrollment databases need to be centralized, because all records must be compared during deduplication. Authentication databases are not limited in this way. In “match-on-card” schemes<sup>9</sup> a user’s private tokens are stored only on a smart card, never in a central database. The ID holder is confirmed as the legitimate holder of the public credential (the smart card) if she can present a fingerprint or PIN matching the one stored on the card. This means that sensitive private tokens are never sent over a network, relaxing the need for reliable connectivity (a useful feature in many developing countries). There is also no central database that could be vulnerable to a large data breach. The “database” is distributed across many smart cards, and any attacker could steal only one set of credentials at a time.

Even when the enrollment process is digital, authentication often is not. Instead of expensive biometric or smart card readers, point-of-service authentication may be nothing more than visual inspection of a photo ID.

### Authorization

Once an ID system has confirmed that the set of tokens presented matches a known person in the database, service providers determine which services the authenticated user is authorized to access (e.g., withdrawing cash or voting).

Authorization decisions are separate from the authentication of credentials. In some cases, a service provider will have a “whitelist” of authorized individuals and will check whether an authenticated ID holder is on the list. An authorization database matches public tokens to information about which services each user may access. Even when both databases are stored together, the process of authentication and authorization are distinct. In other cases, authorizers compare ID-linked information against an authorization policy, for example checking to see whether an ID holder is over 18 or is a local resident.



Photo: Athit Perawongmetha / World Bank

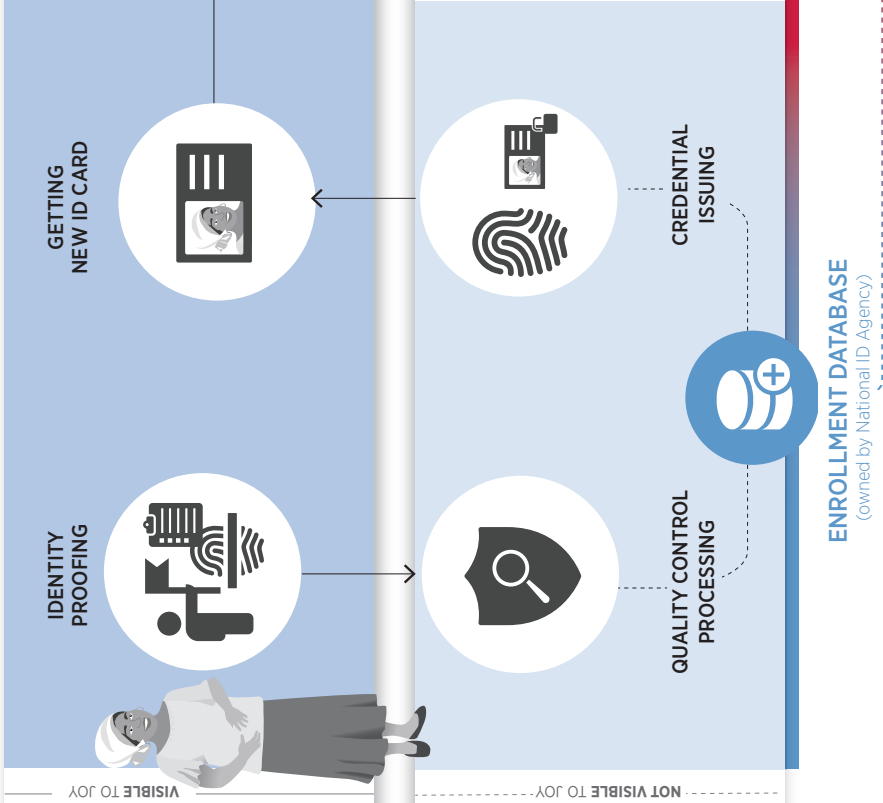
<sup>9</sup> Bergman, Christer (2008). “Match-on-Card for Secure and Scalable Biometric Authentication” in Rath & Govindaraju (eds.), [Advances in Biometrics: Sensors, Algorithms, and Systems](#), pg. 407-421.

## Basic Digital ID Value Chain

Joy is a farmer who wants to get a small loan to get her through to the next harvest. She doesn't have a birth certificate or any formal identity documents. She went to a bank to ask whether she might still be able to open an account and apply for a loan, but they told her that they can't legally give accounts to people without an ID. Fortunately, her country recently launched an enrollment campaign for their new national ID card.

### ENROLLMENT

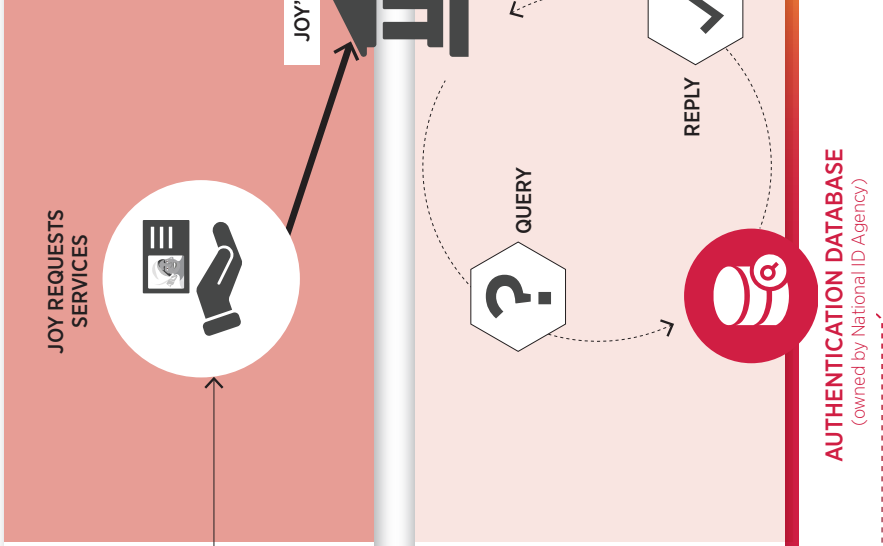
WHO IS JOY, AND HAVE WE SEEN HER BEFORE?



Joy goes to an enrollment center, where she is fingerprinted and has to fill out a lot of forms with biographical information. Because she doesn't have any ID documents, Joy has to get a village leader to vouch for her identity as Joy. The information she shares is passed back to the National Identification Agency, where they check to make sure that forms were filled out correctly and that someone with her information isn't already present in their enrollment database. After this initial check is completed, her information is stored in the National Identification Agency's enrollment database. She returns to the enrollment center to pick up her new ID card.

### AUTHENTICATION

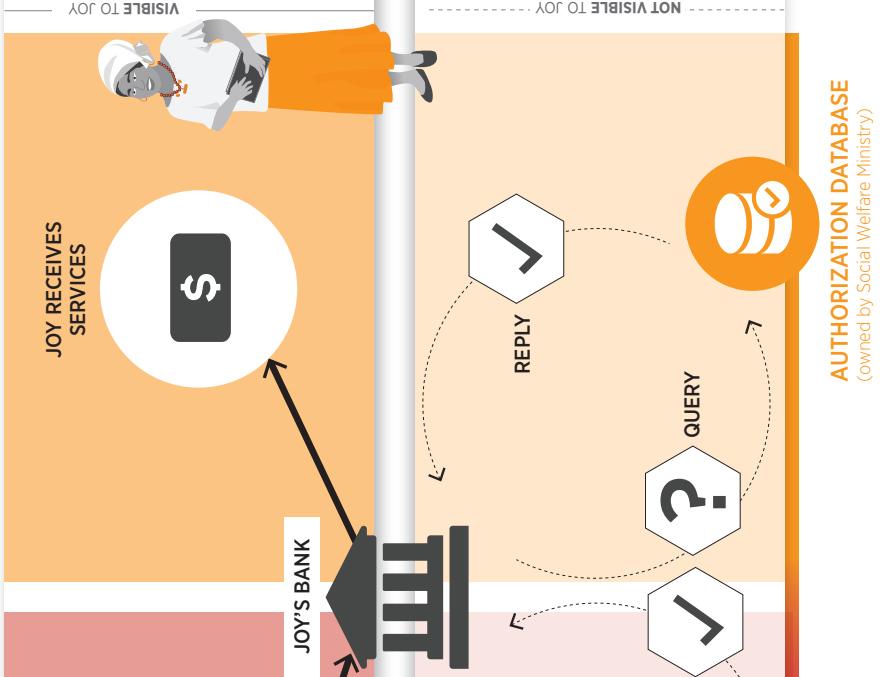
DO JOY'S CREDENTIALS MATCH WHAT WAS ISSUED?



Next, Joy goes to the bank to begin her loan application process. They ask her to show her national ID card and to place her right index finger on an electronic scanner. The bank sends her ID number and a digitized version of her fingerprint to the National Identification Agency's authentication database. This authentication database contains only the information needed to confirm her identity (ID number and one fingerprint). The agency responds that Joy's credentials match and her ID is valid.

### AUTHORIZATION

CAN JOY ACCESS SERVICES?



The loan officer then queries a database from the Social Welfare Ministry to ask whether Joy is eligible for a small business loan. The Ministry doesn't have a copy of Joy's fingerprint templates; they only know her ID number and her loan eligibility. After an affirmative response, Joy signs a loan agreement and gets the money she needs.

ID system categorization
Functional and foundational

We distinguish in this report between “functional” and “foundational” DID systems.

Functional systems generate identities to serve a specific function. Functional systems support the delivery or authorization of a specific service, and may or may not be linked to ID systems that support other functions. Functional systems often aim to cover only some subset of the total population in a country; any given person may have a variety of functional IDs (e.g., driver’s license, health insurance card, voter registration card).

Foundational systems, in contrast, are intended primarily to provide identity as a public good, not to supply a specific service. Foundational systems are typically owned and operated by government institutions, aim for national coverage of their population, and provide credentials that function as an official ID. Foundational ID systems can also underlie multiple functional purposes.

In countries with limited or no foundational systems, functional IDs may evolve to take on a more foundational role. The usage of functional IDs may simply grow to meet a demand for a more foundational system, like state

driver’s licenses in the United States. While they are not required by law, in practice driver’s licenses are used as ID in several contexts unrelated to driving. Functional IDs may also be the only realistic ID option available to some people—for example cross-border populations and refugees—who live on the margins of formal identity systems.

Instrumental and infrastructural

USAID typically makes investments that support functional ID systems. But the distinction between functional and foundational systems does not fully capture the importance of how systems are designed. We further distinguish between “instrumental” and “infrastructural” approaches. The treatment of a DID system as an instrument with which to achieve an objective—an instrumental investment—results in isolated, single-application ID systems. Infrastructural systems, on the other hand, can be repurposed for similar projects and are compatible with existing local systems. In general, they contribute to a more cohesive and sustainable ID ecosystem by creating pathways between the multiple ID systems that exist in a given context. Instrumental and infrastructural approaches should be seen as a spectrum; many digital ID systems have some elements of both approaches.

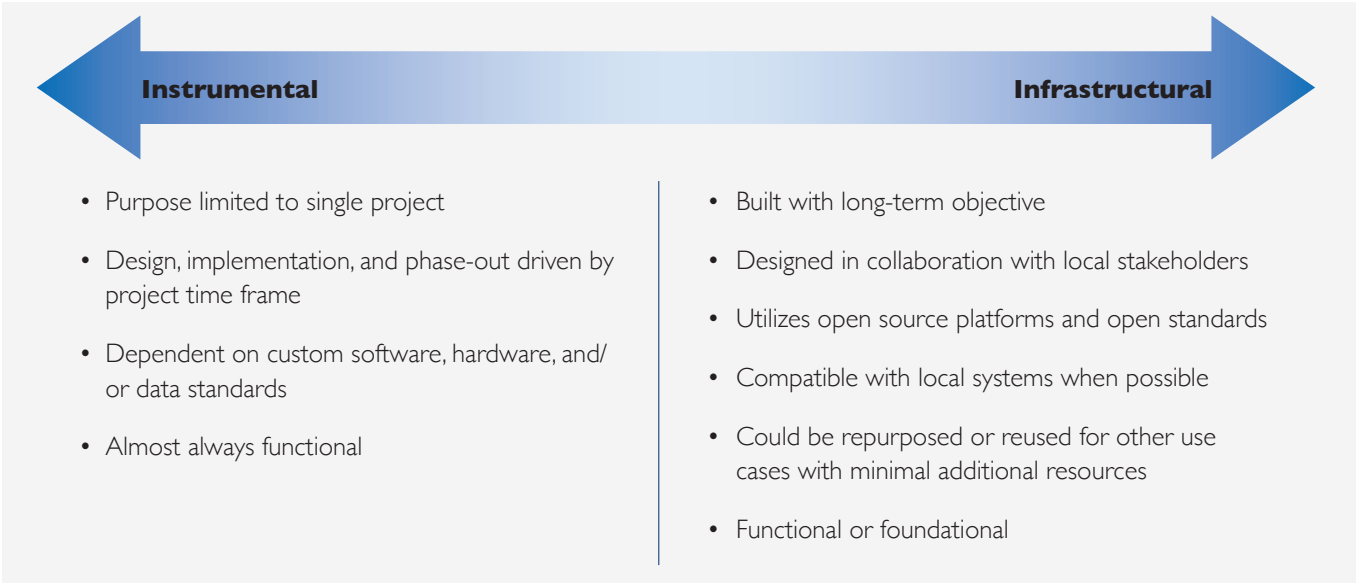
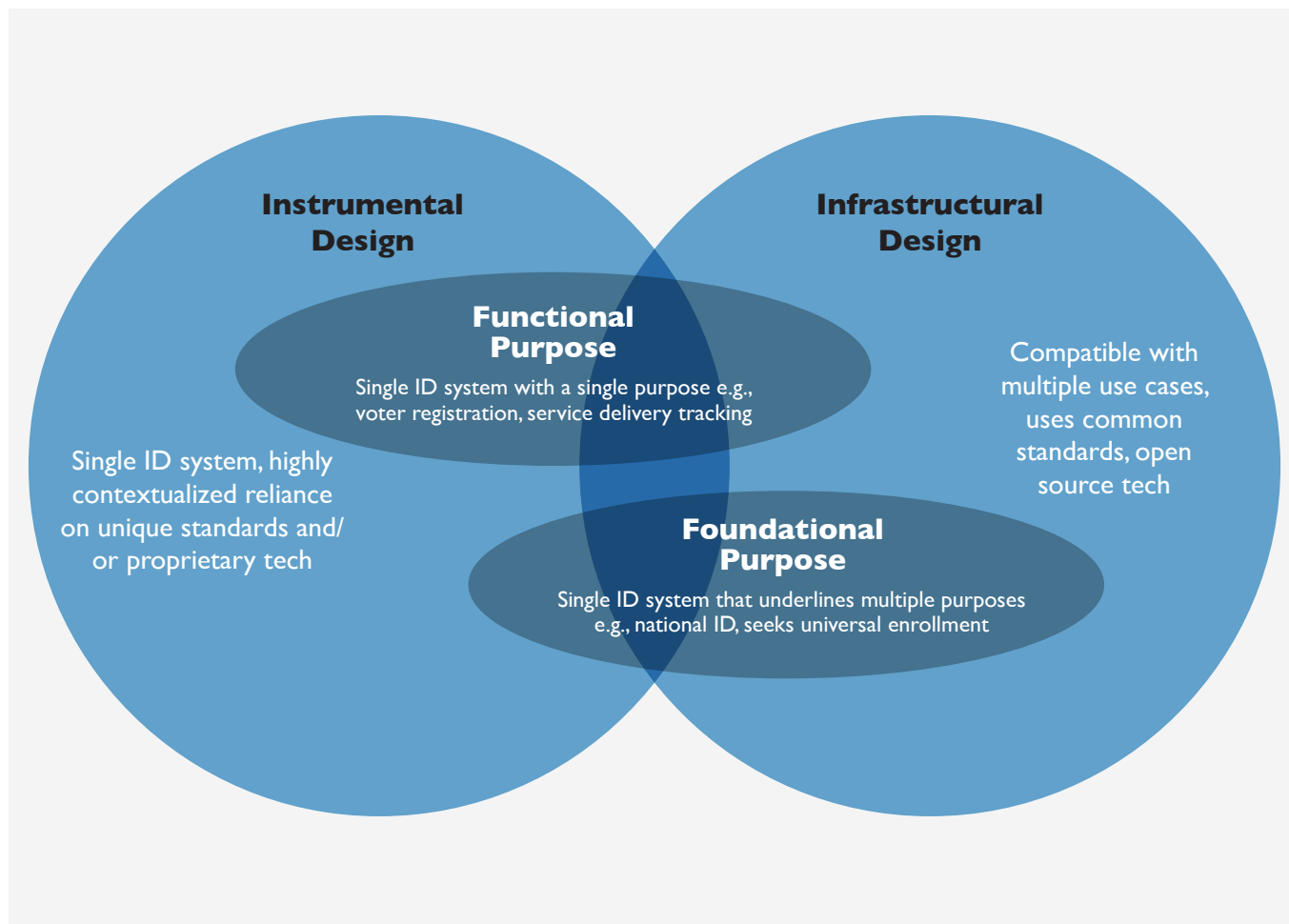


Figure 4: Investments in ID systems tend to fall along a spectrum ranging from “instrumental” on one end (looking at ID systems as an instrument or tool with which to achieve a functional objective) to “infrastructural” on the other (recognizing the importance of contributing to longer-lasting or re-purposable systems with each investment). Most ID investments will combine some elements of both approaches.

Together, the distinction between foundational and functional, and instrumental and infrastructural enable us to more accurately characterize systems. Although USAID and other donors more often invest in functional systems that tend to be instrumental in design, it is possible for functional ID systems to reflect an infrastructural design. Likewise, though foundational systems tend to be infrastructural, instrumental design choices can render them functional in practice. For example, the first national

ID system pursued by Nigeria's Department of National Civil Registration relied on private vendors, was shelved after a few years, and could not be reused when renewed efforts at harmonizing ID systems began years later.<sup>10</sup> Thus, while there is a correlation between systems with a functional purpose and instrumental design and between systems with a foundational purpose and infrastructural design, they are not equivalent (Figure 5).



**Figure 5:** ID systems can be characterized by their purpose and design. Systems with a functional purpose tend to be more instrumental in design, and systems with a foundational purpose tend to be more infrastructural in design. This is, however, not always the case. This diagram shows that both systems with a functional purpose and systems with a foundational purpose can incorporate a variety of design features spanning instrumental to infrastructural elements.

<sup>10</sup>The World Bank Group (2015). "[Identification for Development Identification Systems Analysis Country Assessment: Nigeria](http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-WP-P156810-PUBLIC-1618628-Nigeria-ID4D-Web.pdf)." Available at: <http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-WP-P156810-PUBLIC-1618628-Nigeria-ID4D-Web.pdf>





# 1



## PART 1: From Digital ID to Digital Infrastructure

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. The actors who fund and design an ID system tend to do so within the context of a particular project, in a way that is tailored to a specific problem and its unique environment. This approach is a natural result of how donors do business: investments are directed toward achieving program objectives.

By treating DID as a means to an end rather than as a contributing component of a complex system, the instrumental approach results in a fragmented DID landscape.

Indeed, DIDs *should* be used to enhance the efficiency and effectiveness of specific development projects. At the same time, this project-oriented perspective can overlook opportunities to increase efficiency more broadly, across programs and development objectives. An instrumental approach can lead to larger scale waste and significant opportunity cost.

An indication of the scope of opportunity cost from narrowly focused DID investments comes from biometric voter registration (BVR). 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<sup>11</sup> 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. As a contrasting example, South Africa uses a continuous voter roll with maintenance costs of about \$1 per voter for each election cycle. Generalizing from the 12 BVR projects considered, this would mean that instead of spending \$23 million on a BVR system that works only for a single election, it would cost \$7.5 million per election cycle to maintain a continuous system. Although

this ratio may not generalize to other types of ID systems, rushed deployment of a single-use ID system can incur as much as triple the cost relative to a more sustainable approach.

This instrumental approach is not only inefficient, it often ignores social, political, legal, and economic context that can be essential for program success. For example, if a voter ID presents information about the cardholder's ethnicity or religion in a controversial way, antipathy for the ID card could actually *suppress* voting among offended groups. Failure to balance political and social dynamics of ID systems can thwart the initial program goals and may negatively affect the broader system.

By treating DID as a means to an end rather than as a contributing component of a complex system, the instrumental approach results in a fragmented DID landscape. Single-use BVR systems are a classic 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, investments are wastefully repeated, and data cannot be shared because of inconsistent standards. In the long run, this increases costs, overburdens users, and can exacerbate the systemic problems donors hope to solve.

<sup>11</sup> Gelb & Diofasi (2016). "[Biometric elections in poor countries: Wasteful or a worthwhile investment?](#)" Center for Global Development Working Paper 435.



**Much like roads, bridges, or fiberoptic connections, infrastructural ID systems outlive the projects they were designed to support.**

In contrast, an infrastructural approach views ID systems as core infrastructure to support other systems and activities. Much like roads, bridges, or fiberoptic 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”. An infrastructural approach would replace repeated procurement of bespoke systems with investments that are locally driven, reusable, and optimized for sustainability. Such an approach would seek to avoid siloed systems. This can be done by encouraging stakeholders to converge around common platforms or by developing standards that facilitate reuse.

Infrastructural investment can take different forms. In the short term, urgent development needs may preclude waiting for a foundational ID system that is weak or absent. If a standalone ID system cannot be avoided, it should be built with an eye toward re-purposability in other projects and even potential “backward integration” into a future foundational system. A longer-term ID strategy would focus whenever possible on strengthening foundational ID systems and building project-specific applications on top of them.

The following sections will detail the existing digital ID landscape and the role that donors, including USAID, play in it, with particular attention to the causes and effects of a siloed, instrumental approach to ID programming and opportunities to move towards a more infrastructural approach.

## **Current Approaches to Digital ID Systems in Development**

Our research involved interviews with over 60 stakeholders, including donors, implementers, technology vendors, academics, start-ups, and government officials. To make sense of how the different pieces fit together, we relied extensively on the tools of systems maps and causal loop diagrams.<sup>12</sup> The sections below will gradually build up a map of a notional DID system, introducing each feedback loop with case studies drawn from development projects.

### **Digital identity: An instrumental approach**

Donor investments in digital ID are generally sector focused and project specific. For example, a health program might fund a DID system to better understand its target population. A democracy program might turn to DIDs to increase transparency in voting systems. This instrumental approach often stems from structural incentives (e.g., earmarked funding or contractual obligations), but there are contextual reasons as well.

First, the role that ID plays can differ significantly across sectors. In health, an ID might need only to identify someone as the same person over time—a pseudonym by which one could monitor consistent service delivery to that individual is sufficient. Such an ID might include a unique ID number but no information (such as name or photograph) that could be used to tie a lost or stolen ID back to its original owner. In elections, an ID actually does not need to record someone's identity; rather, it needs to distinguish an individual uniquely and prove one is a resident of a given age, and therefore eligible to cast a vote. Cash transfer programs may require much greater confidence in the accuracy of one's identity to comply with anti-money laundering/combating financing of terrorism (AML/CFT) standards. This typically means recording information such as the ID holder's name, birthdate, and address. Variation in the level of assurance

<sup>12</sup> Systems mapping can be contrasted with the linear “Logical Framework” approach that is common in development planning. Though a linear approach emphasizes how interventions contribute to a higher level goal, a systems view stresses feedback loops that can cause a system to grow, wither, or reach an equilibrium.

(LOA<sup>13</sup>) required for identity authentication in different contexts means that ID systems will not necessarily be compatible across use cases.

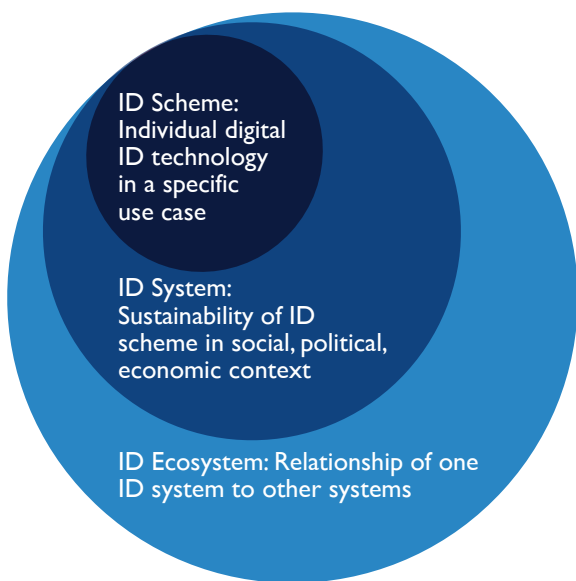
Second, USAID programs operate in contexts where the underlying ID infrastructure varies considerably, and existing systems can only be leveraged where they exist. Even then, concerns about the system's inclusiveness, its privacy and data security protections, and how it is perceived by prospective users may make it inappropriate for a given program, leading to investments in alternative ID systems.

Third, attempts to leverage an existing digital ID system require political navigation and consensus building. The immediate need to deliver on project objectives can discourage these time-intensive approaches.

Finally, technology vendors also push us toward instrumental investments. Their business models may favor bespoke systems that are difficult to reuse or repurpose; this is often a central component of how they make profit. The commercial interests of private sector digital identity systems, coupled with a strong pitch and the appeal of

technology solutions, can create substantial pressure for governments to make investments in systems that are ultimately unsustainable.

In this section, we consider several sector-specific USAID case studies that allow us to explore why and how donors end up with instrumental approaches. For this analysis, we distinguish between digital ID schemes, ID systems, and ID ecosystems. We use the term *DID scheme* to refer to a specific ID technology used in given program. *DID system* refers to the DID scheme in the context of the social and political dynamics that shape its use. *DID ecosystem* refers to the broader environment of a particular country or region in which there may be multiple (functional or foundational) ID systems. We present the main drivers for investments in *DID schemes*. We then analyze how these drivers—often-cited priorities like efficiency, effectiveness, being data driven—lead to different design choices, different system dynamics, and ultimately different levels of ID system sustainability and integration within the ID ecosystem.



