Preliminary Discussion Paper on the Future of Identification and Development

[DRAFT]

Version: 10/31/2015

Alan Gelb and Anna Diofasi
Center for Global Development

This preliminary discussion paper serves as a background document to an upcoming CGD book on identification, biometric technology, and development and as an input to ongoing CGD work in this area.

CGD is grateful for contributions from the Omidyar Network in support of this work.

Contents

1 Introduction

Motivation.

The objective of this paper is to provide a high-level overview of the current state of identification (ID) systems and technology in developing countries from the perspective of economic and social development. There is now great interest in this area, as evidenced by the inclusion of "legal identity for all by 2030, including through birth registration" as one of the targets of the Sustainable Development Goals. This is the first time that such an aspiration has been recognized in the context of global development.

The complex framing of the target reflects an equally complex reality. There is universal agreement on the importance of birth registration and the civil registration of other vital events including death, marriage and divorce. But there is less consensus on the concept and measurement of identity and on the most desirable arrangements to identify citizens and others living on a national territory and to enable them to authenticate their own identities. Social and political views on this question differ across countries and sometimes also between groups.

This is a changing picture. Attitudes to identification are still evolving, as are views on the technology innovations over the last two decades that have revolutionized this area. Traditional paper-based systems of identification are shifting rapidly towards digital identity systems or eID.[1] Technology is now considerably in advance of regulation and promises to remain so as the pace of innovation continues to be high. Today's frontier innovation may be tomorrow's industry standard.

Many developing countries have been implementing national-level ID programs and upgrading existing ones to enhance their capabilities to provide a broad "foundational" eID. There has also been a proliferation of "functional" identification and eID programs that serve particular development applications. Rigorous studies on the impact of these technologies are few and more are urgently needed, but it is clear from the partial evidence available that stronger ID has great potential to support inclusive development. The potential gains are in many areas:

- **Asserting Rights**. Regarding inclusive development, official recognition is essential if individuals are to claim their rights and access the programs and services to which they are entitled. It is no accident that those lacking legal identity or official identity (a term explained below) are among the poorest and most isolated groups in poor countries. Lack of identity is not a major problem for elites.

[1] Digital identity or eID refers to identity systems that involve the use of digital technology, potentially in several ways: digital biometrics to identify and authenticate individuals; electronic databases to store and manage records, and electronic credentials to serve a variety of mobile, online and offline applications. ID as used in this paper should be generally taken to include eID.

- **Strengthening State Capacity**. Regarding efficiency and effectiveness, effective ID (or eID) systems offer a mechanism to strengthen administrative capacity. They can help to rationalize subsidies, services and programs, and to deliver them in a client-centric way with increased speed and convenience. Coupled with modern payment and reporting systems they can also increase the accountability of providers and strengthen the relationship between the state and its citizens through more effective revenue collection.

- **Creating Opportunities**. At the nexus of inclusive development and efficiency, (e)ID can spur entrepreneurship and income growth by reducing transactions costs, making it easier to set up and run small businesses more securely and profitably. ID-enabled solutions such as mobile payments offer both increased security and cost savings to people and business.

However, it is still not clear how much of their potential the new and more rigorous ID systems will realize. They pose several risks, including to the poorest and most vulnerable:

- **Exclusion**. Strong identification can exclude individuals as well as include them. Depending on how programs are implemented, registration and authentication can pose additional obstacles for the poor. People may also be excluded through the tightening of scrutiny on citizenship or other requirements for services.

- **Misuse of Personal Data**. They raise the risk that personal data will be misused against the interests of the subject, whether through security breaches or inappropriate commercial use, including through linking records across multiple databases or by facilitating surveillance. At the same time, strong ID is essential to limit identity theft – another misuse of personal data.

- **Ineffective Rollout**. ID programs may not be implemented in a way that makes them cost-effective. This may be because there are too many incompatible systems, systems that are poorly designed and implemented, or political constraints on the use of ID systems that limit the benefits.

