OMIDYAR NETWORK
A WORLD OF POSITIVE RETURNS

5 surprisingly consequential decisions made by ID-system planners

By Subhashish Bhadra, Principal, Omidyar Network

Mobile First. Internet of Things. Microservices Architecture. Artificial Intelligence. Blockchain. Each of these buzzwords represents new frontiers for national identification systems.

Behind each of them, however, lie fundamental decisions that governments must make at the very inception of their countries' ID systems. These decisions have an outsized influence on inclusion, privacy, and efficiency. They also determine whether otherwise value-neutral technologies become engines of growth or tools of surveillance.

At least five early policy and design decisions stand out as critical influencers of other choices that governments will make in the future and the ID system's ultimate impact on society.

1. What is the purpose of the ID system?

The appropriate use of national ID remains an unanswered and somewhat contentious question.

The purpose of ID systems varies across countries. According to the 2016 World Bank ID4D database, almost 90 countries are also using these programs to deliver subsidies, whereas about half use their ID system to streamline taxation and reduce identity fraud. Voting is another popular use case, especially in Africa and Latin America.

And whether the ID is proof of citizenship is a particularly controversial decision, especially in regions with high inbound migration. India took the decision to separate ID and citizenship – a decision that perhaps aided the rapid uptake of the program. Despite this decision, migration-based tensions in a few Indian states caused enrollment there to lag.

Identification systems across the globe – ranging from Ireland's public services cards to the Australian government's proposed facial recognition legislation – have been accused of straying away from their intended purposes. Such mission creep can create several risks.

Firstly, increasing the instances when ID is required increases chances that more people will be excluded from services. Second, mission creep creates a wider digital footprint that can be used to create a broader profile of an individual, sometimes without consent, and target them. This can increase privacy risk. Thirdly, it increases the power imbalance between institutions and individuals that can be used to curtail civil liberties, especially for vulnerable or persecuted groups.

To avoid such mission creep, ID-system planners need to clearly articulate the intended uses of the system, in the immediate term as well as in future scenarios. Not only will this heavily influence its technical design, but will also lead to the necessary guardrails to protect against potential abuses. For example, if the purpose of the ID system is to de-duplicate beneficiary lists of different subsidy programs, ID planners can create several different ID numbers linked to a single foundational ID ("tokenization").

In 2019, Omidyar Network is embarking on a global research effort in three countries to help provide some insight to the purposes (i.e., use cases) that hold the highest value and highest risk for people and governments.

2. Where does the ID system reside?

The primary purpose of a national ID system is also reflected in the ministry that manages the ID system. Again, according to the 2016 World Bank ID4D dataset, the Ministry of Interior or Home Affairs runs the ID system in 109 countries. Some ID systems aim to bring legitimacy to the electoral process, and are therefore housed with the electoral body. And many ID systems are housed entirely outside of the government, some of which have also sought to develop independent financing models.

The institutional home of the ID system is a critical early decision because it impacts its ability to scale beyond the first use case. For example, multi-purpose ID cards are absent in all of the 12 countries where the electoral body hosts the ID system, and in 90 percent of those where the Ministry of Interior or Home Affairs is the host. The prevalence of multi-purpose ID cards is higher, however, when the system is hosted by autonomous bodies (23 percent), the Ministry of Justice (13 percent), or other agencies (14 percent).

Additionally, where it resides can ultimately affect people's trust and acceptance in the ID system. One that is managed by an independent commission will reduce both the likelihood and perception of institutional bias.

3. What data does the ID system collect?

One of the most consequential decisions that the ID-system planner needs to make is the data that the government collects in order to issue an ID. What data is requested from the user can affect efforts to improve inclusion, social dynamics, privacy, and scalability. It can also work against intentions to reduce the cost, time, and likelihood of failure with an ID system.