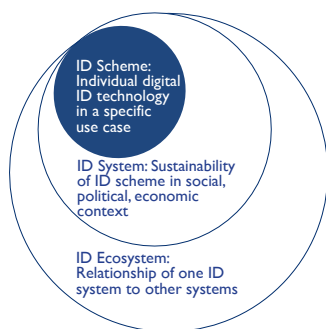
**Figure 6:** ID can be conceptualized in several layers. Individual ID schemes consist of a specific ID technology system. ID systems consider a particular ID scheme in the context of social and political dynamics in which it operates. ID ecosystems consider the relationship between multiple systems. Often ID actors fail to consider the layers of the ID ecosystem outside of their own sphere, and restrict themselves to operating at one level of the ID ecosystem rather than taking a holistic approach.

This gradual expansion of focus reflects the layered relationship of ID schemes, systems, and ecosystems (Figure 6). In the sections below, we use the nested circle diagram to designate the layer of focus for the section.

<sup>13</sup>LOA refers to the degree of confidence that the ID was correctly assigned (at enrollment), as well as the confidence that the individual asserting an ID credential is indeed the person they claim to be (at the point of authentication). McCallister & Brackney (2011). "Text for ITU-T Recommendation X.1254 | ISO/IEC DIS 29115 – Information technology – Security techniques – Entity authentication assurance framework."

## How DID schemes contribute to functional goals

### Inclusion of a target population



In the context of ID schemes, *inclusion* is the degree to which a target population is covered. Generally this refers to the initial entry of an individual's identifying information in the ID scheme, or the enrollment stage.

It can be challenging to enroll everyone. People live in geographically remote areas. Others are marginalized within society. Pakistan's national ID system, NADRA, has deployed mobile enrollment teams and women-only registration centers to include hard-to-reach populations. Although this requires investing resources that might otherwise go toward efficiency gains, prioritizing inclusion can enable higher-order objectives like strengthening democracy or improving government service delivery.

Inclusion can also be the primary goal of an ID intervention. For example, a political push to prioritize inclusion was provided in the United States by the Girls Count Act.<sup>14</sup> This legislation seeks to ensure that all children, including girls, around the world are included in birth registries or recognized by some form of "official documentation." This raises the profile of the need for systems to simply document or enumerate a population, in this case to better inform at an aggregate level the needs for foreign assistance and social welfare programs targeting this demographic.

More often, however, inclusion is the first in a set of more specific goals. The following sections will detail the interplay of these different goals to highlight key features of DID systems and their social context. In each case, inclusion in the ID system makes more data available. These data facilitate various institutional process improvements, such as data-driven decision making, increased efficiency, or greater transparency and accountability. These process improvements, in turn, enable the ID system to contribute to functional goals.



Photo: Bobby Neptune/USAID

<sup>14</sup> United Nations Foundation (2015). "Girls Count Act Bill Brief." [GirlUp.org](http://GirlUp.org).

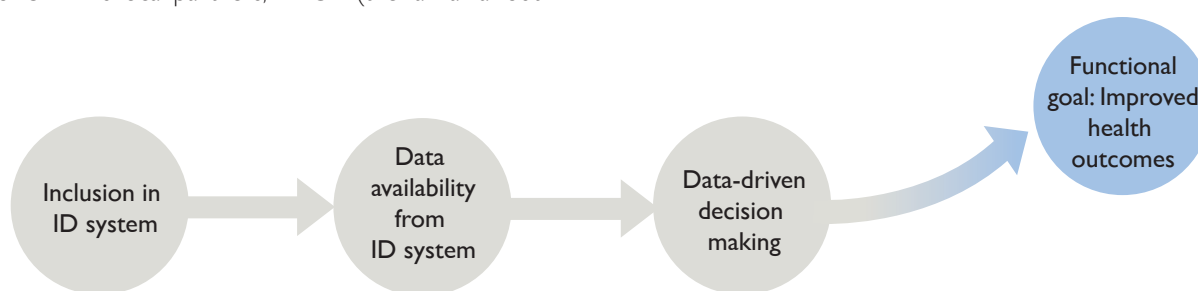


## Data-Driven Decision Making

Digital ID schemes are essentially information systems about people. The data from these schemes can inform the design and delivery of programs to better address the needs of the populations they serve. For example, the Global Health Bureau supports PEPFAR's \$385 million partnership, the DREAMS Initiative,<sup>15</sup> to reduce HIV infection among adolescent girls and young women in southern and eastern Africa. In Tanzania, DREAMS needed a comprehensive ID system to track the enrollment of adolescent girls and young women in the DREAMS program and monitor which services they received. One of USAID's local partners, TAYOA (the Tanzania Youth

Alliance), established a digital ID system to facilitate the tracking of layered service delivery across partners and trained other partners and service providers to use it.

In general, utilization data about who is accessing services can help identify who may need additional outreach, which services are valued, and where services might be combined for greater efficiency. The goal for this system is to enable partners to use these data to improve programming and service delivery efforts.



**Figure 7:** Health actors may create a digital ID system because they seek improved health outcomes. They rely on broad inclusion of targeted individuals in the system, which leads to increased data availability about populations of interest. This data can then support more informed decision making about how to serve population-specific needs, leading to improved programming to help achieve targeted health goals. In reality, improved outcomes will depend on many factors outside the ID system; this simplistic causal linkage reflects design aspirations and motivations.

## Institutional efficiency

Digital ID schemes can also help make institutions more efficient by driving down costs and reducing time spent on paper-based registration or authentication. Digital databases are easier to de-duplicate than their analog counterparts, which can help detect waste and fraud. This is a strong institutional motivator for digital ID schemes at both a programmatic and a national level. For example, Aadhaar's savings for the Indian government have been estimated at upward of \$1 billion per year.<sup>16</sup>

Digital IDs are frequently used in humanitarian aid projects to more efficiently manage benefit distribution.

Humanitarian DID systems typically enroll recipients in a database along with information about which benefits the person is eligible to receive. Enrollment can include biometrics such as fingerprints and iris scans (as in the World Food Programme's SCOPE card system<sup>17</sup> or UNHCR's Biometric Identity Management System<sup>18</sup>). In other cases, only a photograph is used (as in World Vision's Last Mile Mobile Solutions<sup>19</sup>). Beneficiaries are issued a credential that links them, and potentially other household members, to specific benefits.

These systems have quickly gained adoption for several reasons. They can improve the management of aid

<sup>15</sup> USAID (2017). "DREAMS: Partnership to Reduce HIV/AIDS in Adolescent Girls and Young Women."

<sup>16</sup> Aadhaar ID saving Indian govt about \$1 billion per annum: World Bank. Economic Times, Jan 14, 2016. This estimate has also been contested; see Clarke, Kieran (2016).

<sup>17</sup> More Ghost Savings: Understanding the fiscal impact of India's direct transfer program — Update. International Institute for Sustainable Development Policy Brief.

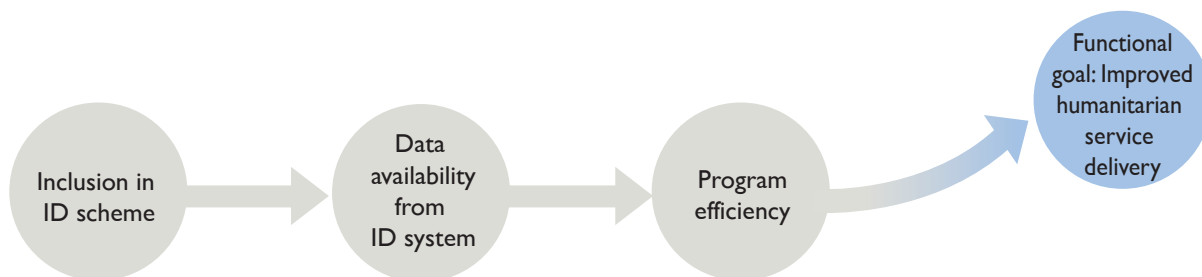
<sup>18</sup> World Food Programme (2015). "SCOPE in five minutes." Accessed May 2017.

<sup>19</sup> UNHCR (2015). "Biometric Identity Management System: Enhancing Registration and Data Management." DPSM Key Initiatives series. Accessed May 2017.

<sup>19</sup> World Vision International (2014). "Last Mile Mobile Solutions (LMMS)." Accessed May 2017.

distribution by decreasing duplication, reducing fraud, and simplifying monitoring and reporting processes. Estimates from World Vision's system suggests cost savings of 15 percent to 40 percent resulting from the deployment of their digital benefit distribution system.<sup>20</sup> Similarly, after the

introduction of fingerprint verification in a Kenyan refugee camp, WFP reported a monthly savings of \$1.5 million and a 20 percent reduction in the number of refugees within 6 months.<sup>21</sup>



**Figure 8:** Humanitarian organizations often create ID systems because they want to reduce waste and fraud and more reliably reach those entitled to receive benefits. Similar to previous examples, effectively including individuals can generate the data necessary for better supply tracking, fraud detection, and resource targeting. The inherent assumption is that improving these processes will lead to better humanitarian service delivery. In practice, outcomes will of course depend on many factors other than the ID system; improvement in terms of cost reduction may not ultimately improve the experience of aid recipients.

Some humanitarian DID schemes allow individuals to use digital authentication to purchase from local markets. These have been promoted for giving refugees and disaster victims greater flexibility and choice in how they receive their benefits. For example, UNHCR's use of an iris-scanning ATM system to distribute cash aid to refugees in Jordan allowed individuals to access benefits from ATMs just like anyone else in their community, offering a more integrated experience for refugees and greater efficiencies for the aid institution.<sup>22</sup> This approach helps avoid stigma by offering an alternative to standing in lines that clearly identify people as aid recipients.

Institutions clearly benefit, but individuals' experiences may differ. In Jordan, iris scanning worked because it integrated well with cultural practices (there, ATMs often use iris scanning technology for identification). In other contexts, introducing iris-scanning for refugees can

actually *further* stigmatize refugee populations if they are required to go through more biometric sharing than resident populations. Although individuals need aid, they may be less than comfortable interfacing with certain technologies or submitting biometric data to international organizations that they may not fully trust.<sup>23</sup> These dynamics are explored further below.

### Transparency and accountability

A digital ID scheme enrolls individuals and generates a digital "paper trail" of information linking people to transactions and to unique entries in digital databases. This "data exhaust" can offer transparency about registration for programs, distribution of resources, or delivery of services. This increased transparency may promote greater accountability, especially when data are easily accessible to multiple actors and thereby harder to obfuscate.

<sup>20</sup> Chibafa, Keith (2014). "Why not digital? Technology as an interagency tool in the Central African Republic." Humanitarian Exchange 62:19-21.

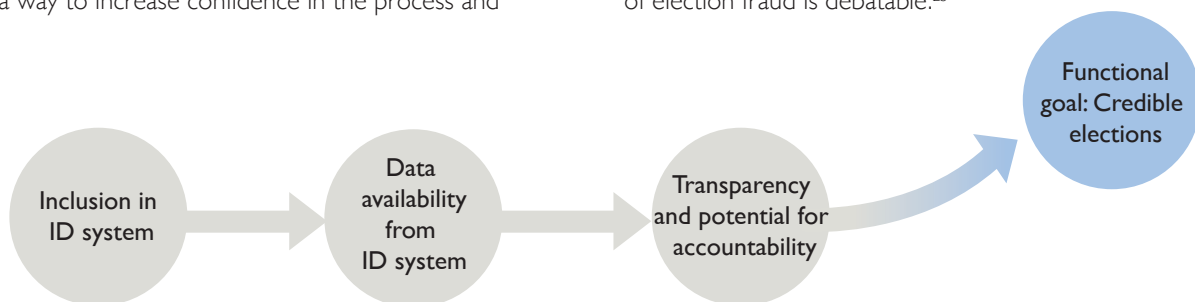
<sup>21</sup> World Food Programme (2016). "WFP and Digital Innovation."

<sup>22</sup> Guthrie, Craig (2016). "Iris solution helps refugees glimpse a brighter future." Planet Biometrics.

<sup>23</sup> Townzen, Rachel (2016). "Trusting Tech Initiatives Isn't Easy for Most Syrians." Pulitzer Center. Available at: <http://pulitzercenter.org/reporting/trusting-tech-initiatives-isnt-easy-most-syrians>.

Many projects aim to digitize voter records in developing democracies. USAID has supported a number of voter registration systems, whether directly or through general technical assistance to host-country governments. Many of these voting systems incorporate biometric technologies. Especially in unstable states, BVR is seen as a way to increase confidence in the process and

outcomes of elections.<sup>24</sup> This is an example of how DID data exhaust can offer transparency: data that are widely shared and difficult to obfuscate can help promote accountability and build trust. This increased confidence often results from implicit trust in the objectivity and neutrality of technology; the real impact on major sources of election fraud is debatable.<sup>25</sup>



**Figure 9:** In some cases, the desire for transparent and credible elections motivates the adoption of digital ID systems. Broad inclusion and resultant data availability are often seen to help create the potential for transparency and accountability and ultimately bolster public confidence in the election and its outcome. In reality, a credible electoral transition requires more than just technology; this diagram simply shows commonly observed motivations for investing in electoral ID systems.

## Consequences of Instrumental DID Schemes

### DID schemes create political dynamics

The direct relationships shown in the previous section rarely tell the entire story. When ID scheme design choices touch on sensitive political issues, broader political dynamics can be introduced. For example, the costs of deploying biometric identification kits, and training people to reliably operate them, are high. Because of this, governments or voting officials have traditionally opted not to use biometrics to authenticate voters at a polling site; instead they are most often used at the point of enrollment to de-duplicate voter rolls and ensure that each registered voter is a distinct individual. Although there are cases where de-duplication of voter registry is a critical problem, it does little to address what are often higher priority concerns of ballot stuffing, removing deceased persons from voter registries, and integrating voter registries with national ID systems.<sup>26</sup> Introducing

BVR can shift focus to registering individuals to the exclusion of other issues.<sup>27</sup> This is a calculation made to leverage the DID scheme to gain credibility, while not necessarily aligning the problem and solution in an optimal way.

Critically, when implemented with insufficient capacity or without regard to political perceptions, BVR can introduce tensions that may ultimately undermine the goal the ID scheme is meant to help achieve—here of more accountable and transparent elections.<sup>28</sup>

Afghanistan's e-Tazkera system<sup>29</sup> is an example of the types of political challenges that ID systems can face. Beginning around 2009, supporters hoped that a digital system would supply accurate population data and reliable voter rolls. Plans were made to introduce a smart card system with digital photos and fingerprints<sup>30</sup> stored on each card. In 2012, the government prioritized a rapid rollout prior to the 2014 elections. The accelerated

<sup>24</sup> Gelb & Diofasi (2016). "Biometric elections in poor countries: Wasteful or a worthwhile investment?" Center for Global Development Working Paper 435.

<sup>25</sup> Personal communication from internal elections expert.

<sup>26</sup> Mungai, Christine (2015). "Dirty hands: Why biometric voting fails in Africa -- and why it doesn't matter in the end." Mail & Guardian Africa.

<sup>27</sup> Personal communication with election expert from International Federation of Electoral Systems.

<sup>28</sup> Ensor, Charlie (2016). "Biometrics in aid and development: Game-changer or trouble-maker?" The Guardian Global Development Professionals Network.

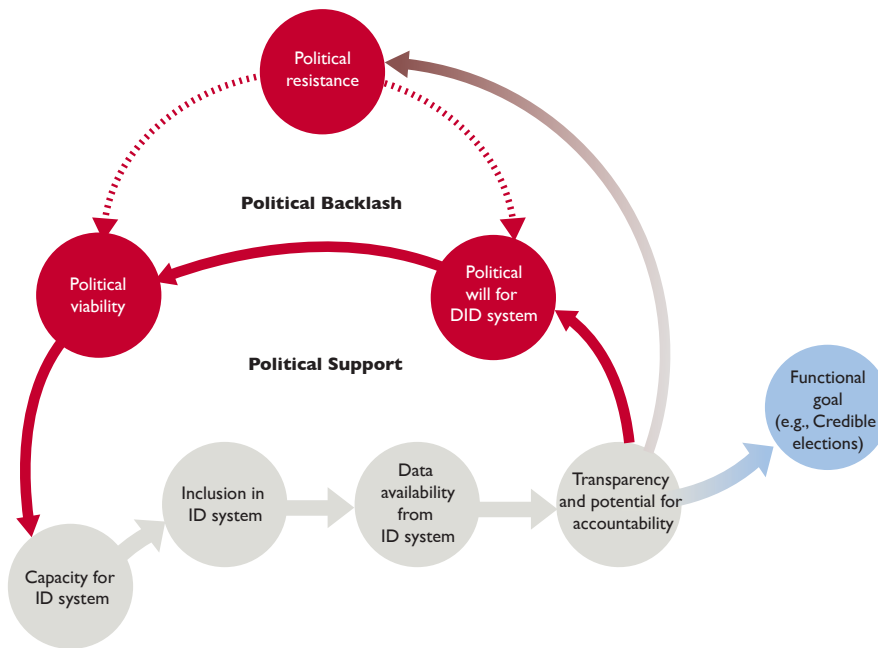
<sup>29</sup> Bjelica & van Bijlert (2016). "The Troubled History of the E-tazkera (Part 1): Political Upheaval." Afghanistan Analysts Network. Bjelica & van Bijlert (2016). "The Troubled History of the E-tazkera (Part 2): Technical Stumbling Blocks." Afghanistan Analysts Network.

<sup>30</sup> Institute for War and Peace Reporting (2015). "Afghans Impatient for New ID Cards".

timeline was unrealistic, in part because many basic issues, including the design of the ID card itself, had not yet been resolved.

Card distribution was already behind schedule when the card design became a focus of political controversy. The Afghan parliament was split between those who wanted the card to list all citizens as having an “Afghan” nationality, and those who favored a more detailed description

of the cardholder’s ethnicity or religion. Parliamentary debates were plagued by walkouts, shouting matches, and procedural irregularities. Eventually the public became involved, leading to protests and clashes with police, and by late 2013, the e-ID issue had become politically radioactive. The National Unity Government attempted to revive e-Tazkera in 2014, only to be met with new protests. At this point, the e-ID program seems to be indefinitely stalled.



**Figure 10:** Political support can add a positive feedback loop that strengthens the causal chain from Figure 10. Solid arrows denote positive relationships, in which two variables tend to increase or decrease together. When ID systems are seen as promoting good governance or reducing corruption, increased transparency can build political will, make the system more viable, and ensure continued financial support. Dashed arrows indicate a negative relationship, in which an increase in one variable leads to a decrease in another. For example, increased transparency can lead to political resistance, where some seek to undermine the system’s political viability, putting other system goals at risk.

If ID schemes are popular, however, they can increase the system’s political viability and may ultimately help secure additional capacity (e.g., resources, technical expertise, training) for the DID system. The Liberia Teacher Training Program (LTP) was a five-year (2010–2015) program<sup>31</sup> that used a biometric ID system to aid in personnel management. The biometric ID system was one part of a larger program that aimed to strengthen the teacher workforce, improve the monitoring and supervision of education quality, and use an information management system to inform policy and programmatic decisions.

<sup>31</sup> USAID (2011) “[Liberia Teacher Training Program: Five-year Work Plan](#).”

To aid transparency and build political capital, the Ministry of Education (MoE) first installed the biometric ID system at their headquarters before issuing to teachers. This actually revealed widespread corruption, leading to dismissal of top officials and elimination of scores of “ghost workers.” The process led to significant cost-savings and helped the MoE improve its public image. Shifting the focus to a biometric ID system for teachers and schools, LTP first had to separate bona fide teachers from ghost-teachers. After a school-by-school check of teacher credentials, the MoE eliminated around 10,000 ghost

teachers (28 percent of the total). This figure included about 1,000 ghost schools—non-existent schools that each employed about six fraudulent teachers at a total cost of around \$600,000 per month.

Given this environment of pervasive corruption, the reforms prompted fierce resistance from within. Although LTTP did have supporters in MoE, it was caught up in

inter-ministerial battles over ID and payment systems. More troublingly, some of LTTP's champions in MoE faced threats of violence, presumably from people whose illicit livelihoods were being endangered. In the end, despite a successful rollout in some areas of the country and substantial cost savings to MoE, the biometric ID system was not scaled further after donor support ended.



### Protecting privacy in ID systems

The centralization of personal data in DID databases can increase privacy threats. The mere existence of large troves of personal data creates the temptation to view those data as the property of the institution. This shift makes it easier to justify querying, exposing, or selling data without concern for individual ID holders. The tendency to “over-collect” information because it’s possible—or to look at it simply because it’s there—is a real concern.

To mitigate these risks, a digital ID scheme must ensure that personal information flows in ways that are context-relevant, what has been termed *contextual integrity*.<sup>32</sup> This means data are shared only when consistent with the initial purpose and/or context under which the individual consented to its use. For example, health data collected from a patient could be shared with doctors involved in her care, but not advertising firms or law enforcement.

Privacy can also be enhanced through the principle of data minimization. Only a confirmation of authorization needs to be transmitted from a database to the point of service. For example, if a citizen of a country wishes to receive social protection benefits and needs to provide identification to confirm she is eligible, a data-minimizing system would send a single bit confirming whether the eligibility requirement is met. In contrast, showing a physical ID card to a distribution manager could disclose additional information—about the user’s gender, home address, place of birth—that is not necessarily needed to confirm eligibility. This approach has also been referred to as “attribute-based credentialing,”<sup>33</sup> and is key to allowing users to control the sharing of their personal information.

Another aspect of data minimization is known as “conditional pseudonymity.” Even if an enrollment database links a set of ID credentials back to a person’s real-world identity, that link may not be relevant for authorization. For example, a clinic referral system may not need to know a patient’s true name, only that they are the same person who received the original referral and are authorized to receive services.

Digital systems allow easier restriction of viewing permissions; this makes attribute-based credentialing and conditional pseudonymity more feasible, which can place the user in greater control over her personal information. A mobile microlender<sup>34</sup> doesn’t need to know a customer’s real name, only how to find her in the event of default. A privacy-conscious borrower might use several different pseudonymous accounts for different loans. The connection between those “personas” and her real-world identity only becomes important if she misses payments. In those cases, pseudonymity becomes conditional; law enforcement or other authorities can access the enrollment database in order to unmask her real-world identity.

Although enrollment and authentication databases are often identical, some<sup>35</sup> have suggested that they should be kept separate for purposes of data security and privacy protection. In this setup, the latter would contain only data needed to respond to authentication queries, not the more detailed profiles needed for de-duplication.

<sup>32</sup> Nissenbaum, Helen (2004). “Privacy as Contextual Integrity.” *Washington Law Review* 79:119.

<sup>33</sup> Mas & Porteous (2015). “Minding the identity gaps.” *Innovations* 10:1-2, pg. 31–54.

<sup>34</sup> Musoni is a Kenya-based microfinance institution that uses entirely mobile-based transactions.

Vizcarra et al. (2017). “Mobile Financial Services in Microfinance Institutions: Musoni in Kenya.” International Finance Corporation.

<sup>35</sup> Nyst et al. (2016). “Digital Identity Issue Analysis.” Consult Hyperion PRJ.1578.



## DID schemes generate privacy and security concerns

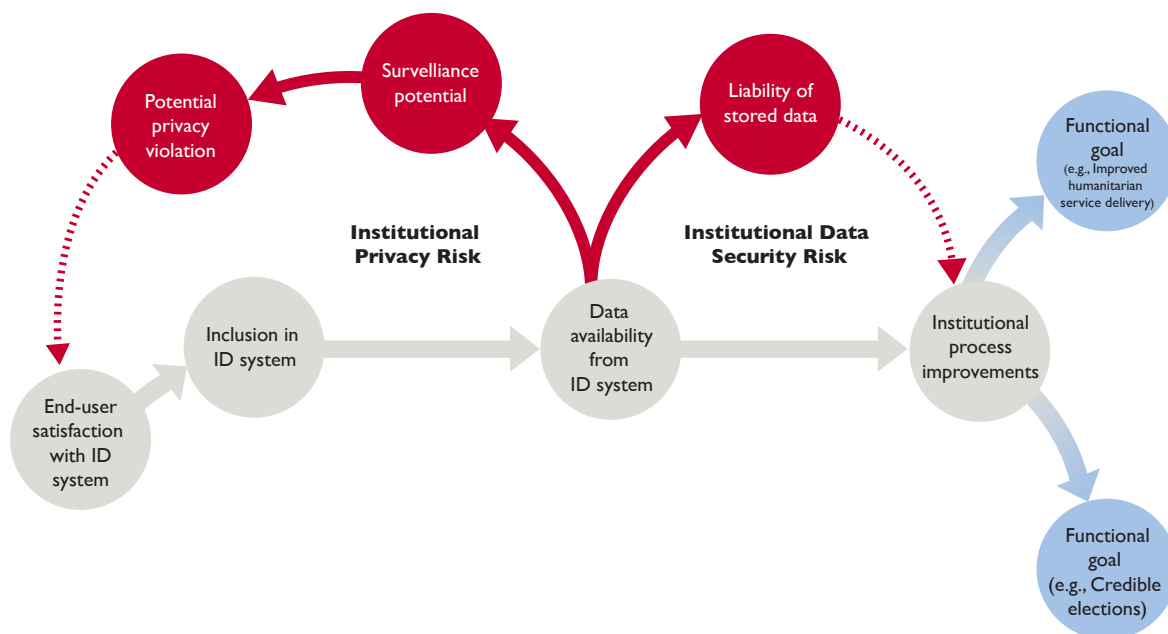
Centralization of personal data makes DID systems a target for malicious actors. Institutions end up bearing the risks of collecting and storing personally identifying information (PII). From an institutional perspective, stores of personal data can be a significant theft liability. The consolidation of information through digital systems amplifies this liability. Digitization can also increase security, however; implementing organizations working in a physically insecure environment may view the storage of information in a remote cloud as a security improvement over files stored on local computer hard drives.

Poor security practices can undermine system function in many ways. For example, some policies strongly penalize database owners for breaches of customer data. This can cause institutions to internalize this “data liability.” If their security measures are expensive or burdensome, this can erode institutional efficiency and effectiveness. One company piloting an electronic identity voucher program

shared an experience in which efforts to secure data led to storing encrypted files with such limited access that field workers could not access the database to continue enrollment.

A perceived privacy threat can also hamper system function. People can subvert an untrusted system by opting out or fabricating personal information. For example, USAID implementing partners who have developed a referral tracking system for HIV prevention said that absent trust between the field agent and enrollee, individuals provide inaccurate information, which can undermine the ability to accurately track referrals.

