SPOTLIGHT 4

ENABLING DIGITAL DEVELOPMENT

Digital identity

Individuals need mechanisms to identify one another and to identify themselves to their communities and governments. While this point may be obvious, it is profoundly important for people's welfare. Simple mechanisms—familiarity, appearance, perhaps vouching by an elder—are sufficient in small, intimate communities. Wider societies and economies require more formal systems—traditionally physical tokens, such as a paper-based identification (ID) card that includes the signatures or representations of their holders, and is verified against documents stored in a central registry. But these formal systems are failing in the developing world. Nearly 2.4 billion people are not registered. They are usually the poorest and most marginalized members of society; about one-quarter are children.[1] They are excluded from a range of rights and services, such as health care, enrollment in school, social welfare, and financial services.

Identity should be a public good. Its importance is now recognized in the post-2015 development agenda, specifically as a Sustainable Development Goal (SDG) target to "promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels."[2] One of the indicators is to "provide legal identity for all, including birth registration, by 2030." The best way to achieve this goal is through *digital identity (digital ID)* systems, central registries storing personal data in digital form and credentials that rely on digital, rather than physical, mechanisms to authenticate the identity of their holder. India's massive Aadhaar program, which has enrolled over 950 million people, has dispensed with the physical ID card altogether. Estonia has created an electronic legal representation of an individual. Through the use of personal identification numbers (PINs) to authenticate the holder against a digital card credential, people can access public services remotely and even sign legal documents and contracts with the same legal validity as if they were signed in person.

Contributed by Joseph Atick, Mariana Dahan, Alan Gelb, and Mia Harbitz.

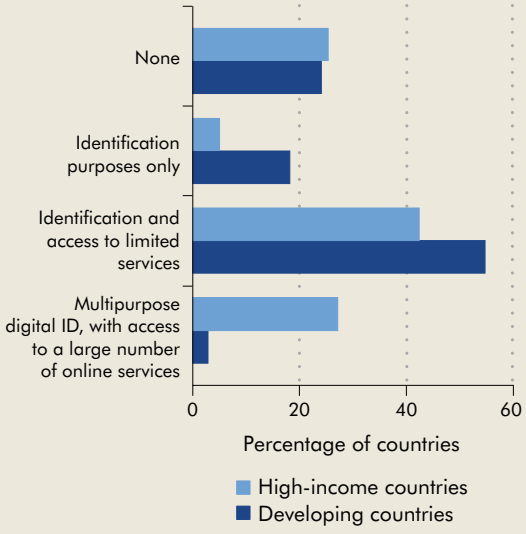
Country-specific use of digital identity

Most developing countries have some form of digital ID scheme tied to specific functions and serving a subset of the population, but only a few have a multipurpose scheme that covers the entire population. Eighteen percent of developing countries have a scheme that is used for identification purposes only; 55 percent have digital IDs that are used for specific functions and services like voting, cash transfers, or health; and only 3 percent have foundational ID schemes that can be used to access an array of online and offline services (figure S4.1). Twenty-four percent of developing countries have no digital ID system.

Although the concept of digital ID is universal, it plays somewhat different roles depending on the country context. In high-income countries, digital ID represents an upgrade from well-established, robust legacy physical ID systems that have worked reasonably well in the past. Belgium, Estonia, Finland, France, the Republic of Korea, and Singapore are some of the countries leveraging existing physical identity infrastructure to create digital ID ecosystems, enabling them to deliver public services more efficiently.

Low-income countries, by contrast, often lack robust civil registration systems and physical IDs and are building their ID systems on a digital basis, leapfrogging the more traditional physically based

Figure S4.1 Different types of digital ID schemes across countries



Source: World Bank ID4D database (various years). Data at http://bit.do/WDR2016-FigS4_1.

system. Identification, rather than e-services, is the main immediate goal. Such systems are being developed in Bangladesh, Guinea, and Kenya. One potential risk associated with leapfrogging to civil identification systems without a solid civil registration system is that in many cases the 0–18 population is excluded, and continues to be unregistered.

In middle-income countries, digital ID is strengthening and progressively replacing physical identity services while supporting the emergence of some e-services. Successful examples are found in Albania, India, Moldova, and Pakistan.

Evidence of impact

Evidence of the impact of digital ID is still largely anecdotal, but there is a growing body of research in at least three key areas—efficient management of social welfare programs, removing ghost workers from the government payroll, and improving the sanctity of elections.