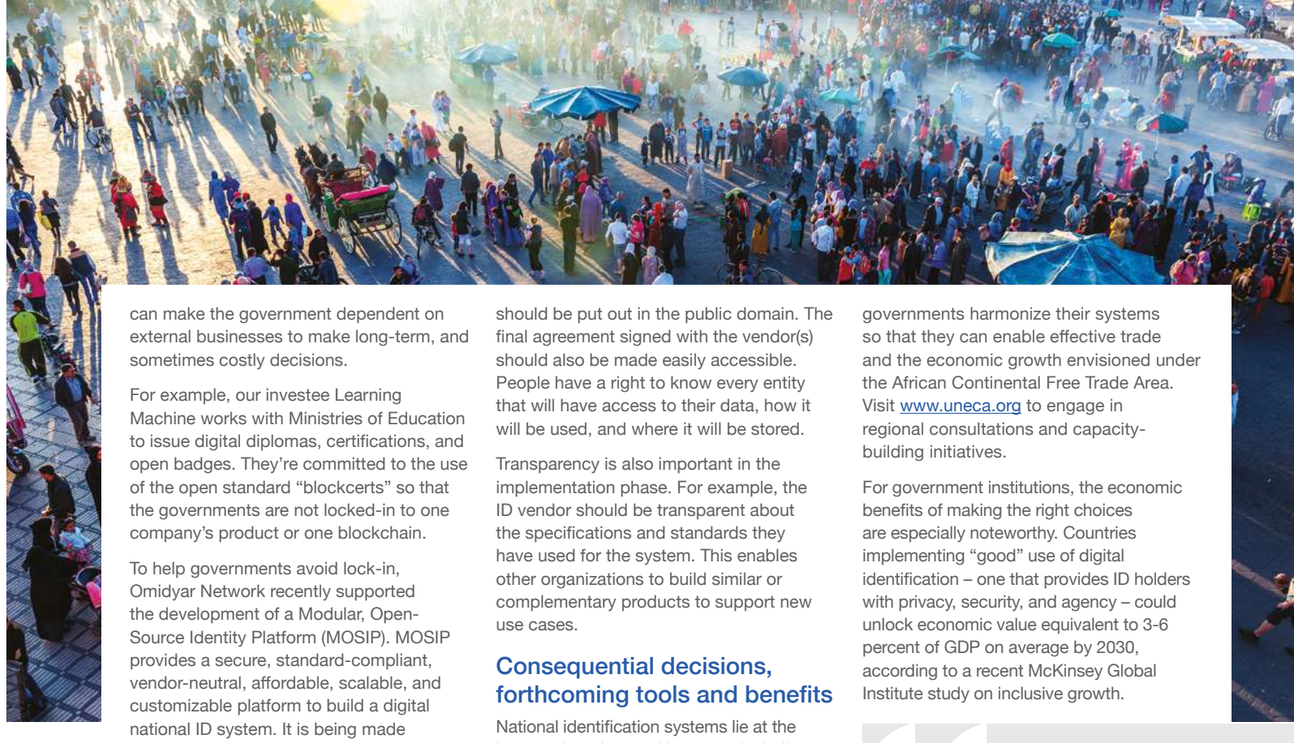
First, fewer data points reduce the cost and increase the speed of enrollment. Individuals may be unwilling or unable to enroll, if they have to answer many questions or supply various forms of documentation. For example, Pakistan's national ID card collects over a dozen data points, which some believe caused low registration rates (only half the country by 2012). In comparison, India's Aadhaar collects four mandatory data fields (along with biometrics) and has been able to enroll nearly the entire adult population within a decade. Moreover, an ID system is less likely to be inclusive if it collects more data. This is especially true in developing countries, where the most vulnerable populations often don't have proper documentation in order to complete all of the requested fields.

Second, data collected by ID systems can also contribute to, or be affected by, social tensions. For example, Afghanistan's e-tazkira ID card has been embroiled in controversies since the beginning due to a proposal to include ethnicity as a data field and worries about discrimination.

Third, greater data collection raises the possibility of surveillance by the government as well. Therefore, many courts and data protection laws have upheld the government should collect only the minimal amount of data in order to be able to issue the ID card and provide related services.

4. Does the government have meaningful choice?

All ID systems need to navigate a myriad of technological choices. Very often, they require technical knowledge, and the future implications of these choices are difficult to grasp. Many governments bring in an external consultant or vendor for the national ID systems. However, the government needs to own the thinking behind the ID system, and ensure that it does not get locked in to a particular vendor or technology. Failure to do so can make the government dependent on external businesses to make long-term, and sometimes costly decisions.



For example, our investee Learning Machine works with Ministries of Education to issue digital diplomas, certifications, and open badges. They're committed to the use of the open standard "blockcerts" so that the governments are not locked-in to one company's product or one blockchain.