The debate points to the fact that technology is neutral and that results depend on the social and political context in which it is applied.

What is new? People identified each other through appearance and behavior long before written records existed. Records were initially local (entries in parish registers) before evolving into national systems of registration and identification. Identity management systems have typically taken centuries to develop and mature in industrial societies but some have a long history. As far back as 1000 years ago, China had a sophisticated system to classify and cross-reference individuals by name, community, landholding and tax obligations. The coverage and quality of formal ID systems has broadly advanced in line with that of social and political institutions although there are some interesting anomalies. Within the contexts of their respective societies identity credentials have typically certified

status or membership (a passport or national ID (NID) card for citizenship) or been linked to some function, right or obligation (tax ID, ration card, driver's license). [2]

The last 15 years have seen a massive surge in the number of more sophisticated eID systems. Several factors are creating demand for new and more effective ID services:

- Security concerns after the events of September 11, 2001 have been and continue to be a major global driver for both technology and systems. ID requirements for cross-border travel are far more demanding than previously. So are financial Know Your Customer (KYC) requirements, aggravating the tension between applying AML/CFT[3] policies and encouraging financial inclusion.[4] Countries are also increasingly requiring SIM card registration, raising the question of how an estimated 2 billion prospective customers, many without identification, are to be registered.

- On the development side, the MDGs marked a shift towards seeing progress more in terms of individual capability than simply as aggregate growth. Programs to deliver direct transfers (conditional and unconditional) and health and education services have grown rapidly. A recent survey by the World Bank that covered 21 developing countries estimates that transfer programs reached some 400 – 500 million recipients. Such programs, and many others related to diverse SDG targets, require accurate identification of individual beneficiaries to be effective and accountable.[5]

- Developing economies and institutions have become more formal, more urban and more sophisticated. This has increased demand for modern ID services, for example, to register property, secure loans and administer taxes. In many developing countries growth of the e-economy and the provision of e-services are creating new demands for e-ID because of the need for participants to authenticate themselves remotely and online.

- The number of migrants has increased to as many as one billion people, including about 250 million who have migrated internationally. This increases the demand for portable or mobile ID. Rapid growing refugee populations are creating new demands for identification to confirm identity as well as to deliver financial support and other services.

[2] See Gellman (2013) and Groebner (2007). For a wider canvas on global ID systems see Breckenridge and Szreter (2012). In contrast to China, pre-colonial Indian states never developed systems beyond enumeration.

[3] Anti-Money Laundering/Combating the Financing of Terrorism

[4] For discussion of approaches to easing the tension between financial integrity and financial inclusion see Task Force Report: Regulations for Improving Financial Inclusion. Center for Global Development 2016 forthcoming.

[5] Dahan and Gelb (2015a) list ten SDG goals where accurate identification is essential for individuals to assert rights or if programs are to be effective.

- The shift towards electoral politics – as in Sub-Saharan Africa since the end of the Cold War – has created a new imperative to identify voters and to authenticate them at the polls to help boost the credibility of the soaring number of elections.[6]

On the supply side, digital biometrics and other ICT advances have been major drivers of change.[7] It is no exaggeration to say that they have been revolutionary, particularly in developing countries with less investment in paper-based legacy systems. Biometrics introduce particular risks and have been strongly resisted for civil applications in some industrialized countries, even though the same countries have built up very large biometric databases for law enforcement and security. Nevertheless, the industry has emerged from the shadows of forensics and security to become the backbone of almost all of the new ID systems put in place in developing countries over the last 15 years. The industry's global growth rate has been around 20-30%, and is higher in developing markets than mature ones (Gelb and Clark 2013a).

This technology has three major implications for the use of ID in development:

- Increased precision, functionality and reach of traditional "top down" ID systems. Manual management of an identity database, including comparing photos and analog fingerprints to detect multiple enrollments and identify individuals against the entire gallery becomes difficult when enrollment exceeds around 100,000 people. Digital multi-modal biometrics offers the possibility of extending this capacity to registers in the hundreds of millions, or even billions of people.