Privacy fears can also drive fragmentation of the ID ecosystem. If an existing system is broadly mistrusted, service providers (including USAID implementers) may choose to build their own system rather than incur reputational risk. ID providers will be unlikely to converge on a shared solution if customer security suffers as a result.



**Figure 11:** Here we see how a notional system is affected by privacy and security risks. An increase in *data availability* leads to an increase in *surveillance potential*. At the same time, *potential for privacy violation*—either real or perceived—will tend to decrease end-user satisfaction. This can translate to a reduced willingness to enroll or participate in a system, and undermine *inclusion*.<sup>36</sup>

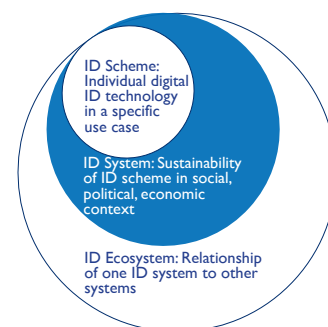
<sup>36</sup>Although limited data exist documenting how many individuals decide not to enroll in digital ID systems because of privacy concerns, we found ample anecdotal evidence to indicate it is a justifiable concern.

Individual privacy risk and institutional data security risk can create negative feedback loops. If not addressed, privacy dynamics can slow or even halt the ID scheme's ability to function, let alone deliver on the functional goal it was intended to support. A DID scheme must ensure that the integrity of personal information is protected, and that institutions storing and managing data can adequately secure the data from breaches and liabilities. The benefits to both institutions and individuals must outweigh the risk of contributing and securing personal data in a DID scheme.

The recent Indian Supreme Court ruling asserting Indians' constitutional right to privacy has underlined concerns about how the Aadhaar system collects and manages personal data. Although participation in Aadhaar is technically voluntary, Aadhaar IDs are required for key services like buying and selling property, setting up bank accounts, filing tax returns, and receiving welfare payments.<sup>38</sup> Critics of Aadhaar raise concerns over the security of the vast amount of data Aadhaar generates that could be potentially misused or tied to government surveillance.<sup>39</sup> A separate court is expected to consider the legality of the Aadhaar scheme in the coming months.<sup>40</sup>

## DID schemes miss opportunities for sustainability

BVR is a key example of how an instrumental approach to DID systems is particularly problematic for sustainability. Elections are recurrent events, and the intention of a BVR exercise is to create an accurate, inclusive, de-duplicated voter roll that can then be maintained going forward.



In Afghanistan cases, however, the registration exercises were time-bound and insulated. When voter registration drives are limited to establishing voter rolls for a single election, and voter databases are not maintained from one election to the next, we end up seeing duplicative or repeated investments, because many of the same voters must be re-registered at each election. This is currently the situation in Afghanistan, as parallel efforts exist between those working to roll out e-Tazkera and those driving for successful democratic elections. USAID is not alone in supporting single-use systems. Experience from the United Nations Development Programme similarly suggests that even when BVR kits are procured with the argument that they may support multiple election cycles, the vast majority of cases result in kits being improperly stored and maintained, and rarely, if ever, reused.<sup>41</sup>

Yet, continuing to funnel resources into technology that will become obsolete and focus only on short-term results creates a dependency on continued funding. Prioritizing the near-term goal of establishing a registry for an upcoming election misses opportunities to develop better integrated, sustainable systems.

<sup>37</sup> "Indian Supreme Court in landmark ruling on privacy."

<sup>38</sup> New York Times (2017). "Affirming Privacy, Rebuking India's Leaders."

<sup>39</sup> Agrawal, Ravi (2017). "India Supreme Court rules privacy a 'fundamental right' in landmark case." CNN.com

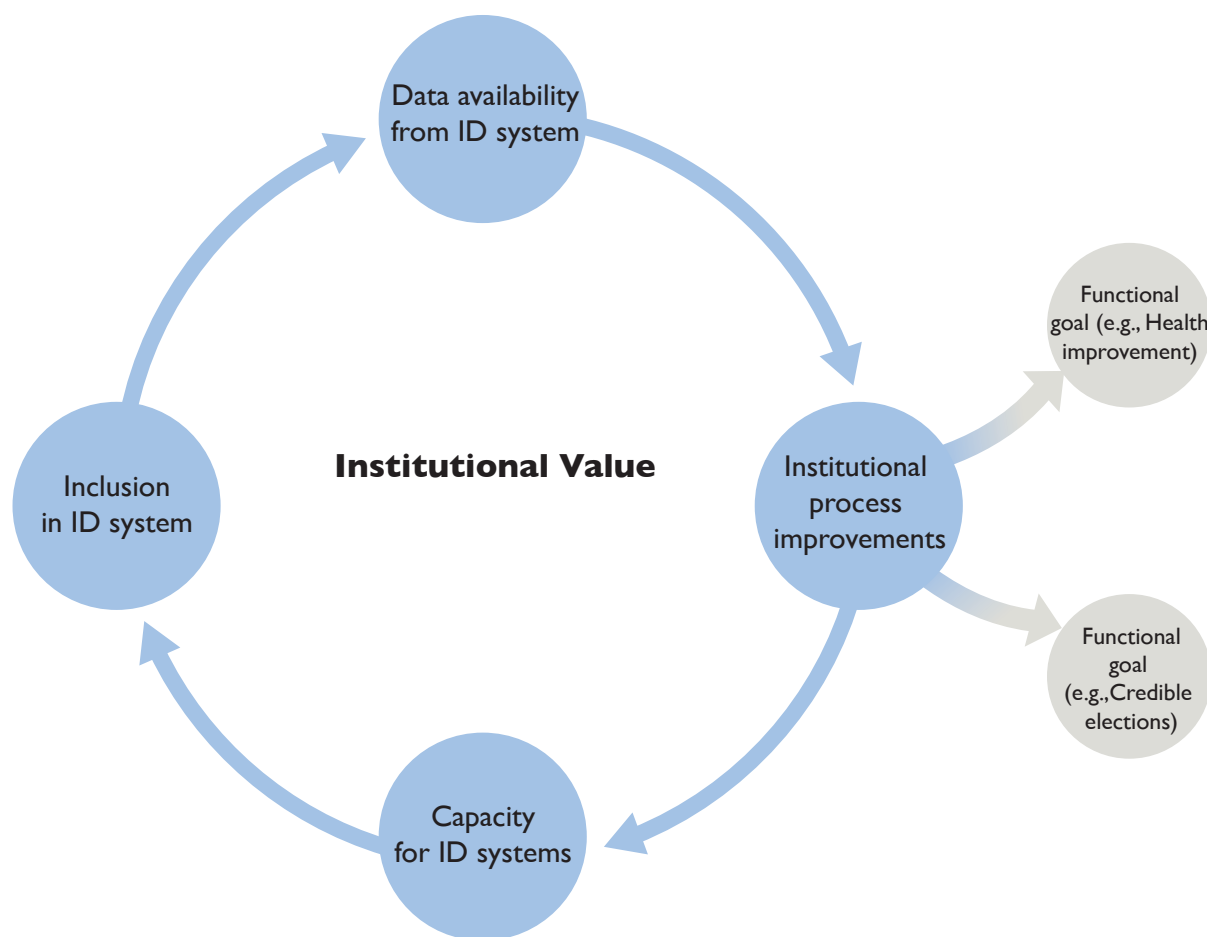
<sup>40</sup> The Wire (2017). "FAQ: What the Right to Privacy Judgment Means for Aadhaar and Mass Surveillance."

<sup>41</sup> McCann, N. (2017). "The evolution of identity management in Africa – What now for voter registration?" ID4Africa 2017 Conference Publication.

### Toward sustainability of DID schemes

Although donor funding of single-use DID systems is the norm, we have opportunities to drive toward more sustainable DID systems. First, when gains emerge through the use of the DID system—for instance, reductions in spending “leakage” that occur when a

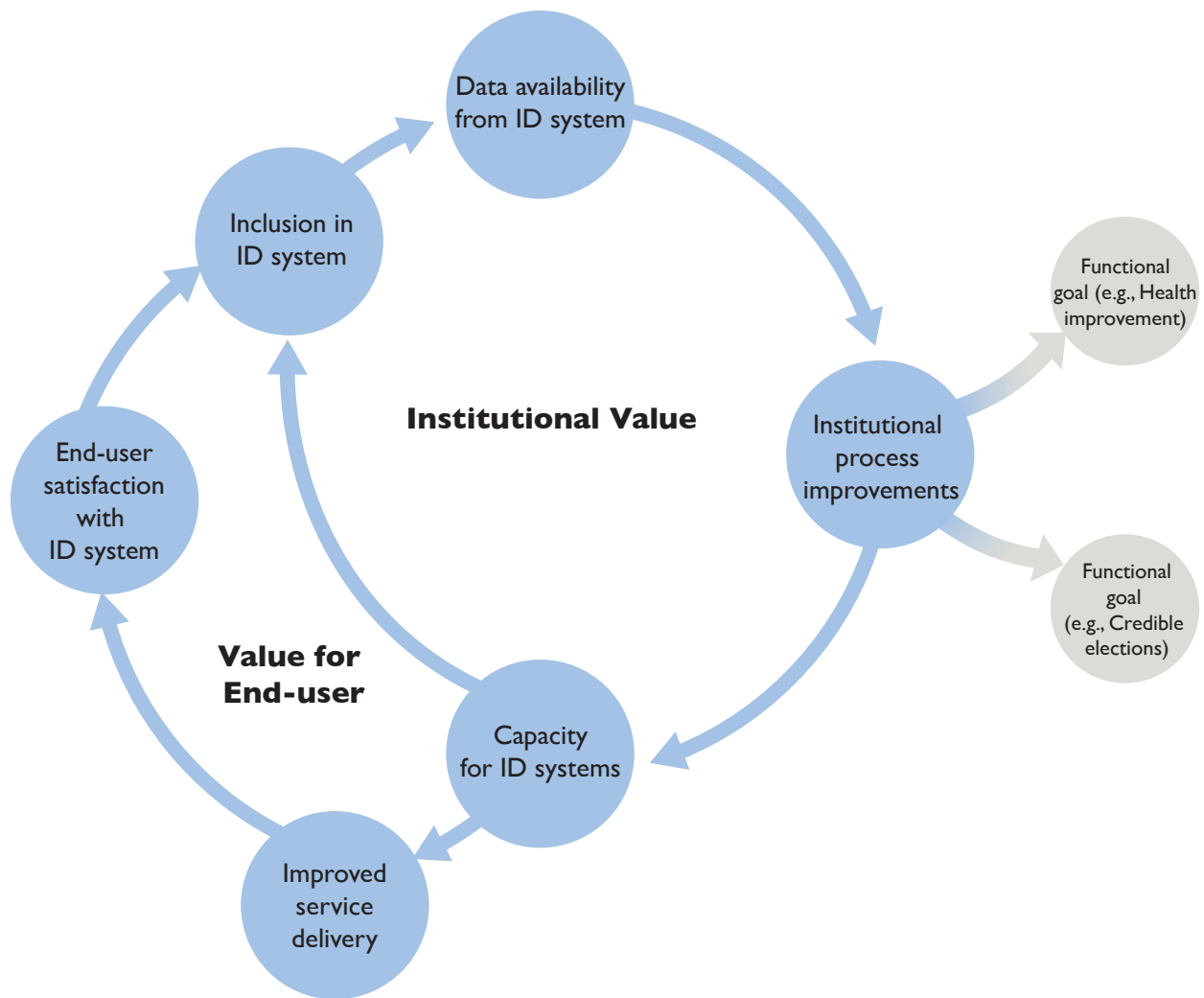
benefits distribution scheme is digitized—these gains can be reinvested in the DID system. This leads to a reinforcing loop whereby the DID system is sustained through its positive outputs. In Figure 12, we envision what this simple setup would look like:



**Figure 12:** Graduating from our original linear causal model (where we’ve simplistically assumed that resources in = benefits out), we now envision the positive-feedback system that begins to take shape when investments (*capacity*) are reinforced by cost savings from the DID scheme (*efficiency, effectiveness*). The closed loop in this figure illustrates the continued investment of resources and capacity to maintain a system over time. “Capacity” refers not only to funding, but also to staff, training, hardware, etc. Note that the sustained feedback loop of ID infrastructure supports functional goals (e.g., improved health, credible elections), but exists independent of sector-specific programs.

This model, of course, is overly simplistic. Even when a DID scheme leads to cost efficiencies, so that resources saved can be reinvested in the DID scheme to “close the loop”, this will ultimately taper off; no system can indefinitely sustain itself by reducing inefficiencies. To achieve a functioning feedback loop, sustainability

must account for the value that is derived by both the *institution* as well as the value derived by the *end users* of the system. Figure 13 represents both the core loop as well as a parallel loop demonstrating the user value being derived from improved user-facing DID-enabled services.



**Figure 13:** The ID value loop is strengthened by service delivery and increased end-user satisfaction. In many cases, ID system designers hope that cost savings can be reinvested in a sustainable system. A high-functioning system is expected to improve service delivery and build customer satisfaction. It is further assumed that satisfied customers will use the system more, further enhancing inclusion. All of these assumptions depend on conditions outside the ID system itself -- they are part of system designers' vision of success.

This loop shows the same four elements from the previous section, with the addition of a parallel branch representing the value derived by the system user. The satisfaction of end users reflects the “demand” side of ID systems. Individual users often need a reason to enroll in ID systems. After all, enrolling in an ID system often requires an investment of time, and requires trust in sharing personal information.<sup>42</sup> As ID systems are increasingly linked to a variety of services, their value increases; this in turn supports inclusion and continued participation in the ID system. Increased inclusion promotes data availability, and more data can help the system run more efficiently, which creates value for the institutions investing in the DID system.

Together the parallel elements of this core feedback loop support greater system growth initially, and greater sustainability over time. If a DID scheme can be constructed to meet not only the needs of an institution, but also to provide improvements in satisfaction of users, there can be more sustained growth of the DID system.

### Sustainability in practice

An initial investment to support the formation of a DID system will get it off the ground, but long-term viability requires more. Sustainable systems need a process for handling new enrollments, developing and maintaining systems for privacy and data protection, and linking systems to services or functions that give people reasons to use their ID. All of these require money.

Two primary funding streams generally enable ID systems to persist; either a funding body (like a government or donor) funnels resources in, or an alternative model for generating revenue is crafted by building value-added services into the “public good” ID system.

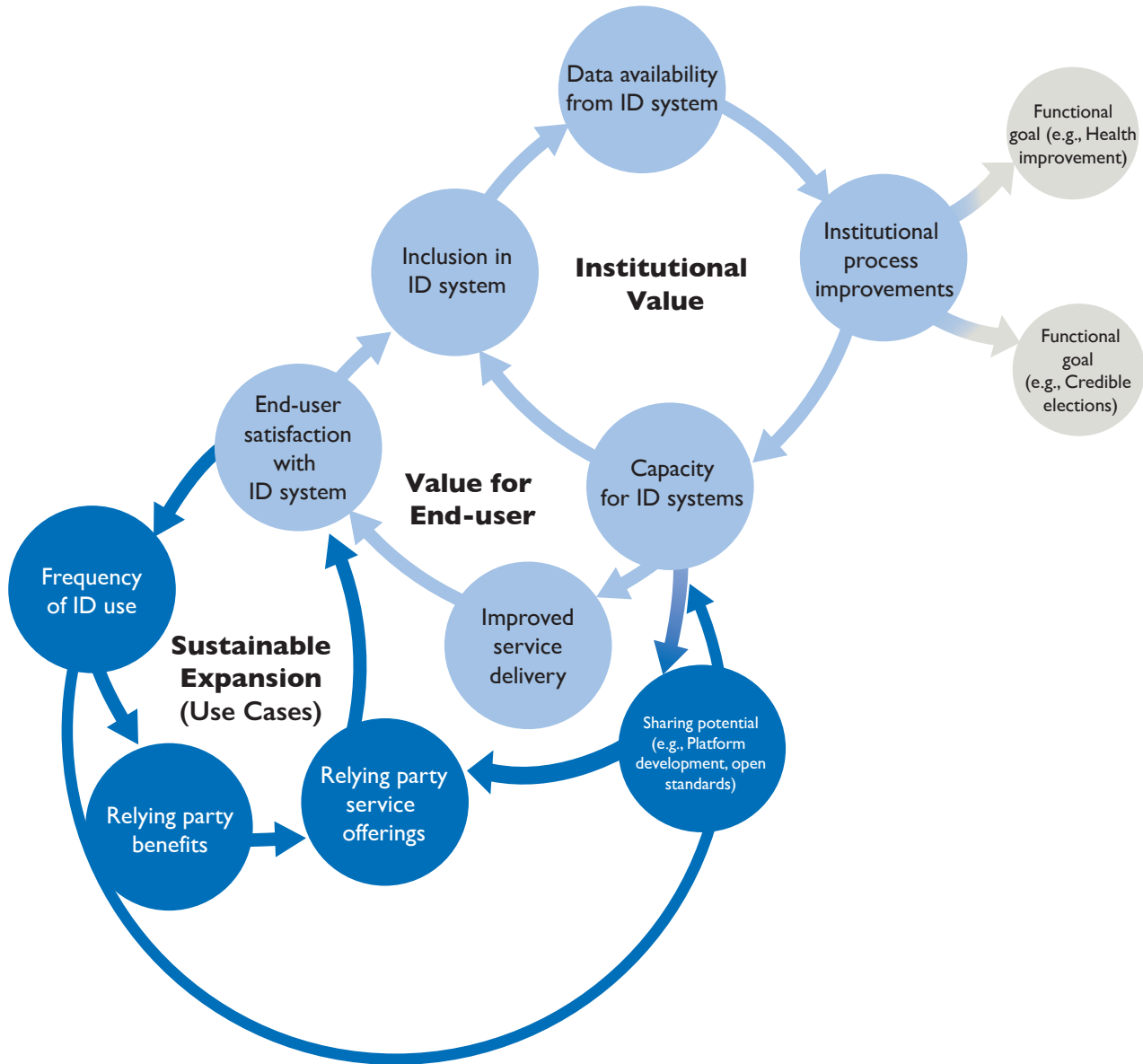
India’s Aadhaar system is an example where the initial public good system architecture can support generation of revenue by non-governmental actors. Although Aadhaar could have been optimized for the sole purpose of distributing welfare benefits, there were a number

of design choices made during its development that facilitated more widespread use. First, the Aadhaar database itself does not include information about what services are authorized for a given user; rather, its design was built using a series of open APIs that allow multiple services to link with the database. This design enables different relying parties to authenticate individual identity using the Aadhaar number and separately link specific services to it.

The non-profit think tank iSPIRT played a significant role in developing the set of open APIs collectively known as IndiaStack<sup>43</sup> which support a suite of services including Aadhaar Authentication, Aadhaar e-KYC, eSign, DigiLocker, Unified Payment Interface (UPI), and others still under development. Through these APIs, the Aadhaar system allows an individual to link her bank account to her Aadhaar number for branchless banking and peer-to-peer payments, facilitates completion of e-KYC to extend access to financial services, enables digital document signing to allow for information sharing, and other related services. These open applications make it possible for Aadhaar to become a foundation<sup>44</sup> for a multitude of social transactions that can ultimately create efficiencies across many sectors. It can also generate revenue by charging fees on transactions that query the ID database, which serves as the infrastructure upon which other services can build.

The structure of this public-good-motivated investment can be understood in the context of the DID system map first put forward in the previous section; Figure 14 shows how the explicit design decision to invest in the construction of a service-oriented add-on capability can help fuel longer term public-serving sustainability. Generally speaking, self-sustaining identity systems require adequate resources to get started, take significant time to reach maturity, and often succeed because they offer access to a broad range of widely valued services.

<sup>44</sup>Ramnath, N.S. (2016). “Aadhaar 2.0: Creating India’s digital infrastructure.” [livemint.com](https://livemint.com).



**Figure 14:** This diagram combines the core causal loop (light blue) with a peripheral feedback loop (dark blue). The core loop indicates the typical value proposition of DID systems for institutions and end users, while the peripheral loop represents sustainable expansion of DID systems. This additional loop demonstrates how the value of infrastructural systems is further enhanced by open platforms and relying party services that provide additional user benefits and ultimately help drive the core system's sustainability. These services can generate revenue through transaction fees that are borne by other actors, including public and private sector actors, or even in some cases even individual ID users. Failure to consider the potential compatibility of a particular scheme with others can miss opportunities to promote more sustainable and widely valued systems.



Other national systems have also addressed the parallel needs of institutions and users to achieve sustainable, infrastructural DID systems. Two notable examples stand out.<sup>45</sup> One is Pakistan's National Database and Registration Authority (NADRA).<sup>46</sup> Whenever a government agency or a private entity (such as a bank) authenticates a user against NADRA's biometric database, they are charged a small fee. NADRA has formed an independent public company (NADRA Technologies Limited) that provides consulting services to other countries seeking to replicate their model. According to former NADRA chairman Tariq Malik, this revenue model was chosen specifically to avoid political interference. As Figure 14 shows, *increasing frequency of ID use generates benefits for relying parties* (e.g., banks) and provides funding that supports *the capacity of the ID system*. If these returns are well-invested, they can improve service delivery and further increase *end-user satisfaction*.

A similar approach was taken by Peru's *Registro Nacional de Identificación y Estado Civil* (RENIEC). RENIEC is partially government-funded, but the bulk of its funding comes from ID document issuance and renewal fees.<sup>47</sup> These fees (and the requirement of a paper birth certificate) have reportedly created some barriers to participation for undocumented and poor populations. Per-person enrollment costs are much higher in remote areas due to reliance on traveling registry teams. Despite these challenges, the 2014 Americas Barometer survey<sup>48</sup> found an ID coverage rate of over 99 percent, and a similar survey reported that Peruvians have more faith in RENIEC than in the Catholic Church. The success in coverage stems largely from linking RENIEC to services

that people find useful, in both the public domain (e.g. government service delivery) and the private domain (e.g. third party service providers).

It is difficult to generalize based on only these examples, but there are broader lessons to be learned from NADRA and RENIEC. First, Pakistan and Peru are lower-middle-income and upper-middle-income countries, respectively; although both have impoverished sub-populations, the transaction or registration fees are within reach of most citizens. Both are smart card systems that connect to a wide variety of services, including finance, health, elections, and security. Both have been around for some time; NADRA's legal mandate dates back to 1973 and the agency has existed since 1999, while RENIEC was established in 1993. Perhaps most importantly, both systems are popular—they seem to be widely perceived as useful and trustworthy, resonating with what we look to ID systems to provide us at a fundamental level. Critically for both RENIEC and NADRA, people use them because they enable access, not simply because they are mandated. Generating popular support is an important “demand-side” factor that contributes to the sustainability of the program.

### From DID schemes to balanced systems

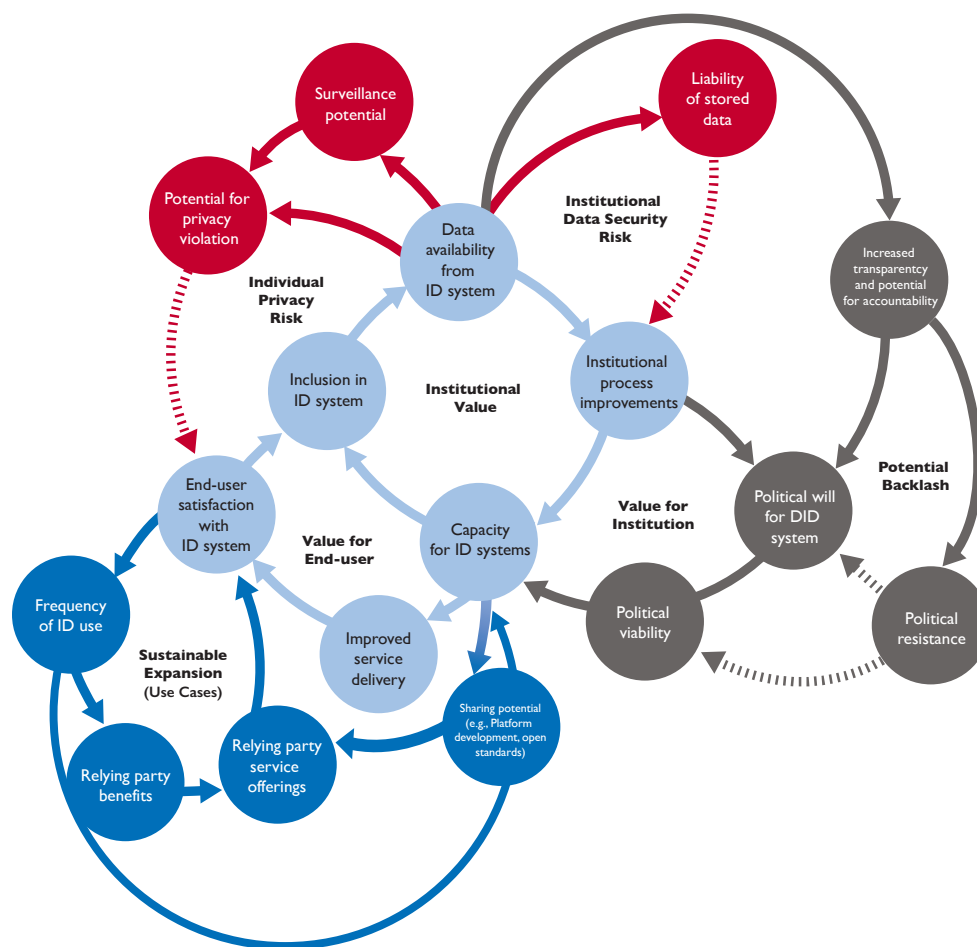
For a system to sustainably serve both individuals and institutions, the core reinforcing loops must balance the potentially opposing loops. That means balancing increasing data availability with privacy and data security risks, balancing the threat of political backlash with stronger political support for transparency and capacity, and balancing investments in expanding the system with generating value for the individuals who need to enroll.

<sup>45</sup> Biscaye et al. (2015). “[Review of National Identity Programs](#).” U. of Washington, Evans School Policy Analysis and Research.

<sup>46</sup> Malik, Tariq (2014). “[Technology in the Service of Development: The NADRA Story](#).” Center for Global Development Essay.