To help governments avoid lock-in, Omidyar Network recently supported the development of a Modular, Open-Source Identity Platform (MOSIP). MOSIP provides a secure, standard-compliant, vendor-neutral, affordable, scalable, and customizable platform to build a digital national ID system. It is being made available for free, as a public good, by the International Institute for Information Technology—Bangalore (IIIT-B) through GitHub and at www.mosip.io.

With the building blocks of MOSIP, countries can design their national ID systems to be context-specific and based on local laws and decisions. The government of Morocco will be the first to use MOSIP to build its digital identification system, with the goal to integrate the system with social safety net programs and help deliver government programs to citizens.

Omidyar Network is also funding research on the technical and policy choices that countries need to make at the time of designing the ID system. This research will identify all major choices, list the available options, and present the benefits and risks of each option. We hope that governments will find this research useful while interacting with their consultants and vendors.

5. Is the process transparent?

Limited state capacity prevents some governments from effectively monitoring how well the ID systems are meeting the public and countries' needs. Academics, civil society organizations, and other diffused stakeholders often assume that role. Recognizing that accountability is essential in any government program, ID-system implementer should plan for an open, collaborative, and detailed consultation process with these groups and the general public, from the very beginning.

For example, transparency is a core principle of high-quality, public procurement and should be built into the process from day one. The tender detailing the needs of an ID-system designer or technology should be put out in the public domain. The final agreement signed with the vendor(s) should also be made easily accessible. People have a right to know every entity that will have access to their data, how it will be used, and where it will be stored.

Transparency is also important in the implementation phase. For example, the ID vendor should be transparent about the specifications and standards they have used for the system. This enables other organizations to build similar or complementary products to support new use cases.

Consequential decisions, forthcoming tools and benefits

National identification systems lie at the intersection of several interests, including efficiency, inclusion, transparency, security and privacy. International efforts to influence how ID systems should be designed, such as the Principles on Identification for Sustainable Development, provide a normative framing. Yet, the societal value of each of these interests depends on the context of the particular country.

Each country has a unique starting point. And when faced with different options, the most optimal choice (if it exists at all) will vary from country to country. Even within countries, various stakeholders place different values on these objectives. To effectively balance all of the interests, system designers need to rigorously evaluate the various choices available to them within parameters set by the country's laws, economic needs, and ultimately, its people. Specifically, they will need to take into account the existing identity landscape, the infrastructure availability, and the constitutional framework of the country, among other things.

Building on the country-level work of the World Bank's ID4D program, Omidyar Network is currently developing a toolkit to help governments navigate some of these difficult moral, technological, political, and economic decisions and explore the trade-offs associated with forming an ID system. New partnerships with the UN Economic Commission for Africa and ID4Africa will also provide capacity-building training and convene government leaders responsible for digital identity policy and technology choices.

Additionally, in November 2018, the United Nations Economic Commission for Africa launched a Centre of Excellence for Digital Identity and is helping governments harmonize their systems so that they can enable effective trade and the economic growth envisioned under the African Continental Free Trade Area. Visit www.uneca.org to engage in regional consultations and capacity-building initiatives.

For government institutions, the economic benefits of making the right choices are especially noteworthy. Countries implementing "good" use of digital identification – one that provides ID holders with privacy, security, and agency – could unlock economic value equivalent to 3-6 percent of GDP on average by 2030, according to a recent McKinsey Global Institute study on inclusive growth.

> **"…when carefully designed, digital ID programs can help people participate more fully in their economy and society as consumers, workers, and citizens. As a result, digital ID may be the next frontier in global value creation and a new force for inclusive growth, especially in emerging economies. But unlocking that value and getting it right is by no means certain or automatic. Achieving widespread adoption of digital ID and realizing the benefits can only occur if governments, businesses, and civil society work together to mitigate risks, ensure privacy, and promote trust."**
>
> Good Digital Identification as a Key for Inclusive Growth, McKinsey Global Institute

Prioritizing privacy and security and empowering ID-holders with agency will align governments with the tenets of Good ID. Good ID is championed by dozens of organizations and people who believe in digital dignity, data protection, quality identification systems that help people thrive, and human-centered technologies.

We invite anyone who is actively designing or refreshing identification systems, building applications on top of them, navigating the legal and political complexities of digital identity, researching the topic, and advocating on behalf of vulnerable groups to join the conversations taking place in person and online. Visit www.good-id.org to access the latest research, guidance, events, and other resources on digital identity.