Efficient management of social programs and welfare distribution

Digital IDs enable targeted cash transfers to bank accounts linked to a unique identifier. This ensures that those who are entitled to receive subsidies or benefits are actually getting them. For example, in India's fuel subsidy program, implementing cash transfers to Aadhaar-linked bank accounts to buy liquefied petroleum gas cylinders saved about US$1 billion per year when applied throughout the country.[3] This is just one of many subsidy programs in India that are being converted to direct transfers using digital ID, potentially saving over US$11 billion per year in government expenditures through reduced leakage and efficiency gains.[4] Other examples of the benefits of digital ID in reducing leakages for social protection or security programs, health insurance, and pension schemes due to duplicates, "ghost" beneficiaries, and corruption are occurring in Chile, the Arab Republic of Egypt, Ghana, Indonesia, Pakistan, South Africa, and Turkey.

Removing ghost employees from the government payroll

The budgets of many developing countries suffer from bloated civil service wages that leave little room for capital investments. For example, the public payroll occupies the bulk of the national budgets of Ghana, Uganda, and Zimbabwe, but weak systems imply that many individuals paid from the payroll do not actually work for the government, and may not even be alive.[5] Nigeria recently implemented a digital ID system for civil servants that enabled it to remove about 62,000 such ghost workers, saving US$1 billion annually, and providing a return on investment of nearly 20,000 percent in one year.[6] The impact of ghost workers is even worse in many other countries, ranging from 10 percent to as high as an estimated 40 percent in Zimbabwe, pointing to the substantial fiscal savings and efficiency gains from digital ID.[7]

Improving electoral integrity

Nigeria used digital IDs to prevent vote rigging in its 2015 elections.[8] The system enrolled about 68 million voters using biometrics (issuing voter cards that encoded the fingerprints of the rightful holder on a chip) and used card readers to authenticate voters, thus preventing 4 million duplicate votes. Although there were some operational challenges at the polls, the election was conducted successfully: all votes were cast, and it was difficult to rig or contest the results in the face of the transparency brought about by digital identity. However, other countries, such as Kenya and Somalia, have not reaped the same benefits from the biometric voter IDs.[9] Therefore, this remains an area of further research.

Developing effective digital ID schemes

Digital ID schemes rely on a backbone of connected systems, databases, and civil or population registries. These in turn have been established through a thorough enrollment process of the targeted population.

SPOTLIGHT 4

SPOTLIGHT 4

Many programs now include the use of both biometric data and traditional biographical data, as well as programs to eliminate duplicate enrollments to help ensure that each individual has only one registered identity and one unique identifying number.

The digital record is the basis for issuance of credentials, which may be cards equipped with bar codes or more advanced chip-based smart cards; they can also be single-function (and provide evidence only of identity) or multifunctional, with the card able to act as a bank card, driving license, and so on. India's Aadhaar program dispenses with the card altogether, providing remote authentication based on the holder's fingerprints or iris scan.[10] Online and mobile environments require enhanced authentication features—such as electronic trust services, which include e-signatures, e-seals, and time stamps—to add confidence in electronic transactions.

Mobile devices offer a compelling proposition for governments seeking to provide identity credentials and widespread access to digital services. In Sub-Saharan Africa, for example, more than half of the population in some countries is without official ID, but more than two-thirds of the residents in the region have a mobile phone subscription. The developing world is home to more than 6 billion of the world's 7 billion mobile subscriptions, making this a technology with considerable potential for registration, storage, and management of digital identity.

For a digital ID system to be effective, it must be rooted in an upgraded legal framework that considers the accessibility and protective measures of the system; clear definitions for the interconnectivity and interoperability with other (administrative or functional) registries; and coordinated investments throughout the country in information and communication technology (ICT) to develop a reliable and secure platform.

Digital identification systems may be developed in response to a specific application (elections, tax, social protection or security, pensions, health insurance, and the like), referred to as *functional schemes.*[11] Or they may be developed as universal multipurpose systems capable of supporting the entire range of needs for legal identity across all applications, known as *foundational identity schemes*. This distinction between functional and foundational systems is not immutable over time; often functional ones evolve to become foundational (in Bangladesh, Haiti, and Mexico, voter ID has become de facto national ID). No matter what the country context is, the priority should be to confer identity for all, either through a universal foundational scheme or through harmonization of the multitude of existing functional systems, so that in their totality they achieve full coverage.