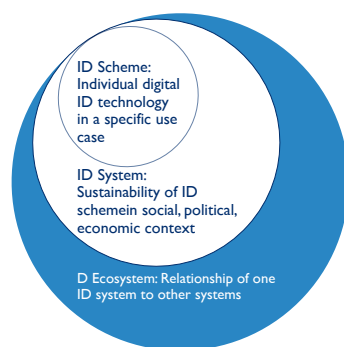
<sup>47</sup> Harbitz & Boekle (2009). “[Democratic Governance, Citizenship, and Legal Identity: Linking Theoretical Discussion and Operational Reality](#).” Inter-American Development Bank Working Paper.

<sup>48</sup> <http://www.vanderbilt.edu/lapop/>



**Figure 15:** This diagram combines all of the causal loops presented in the preceding sections. The core loop still expresses a typical value proposition for DID systems (light blue). The peripheral feedback loops contribute to a system's success or failure in achieving more efficient and effective programs, as well as the long-term sustainability of the system. Investing in DID systems without accounting for privacy risks and institutional data security risks (red) and political support or backlash (gray) can compromise the ability to achieve the desired efficiencies. Failure to consider the potential compatibility of a particular scheme with others (dark blue) can miss opportunities to promote more sustainable and widely valued systems.

## From fragmentation to harmonization:



## Toward an infrastructural approach

Development actors are beginning to see that healthy ID ecosystems enable sustainable development work. Efforts such as ID4D,<sup>49</sup>

ID4Africa,<sup>50</sup> and Mobile for Development<sup>51</sup> aim to use ID to bring currently excluded people into formal

and foundational systems, and to promote efficient, transparent, and trusted transactions. Several of the motivations underlying these more integrated DID systems—greater inclusion and more efficient, data-driven and effective programming—are the same as for instrumental investments. These efforts, however, seek to achieve these goals through support of sustainable infrastructural systems.

A well-integrated ID system is like a road network. Roads are often built and maintained by governments, but roads support both government needs and private commerce. In this analogy, instrumental ID investments are like building a private road to a specific project site; the new road may help the project reach its goals, but

<sup>49</sup> <http://www.worldbank.org/en/programs/id4d>

<sup>50</sup> <http://www.id4africa.com/>

<sup>51</sup> <http://www.gsma.com/mobilefordevelopment/>

repeatedly investing in single-use roads is not optimal. A better approach would involve connecting to existing roads, or coordinating with others who will use the road to share the burden of building and maintaining the road. Similarly, when digital ID systems are recognized as an infrastructural part of both development programs and functioning digital economies, we are better equipped to construct inclusive ID ecosystems that outlive our time-limited interventions.

### Drivers of a fragmented landscape

Despite the growing global recognition of the role of ID in sustainable development, incentives to set up instrumental systems persist. Understanding fragmentation requires looking at a perspective wider than an individual ID system, and thinking about how several different systems might interact. In the next few sections, we walk through several of the drivers of fragmentation that become clear as we consider the dynamics beyond individual DID systems.

### Influence of tech vendors

ID system designers are often subject to pressure by the technology vendors supplying components of the system. Biometric registration kits, smart cards, and smart card readers often use proprietary software that perpetuates reliance on a particular vendor (also known as “vendor lock-in”). This contributes to repeat investments in systems that cannot be easily reused or repurposed. For example, interviewees mentioned that vendor influence contributes to fragmented investments in BVR systems. BVR deployments are often rushed in the run-up to an election; this can hamper transparent procurement and favor politically well-connected firms.

### Project-driven timelines

Similarly, implementers are expected to adhere to specific project timelines. This limits their ability to collaborate and to design systems that are compatible across multiple sectors and/or programs. Designing context-sensitive systems that complement the work of others requires a time investment that is often not allowed by project timelines. Without deliberate efforts to collaborate and

develop relationships, the default approach is to use a system that will most quickly meet the needs of a single program. This typically means working independently and building project-specific ID systems. This can be particularly acute in humanitarian programs, which are deployed in quickly evolving emergency situations where coordination can be difficult.

### Desire for control and project-specific reporting requirements

Implementers may be motivated to build their own ID schemes to simplify the process of linking their programmatic investments to specific outcomes. This could come from rigid monitoring and evaluation (M&E) criteria being imposed on an implementing partner (IP) or quite simply for the “photo op” that branded systems offer. This has been cited as a challenge in humanitarian systems, where implementers are required to ensure that their distributions are attributable and accounted for. Although collecting individual-level data can support data-driven decision making, doing so without commonly adopted data standards and plans for reuse can result in incomparable or partially representative data that can actually undermine decision making.

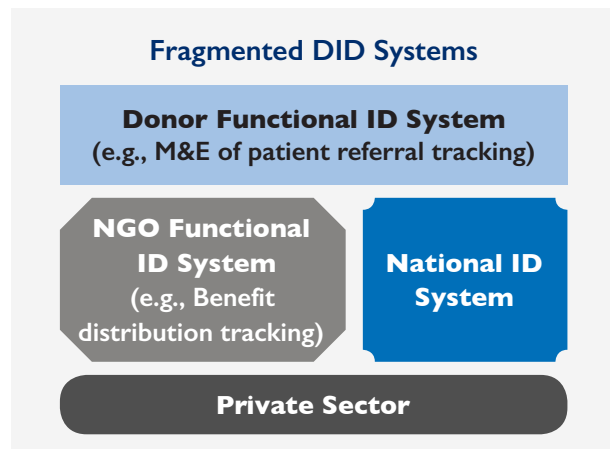
### Piecemeal regulatory landscape

Across the countries in which USAID works, data privacy, management, and protection frameworks are highly variable. In some countries regulations exist but are poorly enforced; in some they are absent altogether. Further, regulations across sectors are highly variable and potentially inconsistent. For example, the regulations around health data and personally identifying information may differ from what financial institutions require for the purposes of meeting AML/CFT requirements, which makes it difficult to build systems that can be repurposed or shared across sectors. This issue has also arisen with IDs issued by humanitarian organizations for refugees, which are not accepted for Know-Your-Customer (KYC) purposes in most destination countries. Reconciling inconsistent or absent regulatory frameworks can be a barrier to developing systems that are easily repurposed or compatible across sectors.

## Gaps in existing infrastructure

Not all countries will have existing digital ID systems—either functional or foundational—that are appropriate for a specific development program. Where there are few other systems that exist, or where protecting privacy and data security of individual information may merit a distinct system, organizations may choose to stand up systems that meet their project needs with little consideration for additional use.

Taken together, these drivers result in a fragmented digital identity landscape in which multiple digital ID systems, each of which may be a well-functioning system, are operating in isolation of each other and missing opportunities to form more sustainable infrastructure for digital development.



**Figure 16:** Isolated ID systems, though often individually successful in achieving the functional goals for which they are developed, can miss opportunities to form a more cohesive, sustainable ID infrastructure.

## Promising paths toward harmonization

Building sustainable digital ID systems is not the primary goal of most USAID programs, yet there are clear steps we can take, and are already taking, to harmonize the programmatic investments in digital ID systems we do make. These steps begin to show potential approaches that let us achieve our core development objectives through better adoption of good practices like the Principles for Digital Development and the Principles on Identification.<sup>52</sup> In the examples that follow, we highlight functional systems that are incorporating aspects of an infrastructural approach.



## Practical implications of an instrumental approach:

One example of a missed opportunity in practice comes from a recent integrated nutrition project in South Asia. An M&E system was designed to support the implementation of the project. In addition to more traditional M&E functions, it included unique identifiers for beneficiaries to track which specific interventions were affecting whom. The unique ID numbers were based around village-level geocodes, and aid recipients interacted with the system only by providing their names and having them checked against a list of registered people. These IDs enabled strong M&E capabilities but were limited-use and not standardized to interoperate with other systems. Since the ID portions of the system were not a primary focus of the integrated nutrition project, they were designed only in service of narrow monitoring and evaluation goals and not set up for scale.

The system had demonstrated broad utility for the project, and staff saw promise in utilizing it in future programming as the initial project came to an end. Unfortunately, however, the system was never designed to be re-purposed for other programs—the geocoding scheme was idiosyncratic, the software was not open-source or built to be picked up by developers not involved with the initial project. At the same time, the implementing partners had transitioned to a new enterprise M&E system and had little interest in maintaining this legacy system for the use of others. Ultimately the system was successful for its original limited-term purpose but lacked the qualities necessary to provide value beyond the life of the project, missing opportunities for efficient repurposing.

<sup>52</sup>World Bank Group and Center for Global Development (2017). "Principles on Identification for Sustainable Development: Toward the Digital Age."

## Encouraging open source solutions

Under USAID's Saving Lives at Birth Grand Challenge, Simprints is using smartphones connected to biometric fingerprint scanners to improve maternal and child health outcomes.<sup>53</sup> By using a fingerprint as a unique ID by which to track and recall health records, the Simprints system allows health care workers to have better access to health data and provide better care to individuals. Several features are consistent with a more infrastructural approach. Use of open fingerprint standards make their system interoperable with other fingerprint databases. This feature also allows linkages with other types of programs that might rely on biometric identifiers, for example microfinance programs or vocational training. Further, they use an open source interface library that allows organizations to sync unique IDs across devices and integrate with other open software, such as Open MRS<sup>54</sup> (an open-source platform for electronic medical records), or ODK<sup>55</sup> and Magpi<sup>56</sup> (for mobile data collection). These systems design choices enhance the value of the system for institutions that may seek to integrate data across programs and partners, allow for organizations to modify and adapt the system over time, and enhance long-term use of the system.

## Encouraging and creating space for collaboration

USAID has played a role in addressing some of the unintended consequences of having multiple organizations develop similar systems independently. Many humanitarian organizations have built their own digital ID systems, customized for the harsh conditions in which they work. For the Syrian refugee response, USAID's Food for Peace Office advocated for implementing partners to move to adopt the same digital ID system to share registration information and in some cases, track benefit distribution. Together with counterparts from the European Union and United Kingdom, USAID is helping the organizations converge assistance being provided on a single card to

streamline tracking and ease the burden on individual refugees. This type of coordination and adoption of a single system is not always appropriate: sometimes needs across institutions are unique enough that system alignment would not actually be beneficial. So although not a universal solution, this offers an approach to limit fragmentation when possible. Together with counterparts from the European Union and United Kingdom, USAID was able to help the organizations converge on a single card to streamline tracking and ease the burden on individual refugees. This type of coordination and adoption of a single system is not always appropriate: sometimes needs across institutions are unique enough that system alignment would not actually be beneficial. So although not a universal solution, this offers an approach to limit fragmentation when possible.<sup>57</sup>

Coordination efforts become especially difficult when different government ministries issue different IDs, complicating partners' choices and introducing political sensitivities. Even when a national ID already exists and includes a program's target population, it can still be a demanding feat for implementing partners to utilize them. In Swaziland, national ID cards are commonly used to access health facilities. USAID's MEASURE program<sup>58</sup> leveraged this existing system rather than building a new patient tracking database. This required working with Swaziland's Ministry of Health, Ministry of Information, Communications and Technology, and Ministry of Homeland Affairs. Interviewees with the MEASURE program felt that the system in Swaziland was working well, and that while challenging, intra - country coordination was worth the effort and contributed to the larger aim of strengthening the health infrastructure within the country. As donors, we must acknowledge the role that we play in either incentivizing or disincentivizing this type of collaboration and alignment.

<sup>53</sup> <https://www.simprints.com/technology/>

<sup>54</sup> <http://openmrs.org/>

<sup>55</sup> <https://opendatakit.org/>

<sup>56</sup> <http://home.magpi.com/>

<sup>57</sup> In this case, data are stored on servers in Rome rather than locally, raising some concern about data ownership. Further, convening multiple partners around one system may not always be desirable; some organizations may have specific requirements or data privacy concerns that would be better served by systems that are distinct yet compatible when data-sharing is necessary.

<sup>58</sup> USAID (2017). "MEASURE Evaluation Phase IV."

## Investing in high level coordination and harmonization of data systems

Health information systems need to effectively coordinate service delivery across many programs, partners, and facilities. Although decisions are based off of aggregated data, they sometimes rely on individual IDs at the local level. Inconsistent use of unique identifiers has contributed to many global health challenges, for example, impeding ability to track testing, cases, and follow-up with Ebola patients during the West Africa Ebola outbreak.<sup>59</sup> The Health Data Collaborative<sup>60</sup> is one example of a current USAID engagement that seeks to align the data collection practices and information systems that underlie health decision making.

## Collaborating to develop good practices in the absence of formal frameworks

In the absence of such frameworks, some organizations are taking steps to begin to establish good practices for data privacy and management. Examples include WFP's data privacy guidelines<sup>61</sup> and recommendations from Cash Learning Partnership to work toward harmonizing ID requirements related to KYC regulations and humanitarian cash transfer programs.<sup>62</sup> Working collaboratively to develop good practices that may eventually become widespread will make it easier for actors to converge around common practices that ultimately create a more cohesive landscape.

## Engaging multiple partners when building new ID schemes

In Botswana, USAID-funded MEASURE Evaluation sought to track referrals of women who experience gender-based violence. Although a national ID system existed in Botswana, it was not well-aligned with the target population, which included a large number of non-citizens. Relying on the national system would have reinforced this exclusion. MEASURE worked with multiple local stakeholders, including the Gender Affairs Department in Botswana's Ministry of Labour and Home Affairs to pilot

a new tracking system.<sup>63</sup> This system allowed partners to more efficiently monitor service provision and identify incomplete referrals, as well as remain inclusive of their target population and limit the sharing of these data within the specified network of service providers. Although a separate system was needed, working with multiple partners across sectors in developing the referral system was necessary and may result in the system having longer term use and value to multiple organizations involved in the project.

## Recognizing the value proposition of a public good

Digital financial services, electronic health records, land ownership records, electronic voting and e-governance all require a robust digital identity through which individuals effectively participate in the larger digital economy. Sector-agnostic or project-agnostic digital ID systems can function as a public good, supporting future innovation and providing a solid digital foundation for multiple functions that require ID.

In the long term, USAID can support public goods ID investments by recognizing their contribution both to the achievement of sustainable development goals and as critical enablers of our programming objectives. With this approach, investments in foundational or national ID systems support lasting infrastructure in host-countries while also meeting programmatic objectives. One example of this approach is USAID's support of My ID My Life, a national ID mobilization and registration campaign in Kenya, which started under the Yes Youth Can (YYC) activity. This was one of the largest youth programs supported by USAID in the world, which is now carried out by Kenya Youth Employment and Skills (K-YES) program with continued support from the County Youth Bunge Forums (CBFs). (Bunge is a Swahili word for parliament.) One part of the Yes Youth Can initiative was the My ID, My Life program, which targeted youths aged 18–35 to help expand access to essential services

<sup>59</sup>See Fast, L. and Wagman, A. (2016). "[Fighting Ebola with Information: Learning from data and information flows in the West Africa Ebola response](#)." Washington DC: U SAID. p.32.

<sup>60</sup><https://www.healthdatacollaborative.org/>

<sup>61</sup>World Food Programme (2016). "[WFP Guide to Personal Data Protection and Privacy](#)."

<sup>62</sup>Levin et al. (2015). "[Know Your Customer Standards and Privacy Recommendations for Cash Transfers](#)." Office of the U.N. High Commissioner for Refugees.

<sup>63</sup>Bloom & Curran (2014). "[M-Health Referral System Designed to Strengthen Access to GBV Services in Botswana](#)." Evaluate: The MEASURE Evaluation Blog.

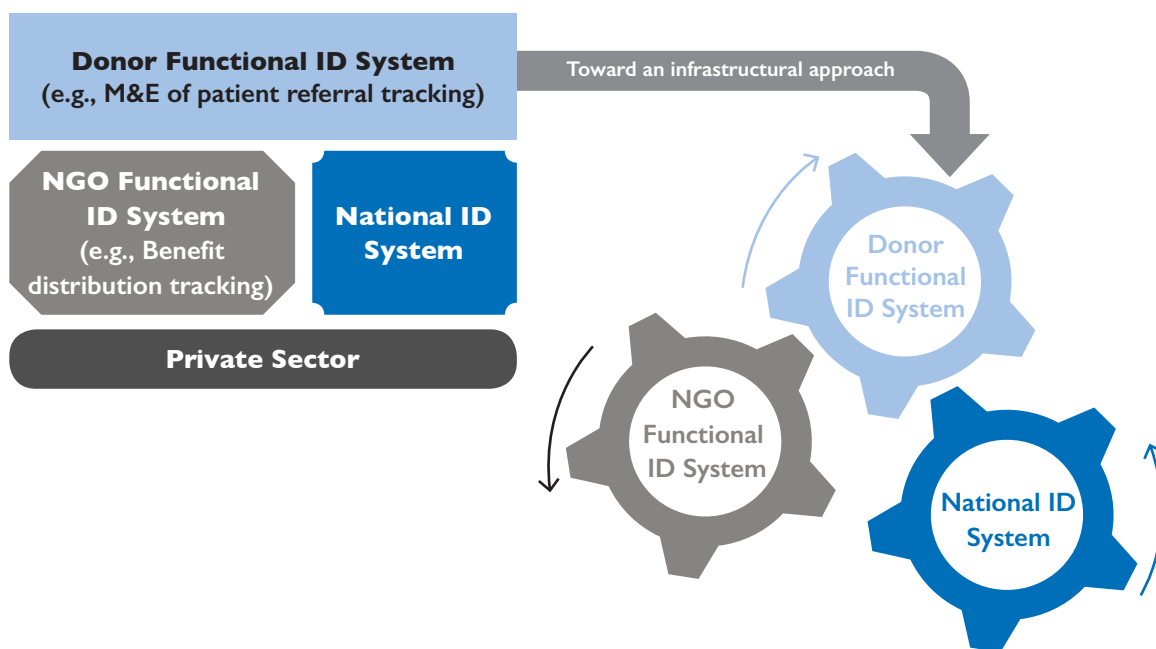


and promote cohesion in an effort to prevent triggers for post-election violence following the 2013 presidential election campaigns. The program engaged youths to help mobilize voters and encourage youth to get the required documentation, including both a national ID card and a voter registration card in advance of the election. The program is estimated to have been responsible for helping approximately one million young Kenyans get national ID cards. In this case, the project recognized the critical role of ID in Kenyan society and targeted youth enrollment in the national ID system as an enabler of the development objective. This approach strengthened the underlying national ID system by improving its inclusiveness, and contributed to the larger objective of strengthening civic participation and youth empowerment in Kenya.

Another example of a public goods investment is in Civil Registration and Vital Statistics (CRVS) systems that link to national identity systems. In Malawi, USAID and Centers for Disease Control and Prevention (CDC) supported the National Registration Bureau (NRB) of

Malawi's Ministry Home Affairs and Internal Security to strengthen its CRVS system and integrate with the electronic medical records system. Now, the NRB is building off this investment to roll out a national ID system that will be linked to the CRVS. With the new system, each newborn will be provided a national identity number from the NRB that will be on the birth certificate and carried forward for life.

This investment in strengthening the underlying CRVS system enhances digital identity infrastructure by strengthening the enrollment process into the national ID system. The initial investment in CRVS and its integration with other systems was made under a PEPFAR initiative to improve HIV case identification in newborns and improve targeting of HIV treatment. By linking the role of the CRVS system to achieving sustainable outcomes in HIV prevention and treatment, the project served a programmatic objective while also strengthening the underlying identity infrastructure.



**Figure 17:** Taking an infrastructural approach to ID systems can facilitate a shift from a fragmented landscape of isolated systems toward a more cohesive ecosystem, in which multiple systems are able to work together to fulfill functional objectives and strengthen the underlying development infrastructure.

## A DID ecosystem that is more than the sum of its parts

These approaches may maintain systems that are independent from others, yet built in ways that are compatible with other systems. Taking steps like these enable individual programmatic investments in DID systems to contribute to a whole that is greater than the sum of its parts. Together, these choices contribute to a DID ecosystem in which individual systems can work together<sup>64</sup> to form a sustainable, inclusive infrastructure for development.

As an Agency, however, these efforts are sporadic rather than part of concerted strategy to support infrastructural investments in digital ID systems as a key part of development infrastructure. Moving forward, this report recommends that USAID consider developing a more consistent approach to supporting digital ID infrastructure and maintaining a commitment to good practices in our reliance on digital identity systems.



### Starting from where we are: Harmonizing disparate systems

For certain populations, the challenges of fragmented systems are more immediate. Take for example the cross-border populations who are the focus of the USAID-funded Regional Action Through Data (RAD) project.

The RAD project is implemented by Broadreach in partnership with the West African Health Organization (WAHO) and the Intergovernmental Authority on Development (IGAD), and local partner Jembi Health Systems. The project seeks to improve the care of cross-border populations such as truck drivers or refugees. One strategy of this project aims to develop a cloud-based platform that will authenticate both patients and providers from any geographic location. This is anticipated to improve health outcomes in two ways. First, provider authentication will ensure that patients see providers whose identity and credentials are verified. Second, patient authentication will allow individual identities to be verified and linked to accurate health information.

The RAD project will have to overcome multiple challenges. First, there is no single identifier that is common to cross-border individuals. Cross-border populations come from multiple cultural and national backgrounds, and there is no standard identity document or even combination of personal information that each individual will be able to present at enrollment. The platform RAD develops, then, must be able to accept a variety of attestations of one's identity, from official ID documents to biometrics to unique knowledge.

Authenticating individual identity in this context is also challenging. Authentication will have to rely on the accuracy of whatever attestations are provided, but these may have varying levels of integrity. For example, a birth certificate from one country may be very easy to duplicate or alter, while in others it may be tightly linked a national database. A person's national ID may be linked to biometric verification in their home country, but the clinic at which they seek care in a neighboring country may not have the proper authentication equipment. Some people may have no prior identity documents at all.

The RAD team will have to be responsive to varying policy and legal contexts that apply to the institutional actors involved in their system. Working across multiple countries will require conforming to countries with different data privacy and protection standards, potential conflicting standards, or no standards at all. Similarly, different clinics will have varying standards for the strength of authentication needed to accept that a patient's identity has been accurately verified. Both health care providers and individual patients will need to trust that the health information linked to their ID has not been altered by unauthorized parties, which requires a level of data integrity as well.

Finally, because it is a regional platform that will serve individuals and providers across multiple regions, there are questions about assigning roles and responsibilities related to data ownership, management, and sustainability. If data are provided by the individual, authenticated by one country's government, accessed by another, and stored on servers in yet another, who "owns" the data? Who is responsible for maintaining it? If the platform is truly of value to multiple countries and yet controlled by none of them, how will it be financed in the long term? This project will likely produce valuable learnings regarding the practical challenges of harmonizing disparate systems.

<sup>64</sup>This is a vast oversimplification of what "working together" can or does look like in the context of identity systems.



## Key Findings

### **Taking an instrumental approach means missed opportunities to reuse or repurpose existing ID schemes.**

One-time, functional ID systems run the risk of over-design to address the problem closest to the designer, limiting the possibility of responsibly reusing the technical system in other contexts.

As an example, the M&E system built for the integrated nutrition project referenced on p. 35 succeeded in its initial purpose to support its project. Unfortunately, it also missed an opportunity to contribute to the success of other programs through durable investment in a reusable ID system. Despite the enthusiasm of mission staff, initial design choices have made it very difficult to repurpose the system for future programs. A more concerted effort to embrace good practices like the Principles for Digital Development at the design stage can help avoid this sort of missed connection in the future.<sup>65</sup>

---

### **Foregoing an infrastructural approach causes donors to miss long-term, durable success.**

Frequently, donor ID investments miss opportunities to build on prior work. As has been mentioned, a number of USAID-supported countries lack a persistent voter roll to which new voters can continually be added. Instead, voter registries are created from scratch for each election, requiring individual voters to re-register every few years—often with proprietary biometric registration kits. Because voter rolls and accompanying biometric

databases are not maintained, these expensive systems are procured and built repeatedly for the same voters in the same precincts. Data from African elections<sup>66</sup> (described above) suggest that a continuous voter roll could bring costs down by as much as \$68M for each election cycle. These repeated expenditures waste opportunities to invest in more durable election systems that can build public confidence and help contribute to breaking cycles of instability.

---

### **Taking an instrumental approach means missed opportunities to better serve the needs of diverse populations.**

Sectorally-focused investments in digital ID schemes can limit donors' ability to serve individuals whose needs extend beyond the focus of any single program. For example, the digital ID schemes underlying cash transfer programs employed in humanitarian response often require extensive collection of background data before issuing an ID linked to their organization, but are not necessarily recognized as forms of IDs that meet the KYC standards necessary to access credit and other financial services. This should not be the case.

<sup>65</sup> <http://digitalprinciples.org/>

<sup>66</sup> Gelb & Diofasi (2016). "Biometric elections in poor countries: Wasteful or a worthwhile investment?" Center for Global Development Working Paper 435.