- Registration (enrollment) and authentication can be de-linked from biographic documentation. This enables identification to be partitioned into its most basic element (I am the person that I claim to be in the register) and other personal and biographic data such as gender, age, address, nationality and parentage that have commonly been bundled together into identification (who I actually am). These other attributes can be termed "ID+". One of the strategic choices facing countries is whether to continue to bundle ID+ into identification or to follow an "ID first" strategy that initially documents the existence of the individual through characteristics like iris or fingerprints that convey little or no other personal details while leaving other aspects of identity (such as determination of national status or legal residence) for later.

- Connectivity opens up the possibility of new decentralized or "federated" approaches to establishing identities and authenticating individuals against them.

[6] Frieden (2015) notes that largely due to the conditioning of Western aid the number of self-proclaimed single party systems fell from 29 to 0 in Sub-Saharan Africa between 1989 and 2004. In 1960-1969 less than one election was held per year; the figure jumped to almost 7 per year in 1990-2012.

[7] Jain and Ross (2015) define contemporary biometric recognition as "the automated recognition of individuals based on their biological or behavioral characteristics". These can include a wide range of features, including fingerprints, vein patterns, hand geometry, face (2D and 3D), iris, ears, DNA, ECG, EEG, voice, signature, dynamic signature, gait, keyboard stroke patterns, smell and others.

This is essentially a return to the oldest local or "third-party" form of identification but executed through digital mechanisms and involving virtual communities, and possibly creating a market for ID services.

The final factor spurring the growth of ID programs in developing countries has been support from the international community. Development partners funded about half of the 160 cases considered in Gelb and Clark (2013a). These have usually been in support of a particular program such as a credible election (often supported by UNDP) or a social transfer system (often bilateral or IFI) rather than a sustained effort to strengthen foundational programs of birth and civil registration. As a result, donor support – often including to multiple programs in the same country at the same time – has sometimes contributed to a proliferation of ID systems with incompatible standards. With civil registration and ID now more frontally on the development agenda, recent initiatives such as the WHO/World Bank joint initiative to scale up civil registration and vital statistics and the World Bank's multi-sectoral ID4D initiative aim to increase the coherence and continuity of support. New initiatives such as ID4Africa are facilitating the exchange of knowledge across developing countries to promote the responsible use of ID for development.[8] Donors do not yet, however, have a forum to coordinate support to ID initiatives and promote performance standards. [9]

Outline and Scope.

Because "legal identity" is associated with legal status as well as identification, another term is needed to encompass the wide variety of identity services and credentials found across the world. Section 2 develops the concept of "official identity" as a broader and more flexible alternative to "legal identity". It provides a perspective on the evolution of identity systems through three phases:

- The first is "the village" model of local ID, whether based on written records or on personal attestation by trusted members of the community. This system is alive and well in many poor countries.

- The second is the dominant model of formal "top-down" legal ID (civil registration and identification) or large-scale ID programs for particular purposes, implemented nationally or on a wide basis. Some of these systems can rely on strong foundational civil registration systems to provide continuous data on births, deaths and family relationships. Others currently need other processes to create an identity baseline for enrollees and update their data bases.

[8] See for example the ID4Africa initiative: http://www.id4africaforum.com/

[9] For more discussion see also Dahan and Gelb (2015a). Until recently, among the Multilateral Development Banks only the Inter-American Development Bank has sustained a core operational focus on strengthening civil registration: http://www.iadb.org/en/topics/government/civil-registration-and-identity,4032.html . See also: http://live.worldbank.org/making-everyone-count and http://www.worldbank.org/content/dam/Worldbank/document/HDN/Health/CRVSScaling-upoverview5-28-14web.pdf.

- The third, still emerging, model is "federated ID" or an "e-village" model, with identification services provided by trusted third parties, possibly commercially or through social or professional networks.