Risks and mitigation

Digital ID schemes tend to be complex, are often politicized, and are subject to failure to deliver on high expectations. Risks associated with unsuccessful implementation can be mitigated by adopting guidelines that have emerged from the collective experience of digital ID schemes' rollouts around the world.[12] In this respect, several areas of focus emerge as critical:

- *Legal and regulatory concerns* about how to best determine the types, extent, and use of information collected under digital ID schemes; how to safeguard the privacy of personal data; and how to craft new primary legislation or rules to avoid unintended consequences such as inadvertent exclusions, onerous mandates that could deter individuals from accessing services, or increased rent-seeking involving registration or certificates.
- *Institutional and administrative concerns* about the institutional location of the civil and identification registries, and their interaction with functional registries or line ministries that need to verify or authenticate identities of beneficiaries or clients. The legal or foundational registries are traditionally located in the ministry of interior, justice, or home affairs; and more recently in special-purpose agencies independent of any line ministry (or loosely affiliated with one), and reporting to the center of government. Without effective coordination, there is a risk of a patchwork of competing schemes that would lack interoperability and consistency. The risk of exclusion would also be higher, as participation in functional IDs is a matter of program eligibility and not a birthright, as in foundational schemes.[13]
- *Technological concerns* about working with the private sector to develop a sustainable digital infrastructure that can reach remote areas and prevent exclusion; ensure interoperability and trusted authentication protocols for data exchange among different services and solution providers; and ensure data security, particularly in the use of biometrics, as well as the long-term accessibility and security of identity records.
- *Business models and procurement concerns* engendered by technology solutions that are tied to specific vendors; lack of open architecture anchored on modularity and open standards; lack of costing guidance

of various IT components; and absence of viable business models and digital ID–enabled services' uptake.

- *Country-specific and cross-border concerns* about what constitutes acceptable unique identifying credentials. This can differ across countries and applications, even as the world has taken steps to define standards for the mutual recognition of foreign citizens' credentials. Uses of digital ID schemes for tracking of ethnic groups and other nefarious purposes may be enabled by the recent advances in "big data" analytics that allow information to be collected and analyzed on an unprecedented scale.

Overcoming these challenges and barriers requires strong leadership, a supportive legal framework, interagency cooperation, mobilization of financial and human resources, and, critically, the trust of users. Incentives, technology, foreign assistance, and reforms will all be critical in achieving tangible results. Equally important is donor coordination at the global, regional, and national levels to ensure inclusive oversight and concerted global action.

Notes

1. World Bank ID4D global data set (April 2015). This number includes approximately 600 million unregistered children.
2. Dahan and Gelb 2015.
3. Barnwal 2015.
4. Banerjee 2015.
5. Public disclosures in media by finance ministers of several countries, monitored by Identity Counsel International and ID4Africa.
6. Gelb and Clark 2013.
7. Proceedings of Parliament of Zimbabwe, February 28, 2012.
8. Based on various reports in the Nigerian media.
9. Gelb and Clark 2013.
10. Dunning, Gelb, and Raghavan 2014.
11. This terminology was first adopted by Gelb and Clark (2013).
12. Gelb and Clark 2013.
13. For example, children are not eligible to register in voter rosters, while middle-income families are not included in poverty programs.

References

Banerjee, Shweta S. 2015. "From Cash to Digital Transfers in India: The Story So Far." CGAP Brief, Consultative Group to Assist the Poor (CGAP), Washington, DC. http://www.cgap.org/sites/default/files/Brief-From-Cash-to-Digital-Transfers-in-India-Feb-2015_0.pdf.

Barnwal, Prabhat. 2015. "Curbing Leakage in Public Programs with Biometric Identification Systems: Evidence from India's Fuel Subsidies." Columbia University School of International and Public Affairs, New York. http://www.columbia.edu/~pb2442/subsidyLeakageUID.pdf.

Dahan, Mariana, and Alan Gelb. 2015. "Role of Identification in the Post-2015 Development Agenda." Essays, World Bank and Center for Global Development, Washington, DC. http://www.cgdev.org/publication/role-identification-post-2015-development-agenda.

Dunning, Casey, Alan Gelb, and Sneha Raghavan. 2014. "Birth Registration, Legal Identity, and the Post-2015 Agenda." Policy Paper 46, Center for Global Development, Washington, DC.

Gelb, Alan, and Julia Clark. 2013. "Identification for Development: The Biometrics Revolution." Working Paper 315, Center for Global Development, Washington, DC.

World Bank. Various years. ID4D (Identification for Development database). World Bank, Washington, DC. http://data.worldbank.org/data-catalog/id4d-dataset.