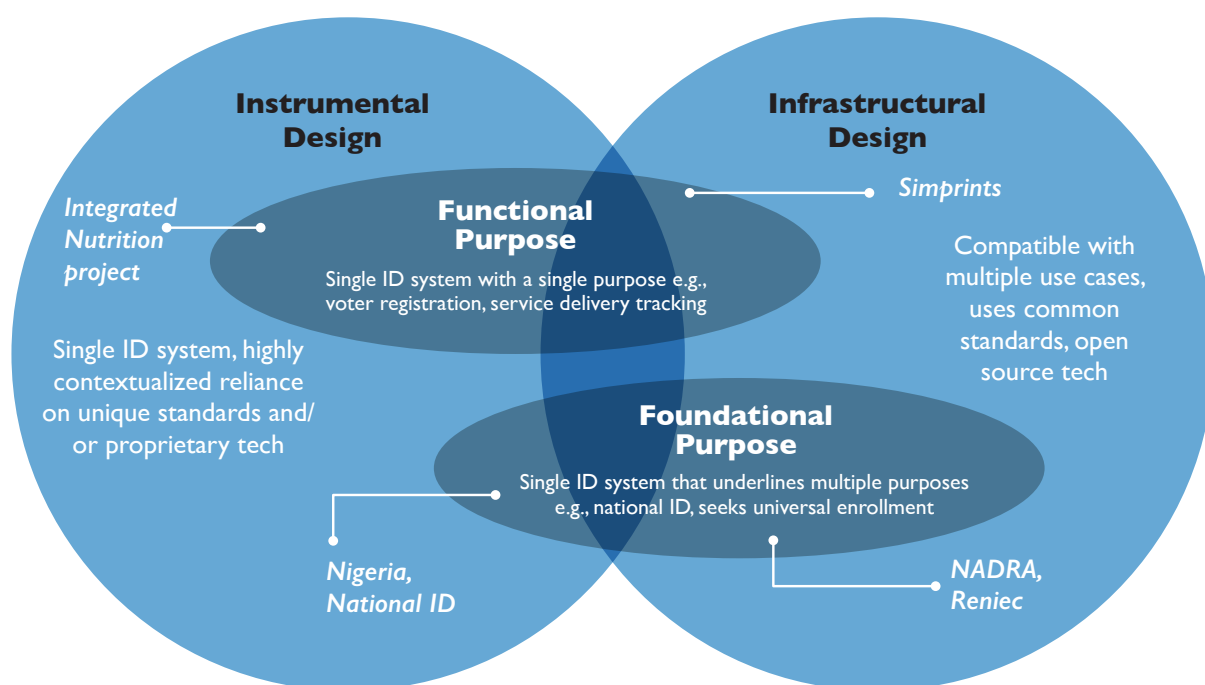
The Cash Learning Partnership<sup>67</sup> has recently developed recommendations for tiered KYC standards in humanitarian response that would allow ID issued by NGOs to meet KYC requirements for some limited services. Working to establish good practices and shared standards across sectors may both enhance the benefit to end-users and eliminate redundant efforts to verify identity of the same individual by different institutions.

## Summary of Digital ID System Landscaping

Part I of this report has examined the present role of digital ID systems in development and in USAID

programming. A substantial “identification gap” makes it harder for the world’s most vulnerable people to exercise their political rights, access life-saving services, and engage in the formal economy. ID systems have the potential to serve as essential development infrastructure that helps to address a wide range of needs. But this potential often goes unrealized.

Instead, the current landscape is fragmented by multiple functional and foundational ID systems that reflect elements of both instrumental and infrastructural design choices. As a whole, this landscape results in inefficiencies and redundant investments, and ultimately fails to bridge the identification gap.



**Figure 18:** Real-world examples of digital ID systems illustrate the ways in which instrumental and infrastructural design choices can manifest in systems with either functional or foundational purpose. Integrated Nutrition project is an example of an M&E platform that used instrumental design choices like unique geocodes and proprietary software for a functional purpose (nutrition). Conversely, Simprints uses open standards that can be integrated across multiple digital platforms and with other biometric systems, representing more infrastructural choices for meeting a functional goal (maternal health). Foundational systems also reflect a spectrum of design choices. Nigeria’s early national ID system relied on proprietary systems that limited later reuse, whereas Peru’s RENIEC reflects common data and technical standards that allow for multiple functional uses to be linked to it.

Donor investments in digital ID systems often proceed from an instrumental mindset, in which functional ID systems serve the goals of a particular project and can be discarded once that project is completed. We argue that, by taking a context-sensitive systems approach and

promoting infrastructural design choices through technical assistance, thought leadership, and our own investments, we can support both functional and foundational ID systems that create pathways to a more sustainable, inclusive identity ecosystem.

<sup>67</sup> Levin et al. (2015). “[Know Your Customer Standards and Privacy Recommendations for Cash Transfers](#).” Office of the U.N. High Commissioner for Refugees.

# 2



## PART 2: Preparing for Futures of Digital ID



New technologies and trends are bringing distinct opportunities to add value for both individuals and institutional actors. As people lead increasingly digital lives, applications of machine learning and algorithmic analysis may lead to new ways of identifying individuals. Data from mobile phone use,<sup>68</sup> social media participation,<sup>69</sup> and e-commerce<sup>70</sup> can uniquely identify people with greater accuracy. 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 data privacy, control over data sharing and use, and surveillance.

New technologies will also cast new actors in the roles of ID providers, authenticators, and authorizers. Official ID has traditionally been provided by governments. Increasingly, technology companies will find new ways to store identity information, authenticate, and authorize new services. These innovations can offer efficiency gains, greater transparency, and better security. At the same time, new actors will also limit the visibility and control that governments and citizens have previously had over identity authentication and service authorization.

As ID-mediated relationships grow more diffuse and complex, trust between people and institutions will play a dominant role. Regardless of which new technologies continue to develop and how systems evolve, future DID systems must still provide value to both individuals and relying institutions. Shared value creation will require a foundation of trust, because a lack of trust will inhibit voluntary participation. There are steps donors can take now to help establish and maintain trust and to shape a future in which the lack of identity is no longer a barrier to being a full participant in society.

## An Evolving DID Landscape

The evolution of digital ID systems will be impacted by a variety of factors. Broad contextual factors—increased connectivity, a growing digital economy, demographic trends, or overall economic growth—are beyond the scope of this study. We focus here on five technology trends that are poised to have near-term impact on the DID ecosystem. Each will be explored in more detail in the following sections.

<sup>68</sup> de Montjoye et al. (2013). "Unique in the Crowd: The privacy bounds of human mobility." *Nature Scientific Reports* 3, 1376.

<sup>69</sup> Narayanan & Shmatikov (2009). "De-anonymizing social networks." 30th IEEE Symposium on Security and Privacy.

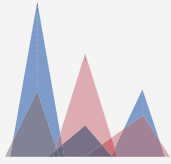
<sup>70</sup> de Montjoye et al. (2015). "Unique in the shopping mall: On the reidentifiability of credit card metadata." *Science* 347 (6221), 536-539.



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

Photo: UN Photo/  
Albert Gonzalez  
Farran





## Focal Trends

→ **Advances in biometrics:** In a biometric ID system, a person's identity is defined by how an electronic device (a biometric reader) recognizes and parses her physical traits. In this view, identity is imposed on a subject when biometrics are captured.

We expect two significant advances in biometrics to influence IDs. First, biometric identification kits are decreasing in size and cost. Low-cost, highly portable or integrable fingerprint readers are poised to make biometric identification more ubiquitous. Second, there are several new technologies that can uniquely identify individuals from less-familiar biometrics such as palm veins, gait, or voice.

→ **Mobile ID:** Mobile phones have become an increasingly significant part of identity system infrastructure. Although mobile devices are likely to be part of all the emerging technology trends discussed, this section will focus on mobile authentication platforms. In mobile authentication, mobile network operators verify individual identity using a registered device in place of a traditional ID card.



Digital footprints can be analyzed to make inferences about an individual's identifying characteristics.



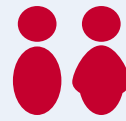
Low-cost, highly portable or integrable readers are poised to make biometric identification more ubiquitous.

Mobile authentication platforms do not substitute for a separate identity proofing or enrollment process. They are a more convenient method of authentication for end-users who already have a registered SIM card. They may also add value for institutions and online relying parties by allowing for higher levels of assurance. Mobile authentication differs from traditional authentication processes in that the authentication query and reply occurs on the token itself—a phone—rather than requiring additional hardware like smartcard or biometric readers.

→ **Algorithmic identification:** Digital footprints can be analyzed to make inferences about an individual's identifying characteristics. Rather than the issuing of personal credentials, "algorithmic ID" refers to authenticating identity based on the patterns and unique features of one's digital footprint. In contrast to one-time biometric capture, identity is inferred from a subject's behavior in a process that is ongoing and more probabilistic. Both processes can be opaque; for most people, the uniqueness of a fingerprint or an iris is just as obscure as that of a browsing history or a phone call pattern.

→ **Blockchain-backed ID:** Blockchain is a distributed ledger technology that spreads data storage and verification across independent nodes. A blockchain is immutable, resilient against hardware failure, and inherently open. All data in the system are accessible and verifiable to all participants, which positions blockchain to be a “trusted” form of transaction logging, in that the transparency of the system safeguards against tampering by individual actors.

Many proposed blockchain-backed ID systems are examples of “accretionary ID,” where an ID is built up over time through a series of interactions with others. Other blockchain ID applications simply use a blockchain ledger as the back-end database for a more traditional ID system. This may improve transparency, but the differences will likely be invisible to typical users.



**In contrast to systems where institutions provide ID credentials, user-controlled IDs build on the premise that people will control the formalization of their identity.**

→ **User-controlled identity:** This is not a new technology, but rather a new identity approach that places the “ownership” of identity more squarely in the hands of ID holders. User-controlled ID is enabled by technologies such as personal data stores, cloud computing, and attribute-based credentialing.

In contrast to systems where institutions provide ID credentials, user-controlled IDs build on the premise that people will control the formalization of their identity. Increased user control could take various forms, from managing distinct digital personas to actively monetizing one’s own personal data. Advocates for self-sovereign ID<sup>71</sup> go further, arguing that new technologies will enable users to assert and curate a self-created ID independent of any state authority.

Emerging trends in digital ID may help overcome some challenges, yet reinforce others. For example, voice and facial recognition technology may offer alternatives that do not require new hardware and instead rely on the near-ubiquity of mobile phones. Yet these advances may introduce concerns of surveillance and exclude those whose bodies are not well-described by biometrics. The emergence of algorithmic IDs may offer more

authentication options to individuals who currently lack identity credentials, yet may be less useful without standards that allow fair comparison to more traditional forms of ID. Blockchain technology may address concerns about the integrity of data records linked to digital IDs, yet create new concerns related to the right to remove or delete data. Self-controlled IDs hint at the ability for individuals to manage a fully portable ID credential, but

<sup>71</sup> Clippinger, John (2014). “Why self-sovereignty matters” in [From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society](#), pg. 21-28. [ID3/Off the Common Books](#).

may be difficult for users to manage effectively. This can further entrench the digital divide for those whose digital familiarity doesn't allow them to appropriately manage a self-controlled digital identity.

The following sections explore the trends described above in more detail. They are arranged in order of similarity to the existing ID paradigm, beginning with next-generation biometrics as a logical extension of existing systems and ending with the disruptive potential of user-controlled ID systems.

## Biometric Advances



### Advanced Biometrics

<b>What is it?</b>	<ul style="list-style-type: none"> <li>• Smaller, cheaper biometric hardware</li> <li>• More diverse biometric modalities</li> <li>• "Revocable" biometric templates that can be invalidated if stolen</li> </ul>
<b>Example use cases</b>	<ul style="list-style-type: none"> <li>• Palm or iris recognition on phones</li> <li>• Authentication based on voice, facial recognition</li> </ul>
<b>What problems can it solve?</b>	<ul style="list-style-type: none"> <li>• Feasibility: Lowers cost, increases ease of integration into daily life</li> <li>• Inconvenience: Allows for unique authentication without having to carry a physical token/credential</li> <li>• Exclusion: Provides multiple alternatives for individuals for whom fingerprint/iris may not be unique or usable</li> </ul>
<b>What problems does it NOT solve?</b>	<ul style="list-style-type: none"> <li>• Identity-proofing: Biometrics still need to be accurately linked to a real person</li> <li>• Centralization of data: Biometric data concentrated in central enrolling or authenticating authority</li> </ul>
<b>What problems could it create?</b>	<ul style="list-style-type: none"> <li>• Heightened potential for surveillance; possible to track and authenticate identity without individual's consent or knowledge</li> <li>• Exclusion of individuals with non-unique biometrics, disability, etc.</li> <li>• Heightened privacy risks; may be difficult to "reissue" if stolen or compromised</li> <li>• Inadvertent exclusion, opt-out, or stigmatization resulting from biometric capture that is inconsistent with social norms or cultural acceptability</li> <li>• Over-reliance on physical characteristics may diminish acceptability of non-biometric forms of verifying identity</li> <li>• Reinforce tendency to put unquestioning trust in the performance of fallible technology</li> </ul>
<b>What is current state of play?</b>	<ul style="list-style-type: none"> <li>• Common uses include mobile fingerprint scanners or iris scanners. For example, biometric "time clocks" to reduce absenteeism among teachers and government employees, and mobile birth registration with electronic fingerprint scanners</li> <li>• Advanced biometrics such as voice, gait recognition represent "state of the art" and are not common in the developing world</li> </ul>

Similar to current applications of biometrics in ID systems, novel biometrics will play different roles at different stages of the ID value chain. At enrollment, biometrics are used to establish that a new user is unique. This requires sufficient high-quality data to distinguish one person from all others seen by the system. For example, 10 fingerprints and two iris scans may be needed to de-duplicate a national-scale database, as in the case of Aadhaar. Similarly, an ID database based on facial recognition might require high-quality photographs at different angles or one based on voice recognition would need an extended recording.

When authenticating an ID, biometrics only need to confirm whether the public tokens presented are legitimate. This task requires less precision than de-duplication; a single fingerprint or a shorter voice recording may suffice.

Given the rapid uptake of low-end smartphones in many developing countries, we can expect them to become important authentication platforms in the near future. Some biometric modalities (e.g., fingerprint and iris) require specialized hardware not included in bare-bones smartphones. Others (e.g., facial recognition and voice) could capture biometrics with simple phone features (camera and microphone, respectively).

### Passive biometric capture

Although biometrics are often used as a private token, many biometrics are not truly private. For example, fingerprints can be retrieved from any smooth surface<sup>72</sup> and iris templates can be extracted from high-quality facial photographs.<sup>73</sup> Simple voice recognition systems might be fooled by a covertly obtained recording. Biometrics may blur the line between public and private tokens. This is especially true for “surveillance biometrics” that can identify a person without her consent or knowledge.

As biometric capture technology improves, the lines between active authentication and passive surveillance will also begin to blur. For example, a touchscreen interface at an ATM could embed a camera that confirms customer identity using facial recognition, or a customer service call center could capture voice biometrics to verify identity. Passive biometric capture can make interactions more seamless for users and provide an additional layer of security, yet augment privacy risks.



**Passive biometric capture can make interactions more seamless for users and provide an additional layer of security, yet also potentially augment privacy risks.**



Photo: UN Photo/Bernardino Soares

<sup>72</sup> Matsumoto et al. (2002). “[Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems](#)” Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV.

<sup>73</sup> Planet Biometrics News (2015). “[Hacker extracts Merkel’s iris image](#)” (Accessed May 2017).

## Inclusion and biometric failure

Biometric authentication can also affect inclusion in the future DID ecosystem. Biometric identification relies upon the inherent diversity of human bodies, but biometric technology can only capture a limited subset of that diversity. Some people will inevitably be excluded.<sup>74</sup> Many people have fingerprints worn down by manual labor: Asian females in particular are often difficult to fingerprint due to finer ridge structures.<sup>75</sup> Retinas can be obscured by cataracts. Birth defects or injuries could exclude some individuals from biometric-based systems.

Other sources of failure may stem from coincidental similarity to another person's biometrics. If facial recognition algorithms are optimized for a majority ethnic group, they may make more errors on minority faces.<sup>76</sup> This, in turn, would exacerbate concerns about racial discrimination and access to services.

Failure can also result if the body changes significantly between the time of enrollment and authentication. Changes over time have been shown with physical biometrics such as iris scans,<sup>77</sup> and even over a 15-month time span with digital signatures.<sup>78</sup> Biometric aging is less of a concern if one authenticates frequently. If someone notices an increase in rejections, she could update an age-dependent biometric by re-enrolling. Marginalized or last-mile populations, however, might find themselves authenticating much less frequently and could be locked out if their bodies change between encounters with the system.

Biometric technology can also limit inclusion due to the trust we place in the robustness of the technology.<sup>79</sup> As systems grow more advanced and reliable, they are likely

to be perceived (especially by non-expert operators) as infallible. Biometric equipment vendors may not be forthcoming about their error rates, independent field evaluations are rare, and anti-spoofing technologies often do not work as well as advertised. Individuals with unusual biology or victims of identity theft could find themselves at odds with a system that everyone else trusts absolutely.<sup>80</sup> If the burden of biometric failure falls disproportionately on people who are poor, elderly, disabled, or ethnic minorities, existing patterns of exclusion and marginalization could be reinforced.

There are proactive policy interventions that can be taken to address some of these concerns. For example, India's Aadhaar program is required by law to enroll everyone; if fingerprints cannot be collected, they collect iris scans; if iris scans cannot be collected, they take a photograph and an Aadhaar number will be issued based on biographical information. This approach has met mixed reviews,<sup>81</sup> yet the development of flexible enrollment procedures is a positive and necessary step in creating an inclusive system.

## Cultural acceptability

Biometric systems require particular sensitivity to cultural norms surrounding personal privacy and physical space. Research on ID users in India<sup>82</sup> has shown that new enrollees are often unfamiliar with the electronic fingerprint scanners and do not align properly or apply sufficient pressure. Technicians may physically assist enrollees through the process, which may be perceived as invasive or inappropriate in some cultures. Similar issues could arise if people are required to remove traditional clothing items (such as a *burqa*) for iris scanning or facial photographs. Fingerprinting can also create unease in communities where it is associated with law enforcement.

<sup>74</sup> Magnet, Shoshana Amielle (2011). "[When Biometrics Fail: Gender, Race, and the Technology of Identity](#)" Duke University Press.

<sup>75</sup> Schneider, John K. "Ultrasonic Fingerprint Sensors," in Ratha & Govindaraju (eds.), *Advances in Biometrics: Sensors, Algorithms and Systems*, pg. 63-74.

<sup>76</sup> Garvie et al. (2016). "[The Perpetual Line-up: Unregulated Police Face Recognition in America](#)," Georgetown Law Center on Privacy & Technology.

<sup>77</sup> Graham-Rowe, Duncan (2012). "[Ageing Eyes Hinder Biometric Scans](#)," Nature News & Comment.

<sup>78</sup> Galbally et al. (2013). "[Aging in Biometrics: An Experimental Analysis on On-Line Signature](#)," PLoS ONE 8(7): e69897.

<sup>79</sup> Gelb & Clark (2013). "[Identification for Development: The Biometrics Revolution](#)," Center for Global Development Working Paper 315.

<sup>80</sup> Magnet, Shoshana Amielle (2011). "[When Biometrics Fail: Gender, Race, and the Technology of Identity](#)," Duke University Press.

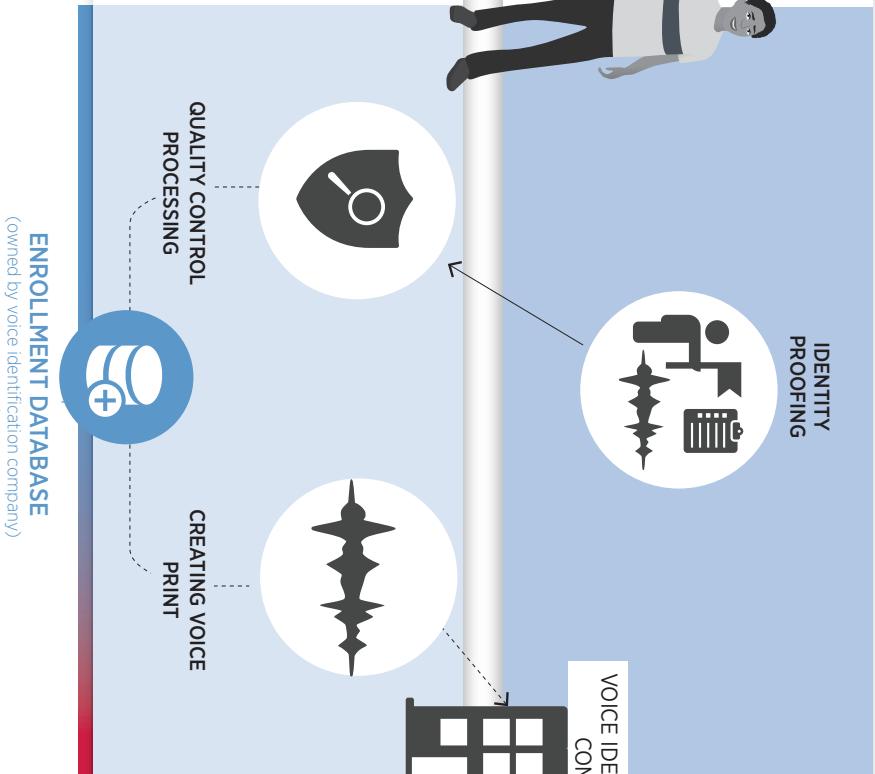
<sup>81</sup> Khurana, Manjira (2016). "[Why Aadhaar is just another burden for India's elderly](#)," Daily O.

<sup>82</sup> As-yet-unpublished Caribou research, aired in workshop (personal communication).

# Advanced Biometrics Digital ID Value Chain

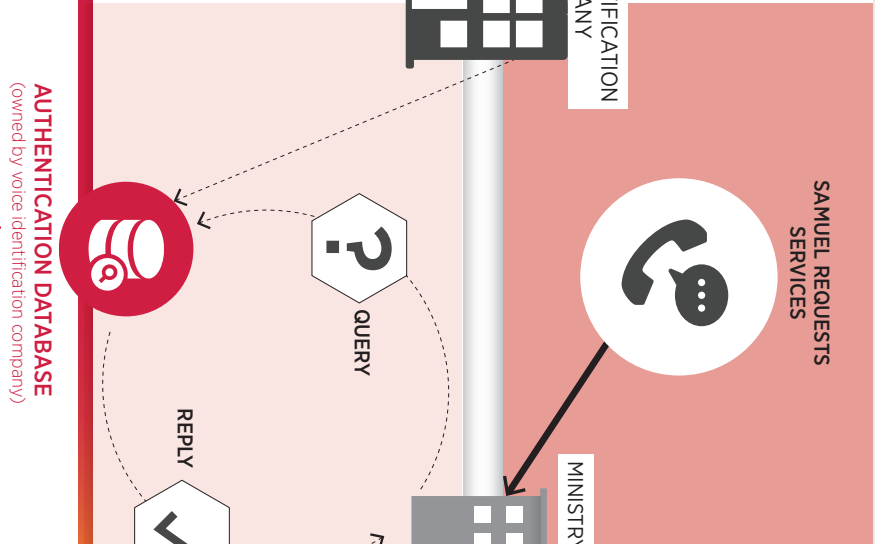
Samuel is a community health worker who often needs to order new supplies for his clinic. The Ministry of Health and international donors are taking steps to secure the supply chain, and his clinic has been enrolled in a pilot program to automatically track orders using health worker identification based on voice recognition. Voice identification systems can be a convenient way to verify the identity of people ordering supplies.

## ENROLLMENT WHO IS SAMUEL, AND HAVE WE SEEN HIM BEFORE?



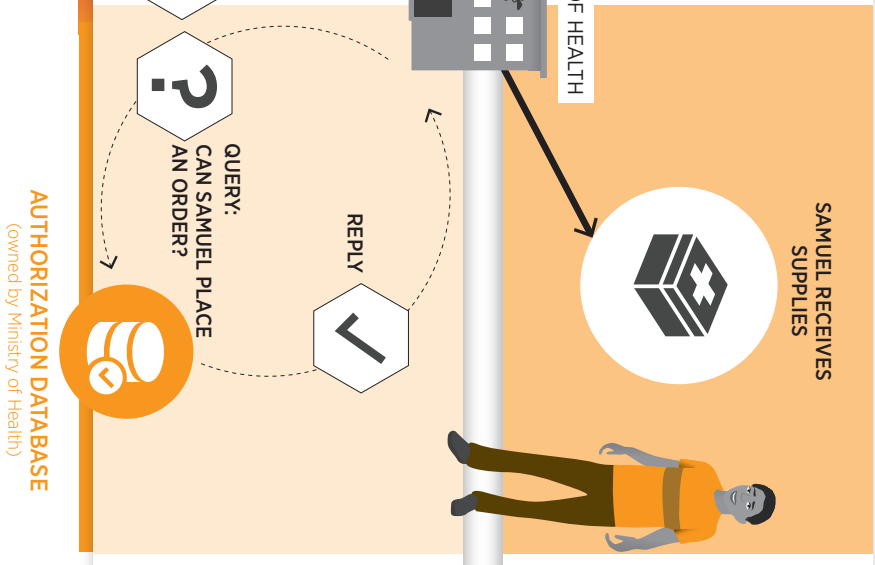
Samuel's supervisor gives him a telephone number and tells him to call it and enroll in the voice recognition system, run by a voice identification company. The call center operator at the clinic where he works, and his supervisor's name. In order to create a unique digital "voice print" for Samuel, she then chats with him for about 20 minutes. After Samuel hangs up, his end of the conversation is used to construct a unique voice print template that is linked to his name and clinic ID and stored in an encrypted format.

## AUTHENTICATION DO SAMUEL'S CREDENTIALS MATCH WHAT WAS ISSUED?



A few days later, Samuel notices that his clinic needs a resupply of antiretrovirals. He phones in to a call center, where he is asked for his name, the name of his clinic, and his order. As he places his order, a computer analyzes his voice to ensure that it matches the voice print created when he enrolled.

## AUTHORIZATION CAN SAMUEL PLACE AN ORDER?



By the time Samuel has finished with his order, his identity has been confirmed. The Ministry of Health confirms Samuel has the authority to request supplies and then places an order for additional supplies. The new biometric system hasn't changed Samuel's experience much -- he orders supplies the same way he always did. Behind the scenes, however, the Ministry of Health has improved abilities to track orders and prevent leakage.