Who has ID? Section 3 provides estimates of the number of people who lack types of official ID, whether a birth certificate or some form of national credential. It is not easy to calculate this number because of the question of what to include as official ID and also because there are often no good estimates of live coverage, even for established programs. One recent estimate suggests as many as 2.4 billion people may lack a widely recognized credential, almost one third of them children who have not been issued with birth certificates (Dahan and Gelb 2015b).

Section 4 considers the architecture and quality of "top-down" official ID systems in more detail. Institutional models for providing ID services differ across countries. Not all follow the "OECD model", although many countries are converging towards it. National-level civil registration/identification programs are usually managed by government departments within a single ministry but there are many other patterns. Some countries have created an independent entity with the clear mandate to register and identify citizens and residents and provide ID-related authentication services to other parts of the government as well as to the private sector. There may be advantages to this model, including the de-politicization of registration and identification. Cases show that countries have a range of choice between public provision (ID seen as a public good) and commercialized provision, including cross-subsidizing basic ID services to the poor and the outreach essential to enroll them.

Turning to the architecture, any advanced system would be expected to do two things. It should provide robust credentials that provide ID as needed to realize rights and to facilitate programs and services. It should also be inclusive, providing credentials to all who have a legitimate claim to them. A third capability is the ability to service multiple applications, or the overall integration of the ID system. This is more complex. Having multiple functional program IDs can undermine programs to roll out a sustainable central program of civil registration and identification. Fragmentation into "ID silos" also raises costs and impacts on the coherence of policies and programs. Yet it must also be acknowledged that the question of whether to integrate all ID services into a single system based on a common unique ID number that is required for virtually all applications raises some concerns. Recognizing that many countries are, in fact, trying to move towards more integrated systems, the paper therefore treats integration as a legitimate area for social choice.

An analysis using the benchmarks above to assess the advancement of ID systems shows how greatly systems vary across countries. However, given that in-depth comparative assessments of ID systems are only starting to be produced, it is not possible to be comprehensive. Civil registration should be the foundation for ID (as it is, for example, in

Botswana and in Uruguay where infants receive their national ID number before leaving the hospital). But it is often weak, with low coverage of births and deaths so that not all ID systems are based on strong civil registries as in the traditional "OECD model". Sustained effort is needed to strengthen this foundation for identity management over the lifecycle. Some countries still have only rudimentary ID systems and need to start almost from the ground up. Other countries have multiple systems, often with limited coverage and quality, and need to move "from confusion to inclusion". Still others have centralized systems with high coverage. However, only in some countries are they integrated into a wide range of functional applications.

Section 5 considers four "frontier" systems. India's Unique Identification (UID or Aadhaar) program represents a distinctive low-cost "ID-first" centralized approach to identity management. Estonia, also a centralized model managed by the state, stands out as the world's most developed e-ID system. The third case is "federated identity" as provided by GOV.UK Verify. Such systems could provide a complement or possibly an alternative market-driven approach to centralized top down systems. The fourth case takes this further, towards the possibility of identification through social or commercial networks. Such an "e-village" system may not be the most urgent development priority for poor countries where connectivity is low, especially among the poor, and the priority is to ensure that all have access to a robust base official identity. But there are already enough examples to suggest that such systems could become attractive to some private users as well as perhaps become accepted as a component of official ID for certain purposes.

Section 6 discusses three highly relevant topics for the operationalization of ID systems: costs, the use of biometrics, and the enrolment of small children. First, it offers benchmark cost estimates for ID systems (enrollment and maintenance) and a comparison with the potential benefits. One conclusion is that the costs of a well-managed ID system would be covered by even a modest improvement in the efficiency and accuracy of public payments for salaries, transfers and pensions. Second, it reviews the evolving role of biometrics in the new systems, including in the frontier area of mobile ID. Third, it considers the problem of providing consistent and robust ID over the life-cycle, in particular the identification of young children beyond traditional birth certificates. Although more can be done to strengthen identification for the young this remains a frontier area for ID.