## Mobile ID



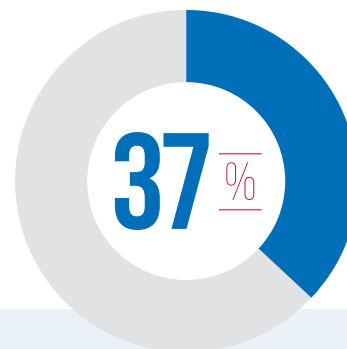
### Mobile ID

<b>What is it?</b>	<ul style="list-style-type: none"> <li>Verifying identity through an account registered with mobile network operators in place of a traditional ID card or document</li> </ul>
<b>Example use cases</b>	<ul style="list-style-type: none"> <li>Secure log-in to online accounts</li> <li>E-Gov services</li> </ul>
<b>What problems can it solve?</b>	<ul style="list-style-type: none"> <li>Inconvenience: Streamlines log-in process for end-users since they no longer have to remember separate login credentials for different user accounts</li> <li>Security: Allows for multi-factor authentication for more secure online transactions</li> </ul>
<b>What problems does it NOT solve?</b>	<ul style="list-style-type: none"> <li>Ubiquitous access: mobile authentication relies on individuals having a persistent account with a mobile network operator (MNO) and continuous access to a mobile device</li> </ul>
<b>What problems could it create?</b>	<ul style="list-style-type: none"> <li>In countries that have mandatory SIM registration requirements, people who lack other forms of official ID may not be able to establish an account</li> <li>May exclude those without access to their own mobile device</li> </ul>
<b>What is current state of play?</b>	<ul style="list-style-type: none"> <li>Mobile authentication services available in dozens of countries<sup>83</sup> (including many in Latin America and South/Southeast Asia)</li> <li>GSMA's Mobile4Development initiatives working to expand access to create enabling environment for mobile IDs to be more inclusive and linked to other services</li> </ul>

<sup>83</sup> <https://www.gsma.com/identity/mobile-connect-deployment-map>

Mobile phones have become an increasingly significant part of identity system infrastructure. For example, mobile phones can provide a mobile “enrollment” option for traditional birth registries.<sup>84</sup> They can serve as a physical token that offers an additional authentication factor to digital identity schemes. Call records, mobile money transactions, and other digital transactions made on feature and smartphones can be leveraged as attestations of one’s identity. Mobile phones can serve as a secure device on which to manage copies of official identity documents.<sup>85</sup> In this section, we focus specifically on the trend of mobile authentication platforms, in which mobile network operators verify individual identity using their registered mobile numbers.

Mobile authentication platforms are typically developed by mobile network operators (MNOs), and can integrate with existing ID systems or serve a complementary role. One of the largest Mobile ID platforms today is GSMA’s smartphone-based Mobile Connect platform.<sup>86</sup> Mobile Connect is designed to offer a single sign-on service that works across mobile operators and service providers. One key element of Mobile Connect is an interoperability layer that connects online vendors and MNOs rather than requiring them to build connections to each other. Mobile Connect was developed in part to strengthen the digital economy by facilitating secure online transactions.



**In emerging and developing countries, smartphone ownership grew from 21 percent to 37 percent in the two years between 2013 and 2015**



Photo: © Dominic Chavez/World Bank

<sup>84</sup> GSMA (2016). “[Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan.](#)”

<sup>85</sup> See, for example, <https://www.yoti.com/>.

<sup>86</sup> Smartphone ownership in the developing world still lags well behind the global average of 43 percent, but it is rapidly increasing. In emerging and developing countries, smartphone ownership grew from 21 percent to 37 percent in the two years between 2013 and 2015. Although significant gaps remain, the rise of smartphone ownership opens possibilities for more widespread use of mobile authentication systems. Poushter, J. (2016). “[Smartphone ownership and Internet Usage Continues to Climb in Emerging Economies But advanced economies still have higher rates of technology use.](#)” Pew Research Center.

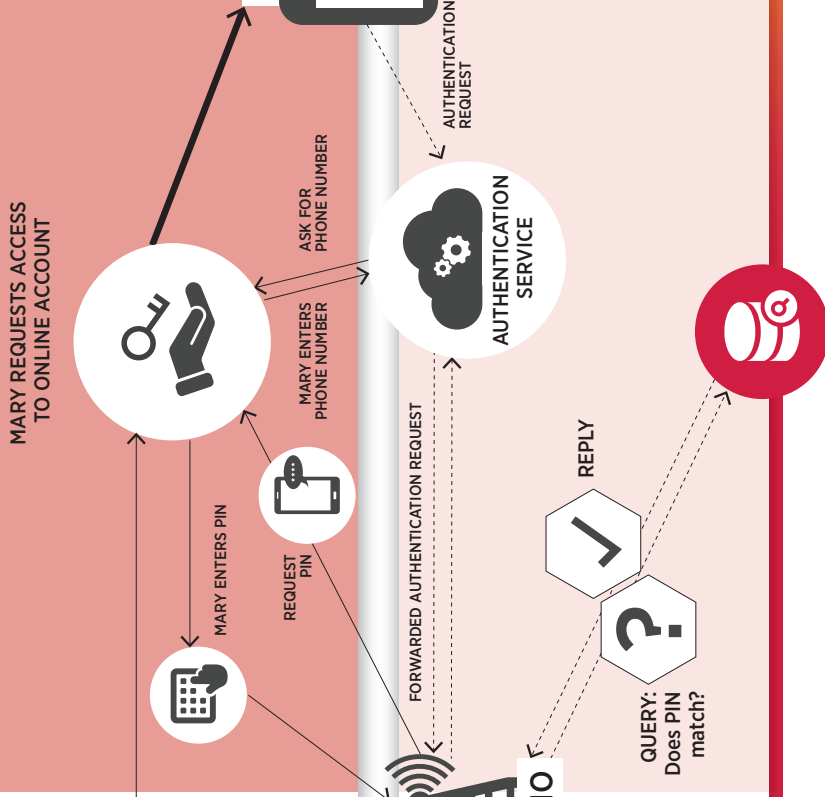
## Mobile ID Value Chain

Mary is a shopkeeper and a sophisticated smartphone user. When she purchased her phone she had to register her SIM card using her official ID. She's started ordering supplies for her shop with an online vendor who lets her create an account to save her shipping and payment information. Mobile authentication can help people like Mary engage in this kind of online activity more seamlessly.

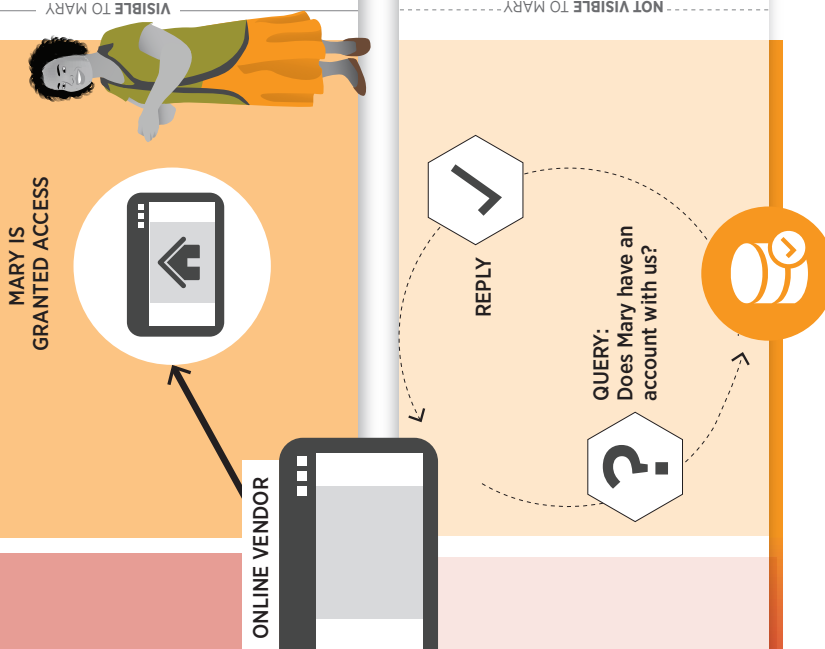
### ENROLLMENT IS THIS MARY'S PHONE?



### AUTHENTICATION DO MARY'S CREDENTIALS MATCH WHAT WAS ISSUED?



### AUTHORIZATION IS MARY A RETURNING CUSTOMER?



#### ENROLLMENT DATABASE (Owned by MNO)

Mary is placing an order one day and sees an icon offering a new way to log in. She taps on it and receives a text message from her mobile network operator (MNO) inviting her to sign up for the mobile authentication service. She is prompted to enter her phone number and some personal information on the authentication service's online application. Mary's MNO sends a message to her phone with a verification code. By entering it, Mary has confirmed that she is the owner of the device. The app prompts her to create a PIN, which is sent to the MNO and linked to her account.

#### AUTHENTICATION DATABASE (Owned by MNO)

The next time Mary wants to place an order online, she taps on the icon for the mobile authentication service and is prompted to enter her phone number. After entering her phone number, the mobile identification service provider identifies Mary's MNO, and the MNO sends Mary a request for her PIN. Mary enters the PIN she created when enrolling. The MNO confirms that Mary's PIN is correct, and the mobile ID service routes the MNO's confirmation back to the online vendor. The mobile authentication service functions as an interoperability layer, ensuring that online vendors can work with any participating MNO and that MNOs don't have to share customer information with vendors. Mary only has to remember her phone number and a single PIN.

#### AUTHORIZATION DATABASE (Owned by online vendor)

Now that Mary's identity has been confirmed, the supplier finds Mary in its customer database. She can access her shared shipping and payment information and proceed with her order. Because this service enables multiple factors of authentication (e.g., physical tokens, PINs, linkage of SIM to official credential), it could potentially be used for higher security applications like online banking.

## Convenience to end-users

Mobile authentication platforms prioritize convenience to individual users. Rather than needing to remember multiple passwords or carry a stack of ID cards, ID users can authenticate securely with a mobile phone. Because the physical token of a phone can be combined with other factors of authentication, such as PINs, passwords, and biometric capture, mobile authentication platforms are capable of multi-factor authentication. This allows them to offer a higher level of assurance than web-only authentication platforms like Google Connect or Facebook Connect, which do not use physical tokens.

In some systems, such as Estonia's Mobiil-ID<sup>87</sup> identity credentials (e.g., private keys) are stored on a secure SIM card. Private tokens sent during authentication (i.e., a PIN) are encrypted and associated with the physical device (the public token). This requires an added step of registering for a specific SIM card, but caters to industries

that require high levels of assurance, such as banking. Mobile-ID ties in to Estonia's extensive e-government system through an interoperability layer called X-Road, which standardizes interfaces between ID-reliant services and ID data sources.

## Implications for inclusion

Mobile IDs still require an initial account with an MNO, many of which have mandatory SIM registration policies.<sup>88</sup> If an official ID is required to register a SIM card, mobile IDs may not be accessible to those who lack official credentials. One clear advantage of mobiles, however, is that they offer a built-in authentication platform. Increasingly, mobile phones are a platform for fingerprint, voice, and facial recognition. Using mobile phones in place of dedicated hardware may be a more affordable way to bring biometric authentication into developing country contexts.



**Rather than needing to remember multiple passwords or carry a stack of ID cards, ID users can authenticate securely with a mobile phone.**

Photo: USAID

<sup>87</sup>e-Estonia.com. "Mobile ID" Accessed May 4, 2017.

<sup>88</sup>GSMA (2016). "Mandatory registration of prepaid SIM cards: Addressing challenges through best practice."

## Algorithmic ID



### Algorithmic ID

<b>What is it?</b>	<ul style="list-style-type: none"> <li>Analysis of a digital footprint to make inferences about a person's identifying characteristics, such as demographics (for authentication) or even creditworthiness (for authorization)</li> </ul>
<b>Example use cases</b>	<ul style="list-style-type: none"> <li>Authentication; Alternative credit-scoring</li> </ul>
<b>What problems can it solve?</b>	<ul style="list-style-type: none"> <li>Authentication: Provides an alternative method for people who lack official ID</li> <li>Credit scoring: Assessments of credit-worthiness for those with no formal credit history</li> </ul>
<b>What problems does it NOT solve?</b>	<ul style="list-style-type: none"> <li>Authentication: Provides an alternative method for people who lack official ID</li> <li>Not currently an "official" ID</li> <li>Users may choose to opt in or opt out, but do not have control over what personal data are used to make inferences about them</li> <li>Likely a complement to official ID systems, not a substitute</li> </ul>
<b>What problems could it create?</b>	<ul style="list-style-type: none"> <li>Opacity: Algorithms are not always transparent about which factors influence outcomes; this makes it difficult for end-users to know how to improve score</li> <li>Unauthorized use: Without privacy protections, judgments could be made without individual knowledge or consent</li> <li>Bias: Data used to train algorithms may not be representative of the population being evaluated; this leads to unreliable results</li> <li>Exclusion: Will exclude individuals who have not had opportunity to create digital footprints</li> </ul>
<b>What is current state of play?</b>	<ul style="list-style-type: none"> <li>Credit scoring apps widely used in some countries; regulatory environment still developing</li> <li>May be most useful for private sector actors trying to deliver services to populations who may lack official ID</li> </ul>

Algorithmic IDs can verify identity claims in the absence of official credentials. While predictions of character and characteristics are not a substitute for official ID, they may enable access to services that historically required official ID. When people have a digital presence but lack an official ID, analysis of their online behavior could be the beginning of an accretionary ID that over time gains acceptability for authenticating identity and authorizing services.

When a person's digital traces are collected and analyzed by MNOs, social media companies, or online merchants, a digital profile can be constructed without the subject's knowledge or consent. This situation is similar to passive biometric collection, and many of the concerns are the same. In particular, algorithmic ID runs the risk of being opaque and extractive. Users may not have options for redress when algorithms make mistakes. In addition, even in models where a user chooses to "opt in" to algorithmic ID services, it's often unclear exactly what a person is agreeing to share with providers.



Mass surveillance and automated processing bring clear dangers of privacy violation and repression. One example of an opaque ID system at massive scale is China's planned "Social Credit System."<sup>89</sup> The proposed system would create an algorithmic credit score for each of China's 1.4 billion citizens, in conjunction with a national ID card. Scoring would include not only financial information, but also criminal records, consumption patterns, and social connections. Proof-of-concept models are being developed by Chinese tech firms such as Sesame Credit (a subsidiary of Alibaba). Sesame's system is integrated with Baihe, a popular dating app, and a mobile game encourages users to guess friends' scores and share their own broadly.<sup>90</sup> This kind of incentivized sharing raises concerns about "horizontal surveillance," a concept explored in more detail below.

### Algorithmic authentication

Algorithmic authentication requires that individuals have a pattern of activities in their digital history against which their asserted identity can be matched. This is similar to credit card theft prevention services that watch for atypical purchases. Algorithmic analysis can also influence authorization by informing decisions about what services a person should be able to access, thus creating service-oriented "slices" of a person's identity.

The credit-scoring and verification company Lenddo offers a verification<sup>91</sup> service in which users submit biographical data (e.g., name, birthdate, employer, email) and an authentication algorithm returns a result of "verified,"

"not verified," or "unable to verify" for each piece of information. This service is intended to facilitate online transactions by engendering trust that online users are who they claim to be.

### Algorithmic credit scoring

Algorithmic credit scoring allows lenders to make credit determinations based on data from one's digital footprint rather than formal credit histories. Applicants are required to opt in at the point of accepting the service in order to share their data (generally collected through a smartphone).

But the inner workings are opaque. A recent video by Lenddo<sup>91</sup> depicts 12,000 variables being collected from a digital footprint and condensed into a single number. Similarly, the Philippine startup Ayannah<sup>92</sup> provides a credit score for undocumented and unbanked consumers using data from bill payments, mobile top-ups, and social media. Another startup, Tala, uses consistency of movement patterns, stability in key relationships, and diverse contact networks as strong repayment predictors.<sup>93</sup>



Algorithmic credit scoring allows lenders to make credit determinations based on "alternative data"—data from one's digital footprint—rather than formal credit histories.



Algorithmic authentication requires that individuals have a pattern of activities in their digital history against which their asserted identity can be matched.

<sup>89</sup> Hatton, Celia (2015). "China 'social credit': Beijing sets up huge system" BBC News, October 26, 2015.

<sup>90</sup> Obemma et al. (2015). "China rates its own citizens - including online behaviour," De Volkskrant April 25, 2015.

<sup>91</sup> Lenddo Verification. <https://www.lenddo.com/products.html> Omidyar Network (2016). "How Does Lenddo Work?" Accessed May 2017.

<sup>92</sup> <http://www.ayannah.com/>

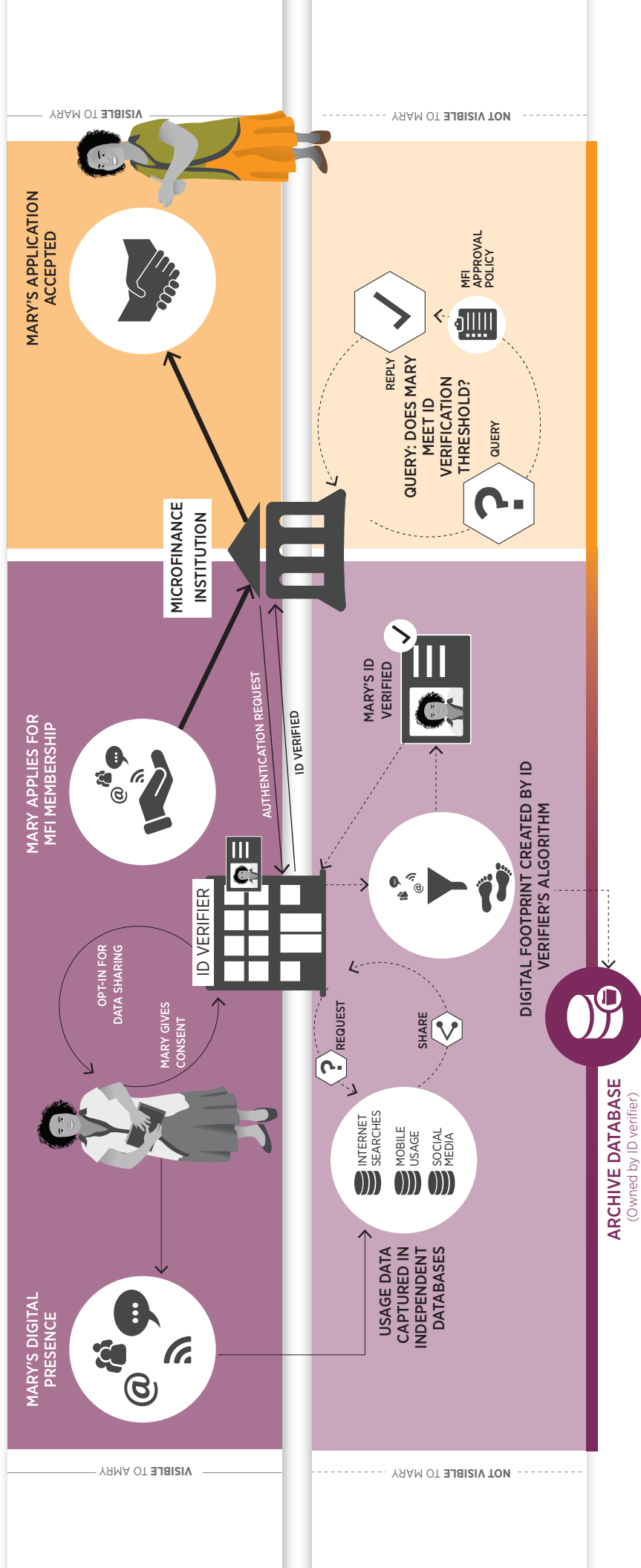
<sup>93</sup> Siroya, Shivani (2016). "A Smart Loan for People With No Credit History (Yet)" TED2016. Accessed May 2017.

## Algorithmic ID Value Chain

Mary is a shopkeeper who recently found out about a microfinance institution (MFI) that could help grow her business. She can sign up with the MFI by accessing an online application through her smartphone. Before offering access, the MFI needs to verify Mary's identity. Algorithmic ID authentication may make it possible for people like Mary to have their identity verified online, using their online presence in place of traditional ID documentation.

### OPT-IN & AUTHENTICATION

CAN WE IDENTIFY MARY BASED ON HER ONLINE PRESENCE?



Having a smartphone has been great for Mary's business. She has used it to advertise through social media, to search for information, and to communicate with clients. This hasn't required any identity proofing - Mary just accepted some terms of service for her online accounts and began interacting in the digital world. Over time, though, her online activity has come to say a lot about who Mary is.

When Mary first heard about the MFI, she visited their website and clicked on the button to join in. Instead of asking for traditional ID credentials, the site directs Mary to an ID verification company to verify her identity online. The ID verification company (IDVC) asks Mary to fill out an application stating who she is - her name, date of birth, where she lives - and then asks Mary to "opt in" with a terms of service agreement. The agreement

explains that Mary is allowing the IDVC to access personal information about her from various sources - for example, her social media company and her Mobile Network Operator. Mary's not sure exactly what data she'll be sharing or what will be done with it, but proceeds with the service in the hopes of having more finance options.

The IDVC queries Mary's digital information, creating a "digital footprint" that draws on multiple data points and uses a proprietary algorithm to confirm Mary's asserted identity. If Mary's online activities have generated enough data to verify her identity claims, the process will return a result indicating which aspects of Mary's identity are verified. The IDVC shares the result of the process with the MFI and archives the result for their records.

Once the result of the verification process is sent back to the MFI affirming Mary's identity, the MFI decides whether to proceed with her application. If the MFI proceeds, Mary will have access to microfinance options without having had to leave her shop or show an official identity. If there is an inconclusive output or insufficient data about Mary to verify her claims, however, Mary will have to prove her identity another way.



With today's lending environments, financially literate customers know that late or missed payments, defaults, bankruptcies, and similar financial slip-ups will negatively affect credit scores. When an algorithm relies on non-financial data, however, even well-informed customers may not understand how it works. If it is difficult to know what will affect credit scoring, people may be less able to manage their scores by adjusting behavior:

This opaque assimilation of information from multiple sources also has significant privacy implications. Without knowing specifically what data are being shared or sold, a user is unlikely to fully appreciate potential privacy harms. Given the richness of insights that can be gleaned from patterns like social media usage, social networks, or purchase patterns,<sup>94</sup> this is especially alarming.

The opacity of algorithmic decision making can also impede enforcement of anti-discrimination laws. For example, lenders might be legally prohibited from directly considering an applicant's gender or ethnicity, but these attributes could be inferred indirectly from personal data. The opaque nature of the algorithm does not allow for direct accountability and oversight mechanisms to intervene.

In these examples, the company developing the algorithm assumes the task of authorizing people for credit. Although financial institutions still make the final decision, they rely on the algorithm to predict repayment and mitigate lending risk. Trust in an algorithm substitutes for prior lending history that otherwise forms the basis of a credit score.

The analysis of digital footprints to uniquely identify people can enable new types of ID systems. Algorithmic analysis offers an alternative method of authenticating individual identity and authorizing services that require some level of confidence about a person's character. If such services become widespread, they could serve as a complementary onramp to official ID and inclusion in the formal economy. They also present unique privacy and transparency concerns that must be better understood if we are to establish trust in these new forms of ID.

<sup>94</sup> Electronic Privacy Information Center (2017). "[Privacy and Consumer Profiling](#)."



Photo: Bobby Neptune/USAID

## Blockchain-Backed ID



### Blockchain-Backed ID

<b>What is it?</b>	<ul style="list-style-type: none"> <li>Blockchain-backed ID can refer to: <ul style="list-style-type: none"> <li>An accretionary ID, where an identity is built up over time through a series of transactions stored on a blockchain and verified by others</li> <li>Use of a blockchain-based distributed ledger platform as the back-end database for a more traditional ID system</li> <li>Use of a blockchain-based distributed ledger platform to log transactions linked to a previously established identity</li> </ul> </li> </ul>
<b>Example use cases</b>	<ul style="list-style-type: none"> <li>Economic ID: Provides a permanent, accessible record of transaction history</li> <li>Humanitarian cash transfers: Eliminates opportunities to falsely claim assets to which someone else is entitled</li> <li>Land titling: Securely maintains important records</li> </ul>
<b>What problems can it solve?</b>	<ul style="list-style-type: none"> <li>Resilience: Blockchain records are permanent and accessible from any participating node, offering protection from destruction and loss</li> <li>Persistence: Blockchain records are very difficult to alter; this protects data integrity</li> <li>Corruptibility of Centralized Authority: Democratizing reading and writing to database bypasses role of institutions</li> </ul>
<b>What problems does it NOT solve?</b>	<ul style="list-style-type: none"> <li>Data Validity: Any documents or assets stored using blockchain need to be verified through other means; the integrity of the data is only protected after it is entered</li> </ul>
<b>What problems could it create?</b>	<ul style="list-style-type: none"> <li>Users may not anticipate consequences of permanently storing encrypted information publicly</li> <li>Disruption of traditional role of institutions</li> <li>True understanding of how blockchain technologies work may be held by a select few; may require most people to “trust” a small pool of experts to protect their interests</li> </ul>
<b>What is current state of play?</b>	<ul style="list-style-type: none"> <li>Several international development actors are experimenting with blockchain technologies; applications underlying humanitarian benefit transfer are most closely aligned with identity solutions and</li> <li>There are many start-ups offering blockchain based identity solutions, none yet at scale</li> </ul>

A blockchain<sup>95</sup> is a shared database distributed across networked computers (referred to as nodes). Similar to document-sharing platforms like Google Docs, multiple users can make additions to a blockchain in real time. Unlike a shared spreadsheet, however, a blockchain is an immutable ledger. Once an entry has been made, future additions are valid only if the preceding entry remains unchanged. Due to this distributed transaction record, it is impossible for any actor to change information without others knowing. This feature of incorruptibility is key to blockchain's security, and allows not-yet-trusted parties to maintain a trusted record of their transactions.

Blockchain technology provides an inherent openness; each node has a copy of all ledger entries. This is not a vulnerability; there is no single actor with the authority to change the "open" information on a blockchain. Many systems, such as the blockchain behind the Bitcoin cryptocurrency, are "public." This means that no central authority grants permission to write to the blockchain. In a public blockchain, anyone can set up a new node and the ledger is visible to anyone. A blockchain can also be "private," meaning that only an approved set of trusted nodes can write to the ledger. For private blockchains, the ledger can be either visible to the public or restricted to network members.

Finally, blockchain allows for distributed vetting. An entire virtual community is involved in writing, maintaining, and governing a blockchain. Because any permissioned participant can write to the blockchain, all of them share responsibility for ensuring that new entries are valid. Any submission to the blockchain is retained only if a majority of nodes agree to its validity—the system's integrity depends on "honest" nodes outvoting sloppy or malevolent ones. This could shift our historical reliance on central ID authorities and introduce a wide range of non-traditional actors into the DID ecosystem.

"Blockchain-backed IDs" could refer to pseudonymous identity linked to an existing blockchain. Users of Bitcoin, for example, already have a pseudonymous blockchain ID,

in the form of addresses that can send and receive funds. There are, however, a number of more robust ways for blockchain to intersect with the DID value chain.

Blockchain could replace or complement the databases used for enrollment. Blockchain systems are particularly suited to transactional data where timing is important and tampering could cause significant harm. For example, Estonia recently contracted the blockchain startup Guardtime to secure patient healthcare records.<sup>96</sup> Estonians can access their health records by logging in with a national ID card, and users never see the underlying blockchain. Behind the scenes, this system makes it impossible for changes to the record to be made without notice, improving security and transparency.

One much-discussed feature of some blockchain technologies (particularly those based on Ethereum<sup>97</sup>) is "smart contracts." Also known as self-executing contracts, these are pieces of code whose execution can be triggered by a financial transaction (much like a vending machine), and can in turn launch new transactions. Proposed applications include refund agreements, escrow, insurance, and pull supply chains. In a blockchain-based ID scheme, smart contracts could be used to transparently automate aspects of enrollment quality control, database updates, authentication, and authorization.

## Democratizing enrollment

Distributed ledger technologies like blockchain have potential to democratize enrollment. This could lead to systems in which many actors, not just a central ID issuer, could be trusted to enroll new users by writing their information to a blockchain.

This trust is based on the ability of other nodes to check the quality of newly proposed IDs. Credentials could be checked against a copy of the identity blockchain stored on any node of the network, rather than submitted to a central database for verification. This allows authentication to be decentralized as well.

<sup>95</sup> Narayanan et al. (2016). "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction." Princeton University Press.

<sup>96</sup> Williams-Grut, Oscar (2016). "Estonia is using the technology behind bitcoin to secure 1 million health records." Business Insider, March 3, 2016.

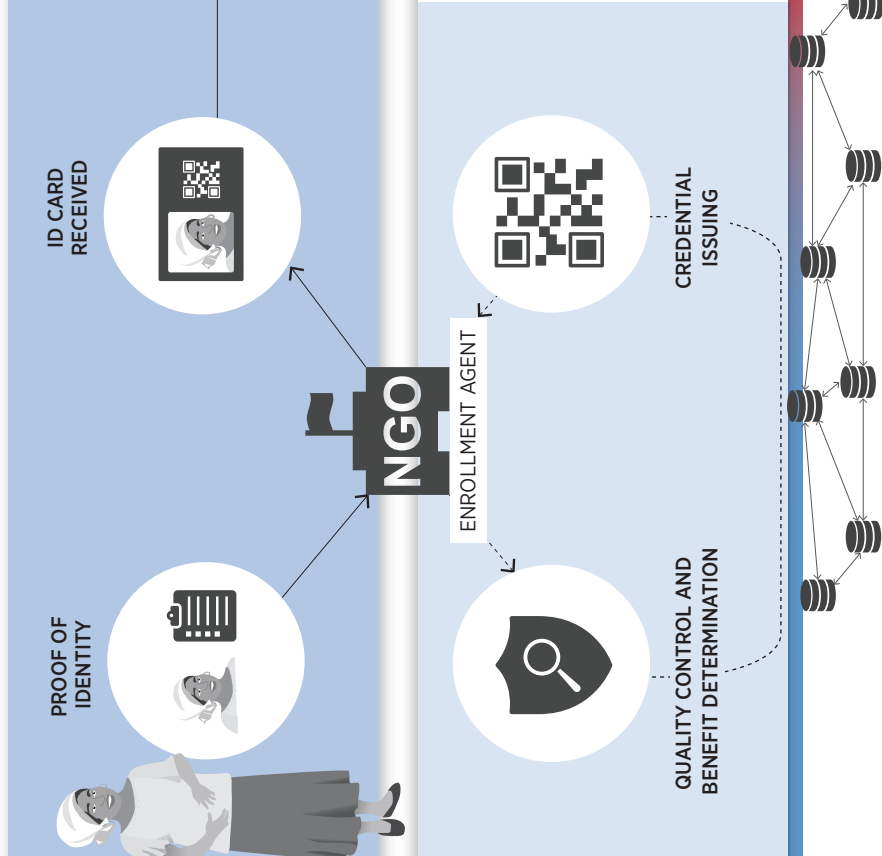
<sup>97</sup> <https://www.ethereum.org/>

# Blockchain-Backed ID Value Chain

Joy is a smallholder farmer whose rural town has just been struck by an earthquake. Her home was damaged, and she has no way to get in touch with family members who could help her out. She's temporarily taking shelter in a camp set up by a humanitarian NGO. They have recently started a new ID system for food aid recipients, aiming to reduce fraud and ensure that benefits are received by the right people.

## ENROLLMENT

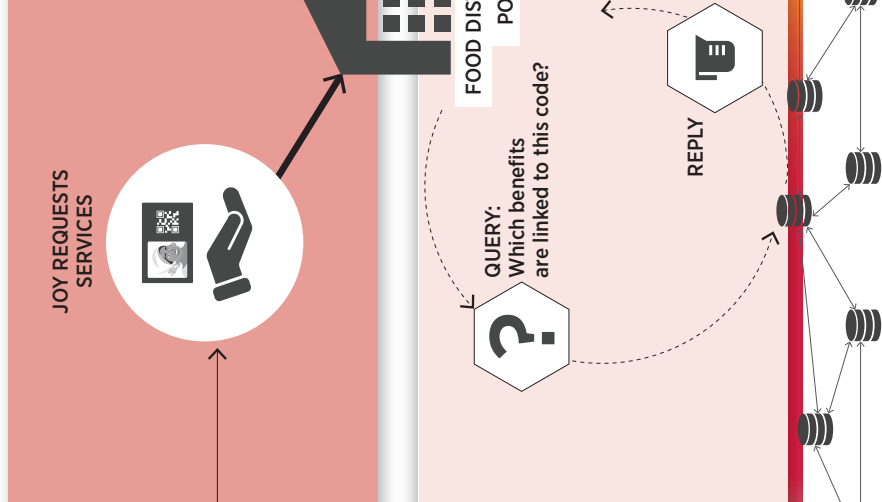
WHO IS JOY, AND HAVE WE SEEN HER BEFORE?



When Joy arrives at the camp, she stands in line to be interviewed by an enrollment agent. The agent works for a humanitarian NGO that participates in a shared blockchain ID system -- several organizations are operating enrollment points at different locations. She gives her name, birthdate, and other personal information. She also agrees to share her information with the Find-My-Relatives service that would enable anyone who knows those pieces of personal information to locate her. They take her picture and print a card with the NGO logo and a QR code on it. When scanned, the QR code translates into a unique personal identifier. A digital record is created linking Joy's identifier to the food ration quantities which she is entitled to receive. Joy's personal information is stored as a cryptographic hash. This means that people who already know Joy's information can confirm whether it is there, but others can't see it. This enrollment record is posted to a distributed database -- a private blockchain -- that is stored on a peer-to-peer computer network. A private IT company has been contracted to set up the network and onboard participating organizations, and all of the relief organizations involved in the earthquake response can write to the private blockchain.

## AUTHENTICATION

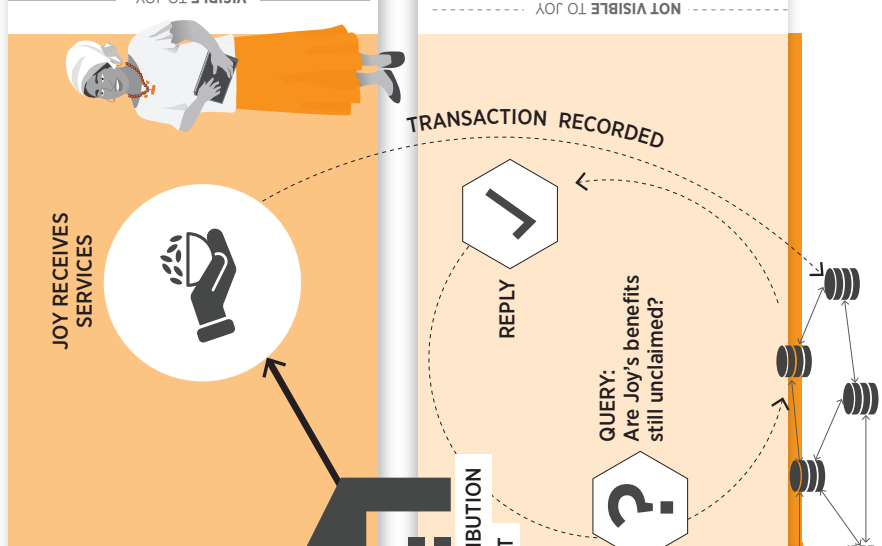
DO JOY'S CREDENTIALS MATCH WHAT WAS ISSUED?



Joy then gets in a different line, for food distribution. When she reaches the front, an aid worker scans Joy's QR code to obtain her personal identifier. The aid worker's computer then queries the blockchain and retrieves her current ration allotment and a face photo for visual confirmation

## AUTHORIZATION

CAN JOY RECEIVE SERVICES NOW?



The blockchain also contains an immutable record of every food aid disbursement linked to Joy's ID. While food distribution points across the area are managed by different NGOs, they all publish transaction records to the same blockchain. The aid worker checks to make sure that Joy's benefits haven't been collected from any of the other sites today. Once this has been confirmed, Joy gets her food ration.

One unavoidable feature of the current blockchain landscape is hype.

For example, a blockchain-backed ID scheme could involve private-sector enrollment agents. These agents would collect personal data, create new IDs, and publish them on a blockchain network. Sensitive information (such as biometric templates) would be encrypted with a private key before publication. When a service provider agrees to adopt a blockchain-backed scheme and seeks to authenticate an ID in that scheme, any copy of the blockchain could be queried to obtain encrypted credentials. Token validity can then be confirmed using a match-on-card scheme (See “Digital ID Systems: How they work”).

## Humanitarian use cases

Several applications of blockchain-based identity systems have emerged in the humanitarian sector. For example, BanQu is a startup that allows users to build an identity through (non-cryptocurrency) mobile money transactions. Their model is similar to algorithmic credit scoring, except that instead of relying on a trusted algorithm that ingests digital footprints, BanQu uses a blockchain to substantiate new digital traces. With the right enabling environment, these accreted identities could unlock credit, meet KYC requirements, or potentially even serve as a gateway to formal ID.

BanQu has piloted their economic IDs with a group of refugees in Kenya in the hopes of transforming economic activities associated with their refugee status (e.g., cash transfers, remittances) into a trusted, portable record of financial activities that they can use to access financial and social services in the future. In this case, the openness and immutability of the blockchain platform is intended to encourage formal institutions to trust people who otherwise may lack credit histories and official identification.

Blockchain technology is also being used to improve the efficiency and security of humanitarian cash transfer programs. WFP’s Building Blocks<sup>98</sup> project piloted and

continues to implement a blockchain-backed platform to track the redemption of cash benefits by more than 10,000 Syrian refugees in Jordan. This system allows WFP to have a transparent, secure, and trusted record of how benefits are spent, lowering potential for misuse and creating cost-savings for WFP. The Building Blocks project uses a private fork of the Ethereum blockchain, allowing WFP to control who participates in their system, while leveraging the existing protocol of a public blockchain.<sup>99</sup>

Other efforts also exist. For example, AID:Tech is a startup company that uses blockchain to provide a shared record about who received aid. AID:Tech’s product is a standalone ID scheme in which an aid organization enrolls eligible beneficiaries, issues a card with a QR code, and links each unique code to a set of benefits. The beneficiaries can then use the card at local markets to authorize distribution of benefits associated with their card, and these distributions are tracked in near real time on a distributed ledger platform. This application uses a blockchain platform to bring transparency to the authorization process. Blockchain-backed ID solutions like these could help donors and humanitarian implementers to trust their partners by making aid distribution more transparent. Using blockchain-backed ID in settings plagued by corruption and uncertainty could reduce risk for donors and service providers, yet requires strong connectivity to realize near-real time transparency.

One unavoidable feature of the current blockchain landscape is hype. Well-managed hype may help to build political support (at least in the short run), but inflated expectations can collapse into disappointment and suspicion that undermine future progress. As with all emerging technologies, it will remain important to evaluate the practical performance of blockchain-backed systems and evaluate where they truly perform better than alternative systems.

<sup>98</sup> <http://innovation.wfp.org/project/building-blocks>.

<sup>99</sup> <https://aid.technology/>.



## User-Controlled ID



### User-Controlled ID

<b>What is it?</b>	<ul style="list-style-type: none"> <li>An approach rather than one technology</li> <li>Increases individual control over identity information, management, and sharing</li> </ul>
<b>Example use cases</b>	<ul style="list-style-type: none"> <li>DigiLocker, Yoti, Sovrin and Hyperledger Indy<sup>100</sup></li> </ul>
<b>What problems can it solve?</b>	<ul style="list-style-type: none"> <li>Allows users to share only data needed and no more, better preserving privacy</li> </ul>
<b>What problems does it NOT solve?</b>	<ul style="list-style-type: none"> <li>Requires high levels of digital literacy and ability to manage personal data</li> <li>Policy/regulatory environment may not provide sufficient protections for users (e.g., clear definitions of data ownership, means of recourse in the case of data loss or breach)</li> <li>Clear standards to judge the reliability of a self-asserted ID in terms similar to institutionally granted IDs</li> </ul>
<b>What problems could it create?</b>	<ul style="list-style-type: none"> <li>Significant and poorly understood dependencies (e.g., digital infrastructure, digital literacy)</li> <li>Inefficient or ineffective investment in a premature technology solution</li> </ul>
<b>What is current state of play?</b>	<ul style="list-style-type: none"> <li>There are several apps that incorporate elements of user-controlled systems catering to high-income contexts, generally very early stages</li> <li>To our knowledge, there are no examples of fully user-controlled systems to date</li> </ul>

<sup>100</sup> <https://digilocker.gov.in/>, <https://www.yoti.com/>, <https://sovrin.org/>



Photo: Guimba Souleymane, International Red Cross Niger.





Photo: Simone D. McCourtie / World Bank

In our discussion of the original ID value chain (Figure 3), some elements are directly visible to the ID holder. Enrollees volunteer their credentials and receive ID tokens in return. ID users present tokens for authentication and receive a service in return. Processes such as enrollee deduplication, data storage, and authentication queries, however, all happen outside the ID holder's view. User-controlled ID aims to give some of these "invisible" elements back to ID users. It involves a spectrum of options that may let users choose what data they provide at enrollment, where it is stored, or how authentication requests should be handled.

Several examples illustrate this nascent move toward greater user control, including India's DigiLocker<sup>101</sup>, the U.K. startup Yoti<sup>102</sup>, uPort<sup>103</sup>, the Open Mustard Seed framework<sup>104</sup>, Sovrin and the Hyperledger Indy project.<sup>105</sup> DigiLocker provides Indians with 1 GB of cloud storage to securely store digital copies of personal documents. Government agencies can issue documents directly to DigiLocker. Agencies can also access needed documents directly, rather than requiring people to bring paper copies to government offices. Any access activity is logged and shared with the user. Users can upload, e-sign, and share documents of their own choosing, enabling usage of DigiLocker as a more general-purpose data-sharing platform.

In Yoti's smartphone app, users begin a profile by taking a selfie and link the profile to an official ID. They can then selectively share certain attributes with others. For example, a user might share her age with a bartender but conceal her name and address. Like DigiLocker, Yoti is a hybrid of the state-led systems that have historically shaped ID and an emerging trend of increased user control. It relies on an official ID to support user profiles, but increases user agency by allowing custom attribute management.

Open Mustard Seed, uPort, and Hyperledger Indy are all open-source projects that aim to build independent ID management systems on top of blockchain technologies. As of the time of this writing, all three appear to be in a development phase and have not yet been deployed for broad user applications.



**User-controlled ID aims to give some of the more "invisible" elements of an ID system back to ID users.**

<sup>101</sup> <https://digilocker.gov.in/>

<sup>102</sup> <https://www.yoti.com/>

<sup>103</sup> <https://www.uport.me/>

<sup>104</sup> <https://idcubed.org/open-platform/platform/>

<sup>105</sup> <https://sovrin.org/>

## User-Controlled ID Value Chain

Mary is a shopkeeper and sophisticated smartphone user. She is concerned about how much of her personal information she has to entrust to other actors just to take part in daily business activities. In the future, user-controlled IDs may give people like Mary greater control over the storage, security, and sharing of their personal information.

### ENROLLMENT

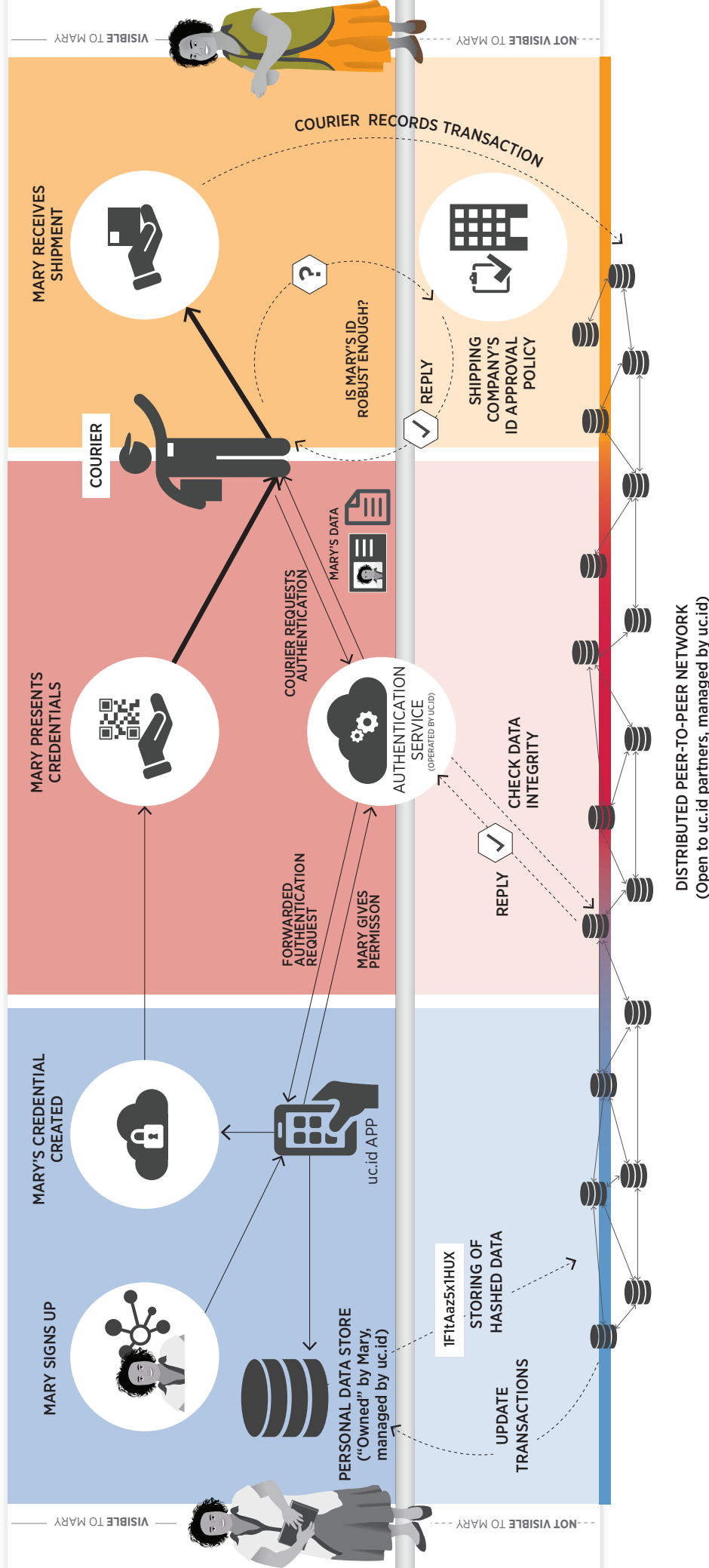
WHO DOES MARY SAY SHE IS?

### AUTHENTICATION

DO MARY'S CREDENTIALS MATCH WHAT SHE CREATED?

### AUTHORIZATION

CAN MARY RECEIVE SERVICES?



Mary learns about a new ID service called uc.id that would allow Mary, not a government or private company, to control how her ID is established and shared. Mary visits uc.id's website and sets up an account by choosing a PIN, uploading a selfie, and giving access to her social media connections as initial proof of who she is. She later decides to add her business registration and other important identity attestations. These data are uploaded to a cloud-based "personal data store" (PDS). The company claims that no one will be able to access Mary's data without her permission. A cryptographic hash of Mary's personal data is recorded on a blockchain, as evidence that her data haven't been altered. Although the PDS "belongs" to Mary, it is hosted on a cloud server owned by uc.id.

Mary's store receives a large shipment that she needs to sign for, and the shipping courier happens to accept uc.id. She opens the uc.id app on her smartphone, which displays a QR code. This QR code encodes a URL for Mary's personal data store, so that the courier's query is directed to the right place. After he scans it, her smartphone shows a notification from uc.id, prompting her to enter her PIN and asking whether she wants to accept a request for identity verification. Using uc.id allows Mary to choose which data from her PDS to share to verify her identity; this time she opts to share her photo and business registration. The uc.id authentication service queries the uc.id blockchain to be sure that Mary's PIN is correct and her stored data have not changed. The uc.id authentication service then sends Mary's photo and registration to the courier's smartphone. There is no third-party authentication database; all of the data about Mary are coming directly from her own PDS.

The courier can see her facial photo, confirming that Mary is the same person who registered for the uc.id service. Based on the registration documents, the dashboard on the courier's phone indicates that Mary is a "low risk for impersonation." The company policy is to accept any uc.id ID that meets this criterion in addition to visual confirmation. With these criteria satisfied, Mary can collect her shipment. In the future, after several more transactions are recorded on the uc.id blockchain, Mary will have established a digital reputation as someone who places regular orders with a consistent group of suppliers and pays promptly.

## New actors, evolving roles

Granting users more control over their identities is likely to introduce new actors into the ID ecosystem. Given current trends and emerging use cases, we may see greater proliferation of the personal data stores projected by some writers.<sup>106</sup> This would mean a shift away from centralized ID databases and toward cloud-based repositories to which a user would upload personal data and ID credentials of her choosing. Authentication queries would then be handled by the individual's personal database, rather than one managed by a broader ID system. Correct routing of queries would likely rely on authentication services that serve as interoperability layers, connecting services and users through a standardized interface. In many proposed schemes, a public blockchain is used to guarantee the integrity of these user-controlled data repositories. New companies or agencies would need to step into the role of hosting, managing, funding, securing, and auditing this personal ID infrastructure.

Many people will lack the ability or inclination to manage their own personal data stores. "Personal data managers" may step in to fill this gap by ensuring that content and security settings meet their clients' needs. For users who want to separate different aspects of their identities, data managers could ease the burden of juggling digital personas,<sup>107</sup> especially when interfaces are nuanced by attribute-based credentialing or conditional pseudonymity. Data management could be provided either through tailored personal service or algorithmic assistants.

If personal data are owned by individuals rather than by ID-granting institutions, some will want to sell their data. Indeed, personal data has been described as a new "asset class"<sup>108</sup> and is already contributing to private sector profits.<sup>109</sup> With greater user control, we may see the rise of "personal data brokers" and other middlemen between ID holders and data-hungry corporations. They could be joined by a new cohort of regulators, appraisers,

consumer advocates, and others seeking to protect individual or corporate interests.

## Limits on empowerment

User-controlled ID will not universally empower people. The benefits of personal data stores will depend on users' ability to access the internet and their understanding of digital tools such as cloud storage. Even if users own their data and can determine access to it, they still do not own the servers on which their data are hosted. Those servers may be subject to search or seizure by authorities in the countries in which they reside. The service operators will need to be compensated, possibly by means of user fees, data licensing, donations, or government subsidies. Finally, protection from surveillance by the system owner will require strong encryption of stored data—a tall order even for experienced internet users.

## Trend Implications

Several common themes emerge from the five trends detailed above. These include 1) balancing data protection and innovation, 2) a need for standards of identity proofing, 3) security concerns, and 4) new types of privacy concerns, like surreptitious biometric collection and horizontal surveillance. We also recognize the continuing relevance of system dynamics (e.g., political buy-in and sustainability) explored in Part I of this paper.

## Balancing data protection and innovation

One common feature of the emerging ID technology trends discussed above is personal data. All ID systems require data about people to be collected, analyzed, and stored. These data may come from financial transactions, mobile usage patterns, or novel biometrics. Some will be highly valuable, both as business assets, but as well targets for theft or surveillance. Robust data protection regulations can shield users from exploitation and limit the liability of ID technology innovators. At the same time, overly protective approaches run the risk of

<sup>106</sup> Bollier & Clippinger (2014). "The next great internet disruption: Authority and governance." In ["From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society"](#), pg. 21–28. ID3/Off the Common Books.

<sup>107</sup> Mas & Porteous (2015). "Minding the identity gaps." *Innovations* 10:1–2, pg. 31–54.

<sup>108</sup> World Economic Forum (2011). ["Personal Data: The Emergence of a New Asset Class."](#)

<sup>109</sup> Brown, Meta S. (2015). ["When and Where To Buy Consumer Data \(And 12 Companies Who Sell It\)."](#) Forbes.com.

stifling innovation rather than promoting it. Additionally, digital data protection is an evolving concept, and few effective data protection frameworks exist to learn from in a development context. Existing frameworks have been borrowed from or repurposed between distinct regulatory environments. This has led to data protection laws sometimes being adopted without enforcement resources or adequate adaptation to local context, rendering them ineffective or inappropriate in practice.

Many developing countries are currently adopting or are expected to adopt laws based on the European Union's General Data Protection Regulation (GDPR).<sup>110</sup> The GDPR defines specific rights of *data subjects* (people about whom data has been collected). *Data controllers*—people or organizations who collect, process and store these data—are required to give effect to these rights. These rights include a right to access, under which data subjects can demand to know what data about them a data controller holds, as well as how it was obtained, how long it will be stored, and the purposes for which it is being used. Upon request from data subjects, data controllers are required to correct mistakes, limit the processing of data, or delete records if consent is withdrawn. Data subjects have the right to obtain their data in a machine-readable format and transfer it to a new controller if desired. Evaluation of data subjects based on automatic processing of their data is permitted only with explicit consent and appropriate safeguards.

Laws such as GDPR set a high bar for data management practices. There are concerns that similarly prescriptive regulations could be adopted in countries that lack the local capacity for effective enforcement or widespread compliance. The passing of ambitious laws is never the end goal; regulatory reforms should always be accompanied by building local technical capacity.

Effective, locally appropriate data protection laws can help prevent serious violations of user privacy and agency. Clearly defined and enforceable individual rights are probably the surest way to protect people from digital manipulation or coercion. When people are empowered to call corporations or government agencies to account for how their data are being used, the foundations of trust in the ID ecosystem are likely to be strengthened.

We must also balance the drive to protect privacy with the benefits that can be gained from less constrained regulatory environments. The flexibility to innovate can drive economic growth and spur improved service offerings. Companies may hesitate to trust a government they see as unsympathetic to their operational concerns. To foster an environment that promotes business growth and protects individual privacy, local regulatory and legal frameworks must proportionally weigh the interests of both ID users and providers.

## A need for standards

If novel ID technologies are to be integrated into existing ID systems, we will need broadly applicable criteria for comparing the trustworthiness of different identity attributes. For example, is six months of mobility data roughly equivalent to a fingerprint? How does a 20-minute voice recording compare to a facial photograph? These judgments must be informed by research into how reliably one person can be distinguished from millions of others using a certain quality and quantity of identifying data. It will also be important to weigh vulnerabilities, with easily faked data providing a lower level of confidence. In the U.S. context, the National Institute of Standards and Technology is beginning to develop standards<sup>111</sup> for identity proofing to address the challenges arising from the growing diversity of data points that can provide evidence of identity.

<sup>110</sup> A recent global mapping of data privacy laws shows that they are by no means limited to Europe. Globally, the majority of countries have data privacy laws, and fewer than half of countries with laws are European. Growth in the developing world, particularly Africa, has been rapid. Though details vary, data privacy laws show a strong “family resemblance” and show a clear influence of European regulations.

Greenleaf, Graham (2015). “Global Tables of Data Privacy Laws and Bills.” Privacy Laws & Business International Report 133:18-28.

Greenleaf, Graham (2015). “Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority.” Privacy Laws & Business International Report 133.

<sup>111</sup> NIST Information Technology Laboratory (2015). “Measuring Strength of Identity Proofing” Discussion draft from workshop: Applying Measurement Science to the Identity Ecosystem.

As it relates to authorization, many ID frameworks allow different types of credentials to be accepted in different contexts; low-risk transactions can tolerate fairly weak identification, while higher-risk transactions require greater confidence for authorization.<sup>112</sup> This can be linked to the concept of “accretionary ID” mentioned elsewhere—as a person’s digital ID acquires higher-confidence data points, she can be entrusted with access to higher-value services. A tiered approach can present a low barrier to entry for people with few formal credentials while providing them a pathway toward greater inclusion and empowerment.

## Security Concerns

### Biometric theft

Authentication processes often rely on centralized data storehouses, which can be inviting targets for theft. Biometric data are unique because they are irrevocable—one can easily change a stolen password, but not stolen fingerprints. Inadequate protections (both legal and technical) can invite highly damaging breaches and undermine trust in biometric-reliant institutions. Measures can be taken, however, to ensure biometric revocability if digital templates are revealed or stolen.<sup>113</sup> One method, known as “salting,” involves adding random information to a digitized biometric template, so that the template is not uniquely determined by the original biometric data. Another related approach uses one-way transformations, such as cryptographic hashes, that rely on a private key held by the user.<sup>114</sup> Only the encrypted data are stored in a database. During authentication, the template presented for matching is encrypted using the same hash, and authentication is successful if the two templates match *after* encryption.

### Blockchain privacy and security

ID applications will often require private information to be stored on a public blockchain. This is typically done using public-key cryptography, where encrypted data

can only be decoded by those with a private key. Even if information on a blockchain is uninterpretable to those without the private key, they can still be confident that it has not been changed since it was added to the ledger. This turns some data management tasks into key management tasks. For example, because blockchain entries cannot be deleted, requirements to delete sensitive personally identifiable information (e.g., after a defined period of use) would be replaced with requirements to delete the private keys capable of decrypting it.

Although encryption of stored data can decrease the risk of data breaches, there can still be danger of data theft if private keys are stolen. The best approach is probably to distribute public key storage as widely as possible—for example using match-on-card architectures<sup>115</sup>—to minimize the impact of any single breach. As data ownership migrates from a centrally held “honey pot” paradigm over to a more diffuse, distributed paradigm, it is unclear how data protections and data breach liability will similarly migrate. A central authority holds responsibility when a data store in its possession is compromised. Liability for breach of information in federated or distributed systems is far less clear cut.

The public Bitcoin blockchain is widely considered to be secure, but it is possible that it could be subverted by malicious actors. Incidents such as the June 2016 hack of The DAO, an Ethereum-based crowdfunding platform,<sup>116</sup> could be very disruptive if they targeted a large ID system. Private blockchains avoid some risks, but may actually be more vulnerable if corrupt actors are allowed to participate.



**A central authority holds responsibility when a data store in its possession is compromised. Liability for breach of information in federated or distributed systems is far less clear cut.**

<sup>112</sup> See previous section “Digital Identity: An Instrumental Approach” for more information on levels of assurance.

<sup>113</sup> Boulton and Woodworth (2008). “Privacy and Security Enhancements in Biometrics.” In Ratha & Govindaraju (eds.), *Advances in Biometrics: Sensors, Algorithms and Systems*, pg. 423–445; Dev Technology Group “*Emerging Biometric Technology: Revocable Biometric Features*” (Accessed May 2017.)

<sup>114</sup> Scheirer et al. (2013). “*Beyond PKI: The Biocryptographic Key Infrastructure*” In Campisi, Patrizio (ed.) *Security and Privacy in Biometrics*, Springer.

Hao et al. (2005). “*Combining cryptography with biometrics effectively*” University of Cambridge Computer Laboratory, Technical Report Number 640.

<sup>115</sup> Bergman, Christer (2008). “Match-on-Card for Secure and Scalable Biometric Authentication” In Ratha & Govindaraju (eds.), *Advances in Biometrics: Sensors, Algorithms and Systems*, pg. 407–421.

<sup>116</sup> Popper, Nathaniel. “*A Hacking of More Than \$50 Million Dashes Hopes in the World of Virtual Currency*,” New York Times, June 17, 2016.



## Horizontal Surveillance

Privacy concerns related to digital ID have traditionally focused on a “Big Brother” scenario, in which governments or large corporations stockpile information on ordinary people. As ID becomes more integrated with everyday digital transactions and an increasing number of actors have access to information that can be informative of individual character and behavior, people may find themselves requesting more attributes of others before entering into transactional relationships with them. We may find ourselves increasingly surveilled by our peers—so-called horizontal surveillance.

For example, TrustID<sup>117</sup> is an application built on top of India’s Aadhaar system that allows users to verify the identity of domestic help or prospective employees. The developers of TrustID are hoping to integrate with criminal records, potentially allowing anyone to conduct a background check on an employee, a neighbor, or a daughter’s new boyfriend. When coupled with the digitization of reputation, horizontal surveillance could change identity from a static label applied by the state to something built by of one’s peers.



<sup>117</sup> Bhargava, Yuthika (2016). “[App to verify domestic helps, employees using Aadhaar](#)” The Hindu, March 6, 2016.



## Systems-level Implications



### Advanced Biometrics

Next-generation biometrics can have contradictory effects in the ID system. If they provide a more streamlined user interface, they could strengthen ID systems by increasing frequency of use and enabling sustainability and expansion. At the same time, passive biometric capture could increase both privacy and security concerns. Whether new biometric technologies aid or derail ID systems will likely depend on which other measures are in place to mitigate privacy concerns or political backlash.



### Mobile ID

By leveraging an authentication platform (mobile phones) that is already familiar to users and integrated into their daily lives, mobile IDs can increase the convenience of ID use. More convenient and frequent usage will make it easier for relying parties to monetize ID services, contributing to sustainability for the entire system. At the same time, reliance on mobile authentication could lead to underinvestment in other types of authentication platforms (such as card readers). Those without mobile phones could be excluded from authentication and less able to access ID-enabled services.



### Algorithmic ID

By providing new ways to access formal systems, algorithmic ID can expand inclusion, as long as concerns about digital exclusion are addressed. Algorithmic ID platforms will also need to account for cultural sensitivities; for example the acceptable balance between privacy and convenience varies across cultures. Algorithmic credit scoring and similar services can expand the suite of ID-enabled service offerings, while

the potential for data sharing could be harmed by a proliferation of proprietary systems. More troublingly, algorithmic ID can heighten fears about surveillance and privacy or undermine transparency.



### Blockchain-Backed ID

Blockchain can enable new routes for inclusion through democratization of enrollment or accretionary ID, strengthening ID systems by expanding their user base. At the same time, high demands on connectivity and digital literacy may exclude some users, undermining the system's inclusivity and usefulness. Blockchain-enabled data sharing can also increase transparency while mitigating data security risks. Blockchain can be an effective tool for data sharing with open standards, which could aid in platform development and expand relying party service offerings.

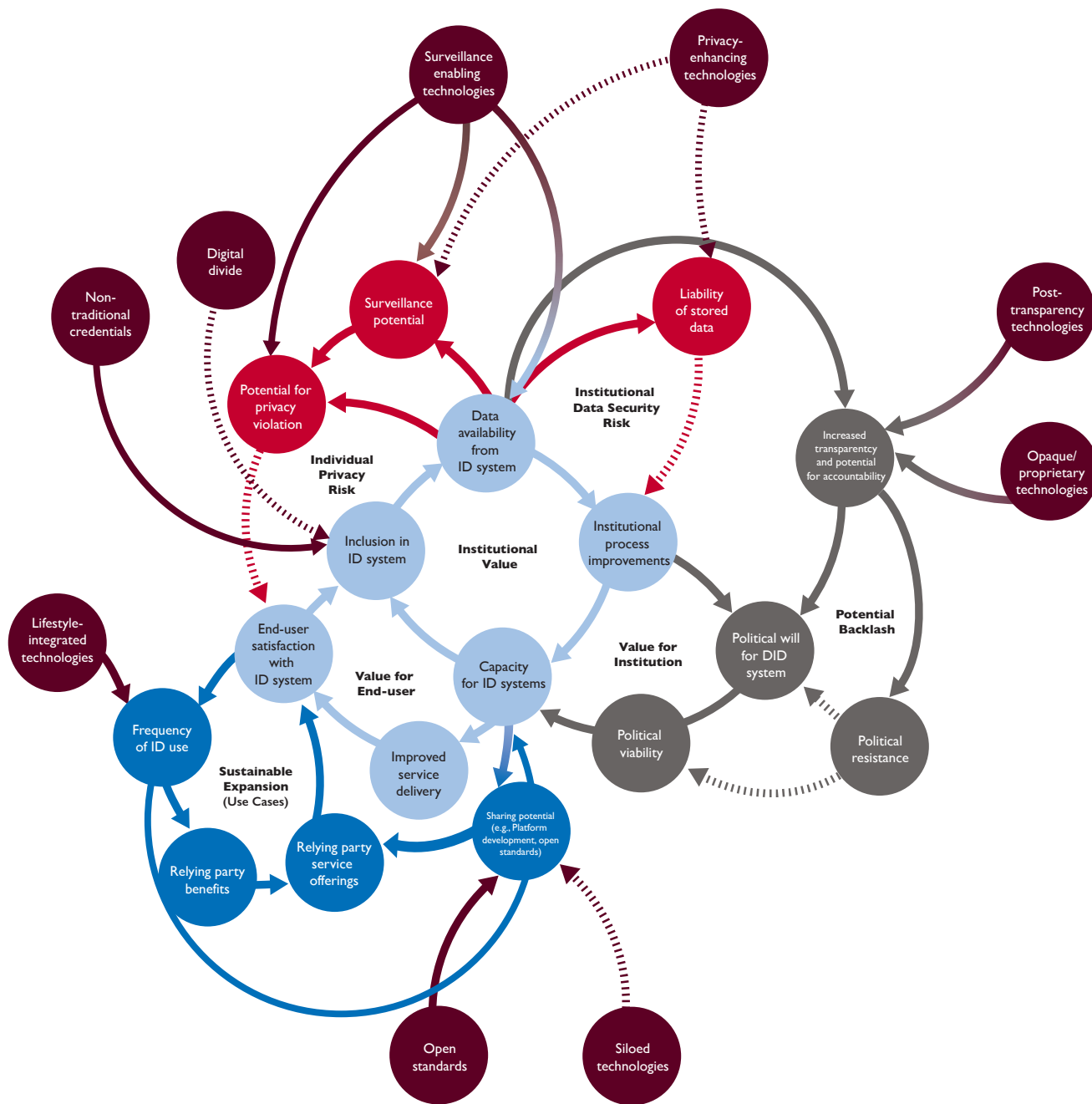


### User-Controlled ID

Increased user control has the potential to change nearly every aspect of the ID system. Like other emerging technology trends, user-controlled ID can expand inclusion by creating new pathways to identification. It can also widen existing disparities in digital access. The storage of user data in personal data stores rather than centralized databases can diminish individual and institutional privacy risks but may enable horizontal surveillance. Societies weighing the benefits of such systems will need to make policy choices about how much responsibility and risk should be centralized or dispersed.

The DID system initially presented in Part I of this report can help us understand the broader implications of these emerging trends in ID technology. At an abstract level, we can interpret ID technologies in terms of their impact

on a few key nodes in the system, particularly those related to inclusion, surveillance, privacy, transparency, and potential for platform sharing. These interpretative categories are shown in the figure below.



**Figure 24:** The above figure incorporates impacts of emerging technology trends on the digital ID system introduced in Part I. Examples of how each of the technology trends affect digital ID are provided in Table I and accompanying text [below]. An already-intricate system is poised to become even more dynamic and complex with the increased reliance, use, and incorporation of emergent ID solutions. It is increasingly important for implementers and donors to understand the complexities of the ID landscape rather than taking an instrumental, systems-blind approach.

To make things more concrete, we can assign features of different emerging ID technologies to each of these categories. The following table is not exhaustive, but

illustrates how to think about these new technologies in a systems context.

**Table 1:**  
**Categories of emerging technologies in digital identity systems**

CATEGORY	EXAMPLES
Lifestyle-integrated technologies	Improved biometric capture Mobile authentication Algorithmic authentication
Non-traditional credentials	Algorithmic enrollment Accreted ID Democratized enrollment Self-asserted ID
Surveillance-enabling technologies	Passive biometrics Algorithmic authentication Horizontal surveillance
Privacy-enhancing technologies	Mobile consent for authentication Revocable biometrics Blockchain data sharing Personal data stores
Pro-transparency technologies	Anti-spoofing biometrics Blockchain data sharing
Transparency-limiting technologies	Opaque algorithms
Proprietary technologies	Proprietary biometric platforms Opaque algorithms
Open standards	Open biometric formats Public blockchains

This kind of systems-based framework also provides a way to think through the implications of emerging ID technologies that were not included in this report. To restate, we have only considered a sampling of what is likely to emerge on the scene in the coming 5–10

years, and there will certainly be trends that we have not identified in this report. For any new or proposed technology, asking about its relationship to these key system nodes will be a good first step toward imagining its likely broader impacts.



## Key Findings

**These trends offer new opportunities for identifying the unidentified.** Traditional ID systems rely heavily on demographic data. New ID systems—whether algorithmic, blockchain-based, or user-controlled—uniquely identify and characterize people based on digital traces. This approach can reveal much more than traditional IDs. Technology-based inferences about a person's trustworthiness can enable unidentified people to gain access to things like credit, banking, or employment. Under traditional systems, these goods are accessible only after successful authentication of an official ID.

**These opportunities risk deepening the degree of exclusion of those without a digital presence.** Some of these opportunities only exist if people can create a digital footprint. This means all people must have ready access to the internet, mobile phones, social media profiles, and other forms of digital engagement. It also means they must be comfortable enough with the technology that they use it frequently enough to generate robust data. Realizing the potential of these alternative IDs will, therefore, require efforts to bridge the digital divide. We must ensure that those who currently lack official ID have access as well as sufficient digital literacy for empowering engagement.

**These exciting new techniques for identification have limitations. In the case of algorithmic ID, a subtle barrier can come from poor modeling of digital behavior.** When predictive algorithms are applied to populations that differ from the “training set,” the results will be less accurate. This can happen, for example, when an algorithmic ID provider first expands into a new, poorly understood market. Similar problems can arise when analyzing data from minority populations whose behavior may differ from the majority. Biometric systems (particularly facial recognition) can also struggle when applied to people who differ markedly from the reference population. We

must be attentive to the potential for new technologies to reinforce existing biases or create new exclusions, and put in place alternative mechanisms to ensure digital ID systems are inclusive and appropriate for the context in which they operate.

**Just as in any analog system, trust cannot be bypassed with technology.** Until we have large scale experience with new technologies in practice, we will not know precisely how well they function and what consequences they may have. Field testing of data-intensive ID technologies will be essential to quantify how much they should be trusted. Although re-training based on local data may be expensive and time-consuming, the alternative—an algorithm that doesn't work or that contributes to the marginalization of a minority population—is far worse. Staying focused on the performance of new technologies in the contexts in which we work will be critical to limit unintended consequences of adopting technology solutions.

**The fragmented ID landscape is poised to become ever more complex as emerging technologies offer alternative avenues for identification.** As major tech companies and international organizations invest in digital ID, people will have more alternatives for a useful ID system beyond what their governments offer them. This will only increase fragmentation and complexity in the ID space. Especially in contexts where the enrollment requirements of an official government ID are restrictive, alternative IDs that offer the undocumented a route to financial and social inclusion will gain traction. Harmonization, or standardization, of alternative identification provision should be a key goal of those investing in identity. 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 ensuring that privacy and individual rights are preserved.

## Recommendations and Moving Forward

A functioning digital economy hinges on the critical infrastructure of digital identity. Emerging trends in digital identity have the potential to offer more inclusive biometrics, leveraging digital footprints to identify those who lack official ID, and potentially providing individuals with more convenient, secure, and portable identification options. At the same time, the digital identity ecosystem is already complex, and these future developments will add more options, new risks, and potentially significant tradeoffs between individual and institutional interests.

In this complex systems environment, we must not underestimate the role of donors like USAID. Action or inaction by donors affects both the positive and negative aspects of these systems' utility and sustainability. Many of the systemic problems we have identified—duplicated efforts, unsustainable or exclusionary technology choices, and failure to design for reuse—can be traced back to our own procurement practices. Major funders set the agenda, and we are responsible for what we promote. Official endorsement of shared principles like the Principles for Digital Development,<sup>118</sup> Principles on Identification,<sup>119</sup> and the Principles for Digital Payments in Humanitarian Response<sup>120</sup> are all a vital first step. At the same time, understanding the practical implementation of these principles in project designs, contracts, and M&E plans lags behind.

Fortunately, there are measures the donor community can take now to improve our approach. We can promote more intentional, forward-looking decision making to protect against an even further fragmented ecosystem in the future.

### Recommendations

#### Develop guidance and a technical support framework

The donor community can combat DID system fragmentation by providing direction through a more standardized DID decisional framework that is rooted in experience. 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. In coming years, these systems will likely evolve to incorporate emerging and untested technologies like new biometrics, mobile platforms, algorithmic authentication, blockchain, and increased user control. This changing context will require donors to understand the impact of these technologies on the system dynamics affecting programming. Supporting research efforts to better understand good practices for achieving more infrastructural ID systems both at present and in the future should be a priority for greater efficiency and more accountable investments.

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

<sup>118</sup> <http://digitalprinciples.org/>

<sup>119</sup> World Bank Group and Center for Global Development (2017). "[Principles on Identification for Sustainable Development: Toward the Digital Age](#)."

<sup>120</sup> Martin, Chrissy & Zimmerman, Jamie M. (2016). "[Eight Principles for Digital Payments in Humanitarian Response](#)." Next Billion Blog.

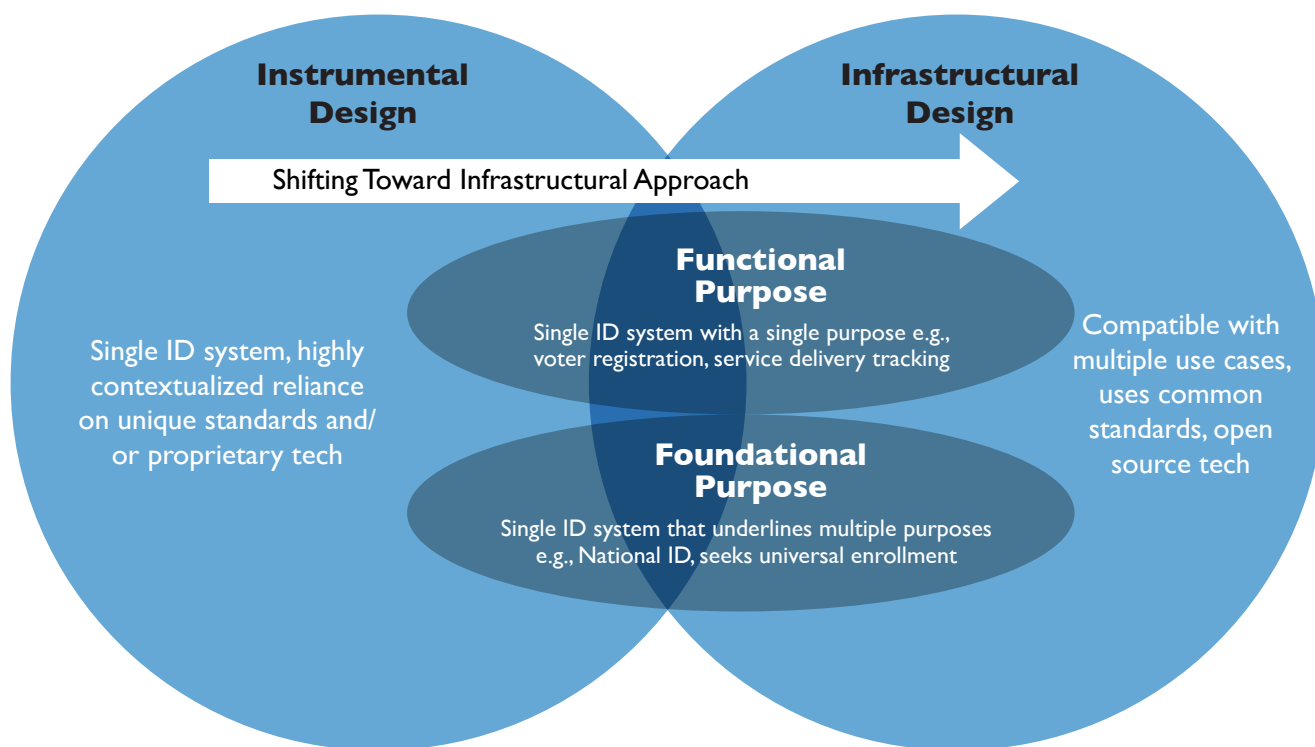
of internal guidance or technical support to draw from as they oversaw the development of DID systems. Addressing this concern should be a first step in driving toward more impactful and effective systems.

### Invest in sustainable, cross-functional DID schemes

A higher impact approach is possible through a substantive reconfiguration of our existing investment strategy in digital ID. Digital ID systems play key roles in development as rich data sources, backbones for digital economies, and tools for more transparent and efficient development programming. This will only become more true as new technologies cause more digital activities to contribute to identity formation and to depend on ID authentication. Recognizing this can help the donor

community better serve its long-term development goals and increase programmatic efficiencies. Embracing digital ID as a worthy cross-cutting initiative could allow donors to reform current fragmented strategies and allow for more meaningful development of technical expertise to draw from across the donor community.

By marshalling the resources of the donor community—inclusive of staff time, financial investments, and influence—around a unified, infrastructural investment strategy, we would move permanently away from reliance on one-time-use schemes and instead toward more durable investments. Greater consolidation of parallel efforts across the donor community could lead to significant efficiency gains and greater coherence of information across programming.



**Figure 25:** Donors can support an infrastructural approach even within the functional systems that typically underlie programmatic investments. By integrating infrastructural design choices in our support of digital ID systems, we can avoid further fragmentation of the digital ID ecosystem and create pathways to more cohesive, sustainable infrastructure that will better serve not only our programs, but ultimately the individuals they aim to serve.



More cross-functional, infrastructural identification systems would move us toward an ecosystem where open standards, open platforms, and context-relevant design practices are the norm, not the exception. Deliberate efforts should be made to partner with local government actors by default. This could promote the use of and support for country-led efforts when appropriate. When such efforts are ill-advised, a cross-cutting emphasis on ID would help donors work from a standardized playbook to assess possible mitigation and amelioration strategies. This shift in investment approach would serve multiple actors and multiple use cases and position our investments to outlive our projects.

### Mitigate privacy risks

Whether we work with government systems or build our own, donors must protect the privacy of those we serve. Although privacy-preserving strategies should be embraced far beyond just the realm of digital identity, digital identification 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. Emerging ID technologies may create greater privacy harms, with new avenues for biometric theft and surveillance. Donors must, therefore, work to mitigate the risks to privacy that our current and future DID investments create.

This can be done 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.

### Convene locally and collaborate globally

The development community has not yet fully realized the potential of digital identity. In some cases, poorly coordinated ID investments even cause harm. 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

As the development community strives to become more coordinated and more effective with our programming, it is clear that donors must take a more coherent approach to digital ID investments. Activities will likely continue to be linked to individual sectoral needs, but if we lack the technical capacity to support more coordinated, compatible investments, critical resources will be committed to limited-purpose systems. In addition, we will miss opportunities to bolster more sustainable local systems that may be naturally positioned to serve as a link across multiple development projects. Donors must work to ensure that we are instead seizing opportunities and realizing the potential of a more coherent, harmonized approach to digital identity.

Those who invest in identity systems have an opportunity to contribute to the responsible development of this space in a way that benefits both institutional effectiveness as well as the lives of individuals who have until now been left behind. To do so, donors need to recognize the ways in which new systems will impact inclusion in the digital economy, protect or compromise the privacy and security of individual data, and offer true advantages over existing alternatives. Donors must focus not only on the technologies themselves, but on how they influence broader system dynamics. Ultimately, development actors should be guided by how ID systems perform in the contexts in which we work, and their ability to balance the instrumental value they offer with their contribution to an inclusive, sustainable digital ecosystem.