Section 7 shifts towards development applications. This is an important and under-researched area. Better understanding of the impact of the new technologies is urgently needed as they begin to be integrated into a variety of programs. While there are many anecdotal references and partial examples, it is difficult to find more than a few rigorous assessments of the application of new ID technology to development programs. We refer to Gelb and Clark (2013a) for overall coverage and focus on certain cases in the areas of finance, transfers and health. The aim is not to be exhaustive but to flag examples of how accurate identification can strengthen the implementation of programs in these areas.

Section 8 considers the three categories of risks: the exclusion of poor people, vulnerable groups, and those of indeterminate citizenship; the misuse of data and the erosion of privacy; and the cost-ineffective rollout of ID programs. The last risk can result from poor ID strategy (or from having no coherent strategy), from corrupt procurement or from poor implementation, including failure to put in place the Point of Service (POS) technology to enable eID to be used as intended. It can also reflect political interests that limit the use of the system in potentially high-payoff applications, such as tax enforcement, that threaten the interests of the elite.

Section 9 concludes, with options for the future and priorities to ensure that the spread of more advanced ID systems contributes to development in a cost-effective and sustainable way.

With such a broad agenda, the treatment is selective. It is light in certain technical areas such as security, encryption and database management. While noting the implications of different models for identity services for data privacy, it does not go deeply into alternative legal and regulatory models. Civil registration is treated as the vital building-block of the ID system that it is, but the paper will not go too far into the details of scaling-up[10]. There will also be less than complete discussion of alternative mechanisms for authentication, such as single-purpose cards, multi-purpose cards, mobiles, or just biometrics. This area is evolving rapidly, so that the perspective of the paper is that systems should aim to provide as broad an authentication menu as possible and enable a "foundational" system to support as many derived systems as needed for particular purposes.

2 Identity and "Official Identity"

> *"The premodern state was, in many crucial respects, partially blind; it knew precious little about its subjects, their wealth, their landholdings and yields, their location, their very identity. It lacked anything like a detailed "map" of its terrain and its people…..As a result, its interventions were often crude and self-defeating… How did the state gradually get a handle on its subjects and their environment? Suddenly, processes as disparate as the creation of permanent last names, the standardization of weights and measures, the establishment of cadastral surveys and population registers, the invention of freehold tenure, the standardization of language and legal discourse, the design of cities, and the organization of transportation seemed comprehensible as attempts at legibility and simplification. In each case, officials took exceptionally complex, illegible, and local social practices, such as land tenure customs or naming customs, and created a standard grid whereby it could be centrally recorded and monitored"* Scott (1998), 'Seeing Like a State' as quoted in Carson (2011)

[10]For more information, see: WHO and World Bank (2014). Global Civil Registration and Vital Statistics Scaling up Investment Plan 2015–2024. Available from: http://www.worldbank.org/content/dam/Worldbank/document/HDN/Health/CRVS%20Scaling-up%20plan%20final%205-28-14web.pdf.

From the earliest days**,** ID systems have relied on one or a combination of the three factors forming the basis of identification:

- Something you have – a card, token or other credential
- Something you know – a password, PIN or ability to provide personal information
- Something you are – a biometric: physical (photo, fingerprint) or behavioral characteristic (speech pattern).

These may be bundled in various ways to enable an individual to authenticate her/himself against a claimed identity or to enable a trusted entity (public or private) to authenticate the individual. The identity itself may be supported by a documented or oral record of interactions (something you have done).

As explained by Scott (1998) above, ID systems based on such factors must be considered in the context of the historical and institutional progression of societies and economies as well as access to technology. They are part of a broader standardization process to render societies "legible" to governments. In many ways states, law enforcement agencies, banks, businesses and others faced the same problems of identification five centuries ago that we do today. Groebner (2007) describes the use of portraits, seals, coats of arms, badges, descriptions, registers, lists, and official signs to identify and authenticate individuals. In Italy, governments commissioned painters, including virtuosos like Giottino, Botticelli, and Andrea del Sarto, to engrave images of delinquents, traitors and bankrupts on the run, for wide circulation.

2.1 Three Phases of Identity.

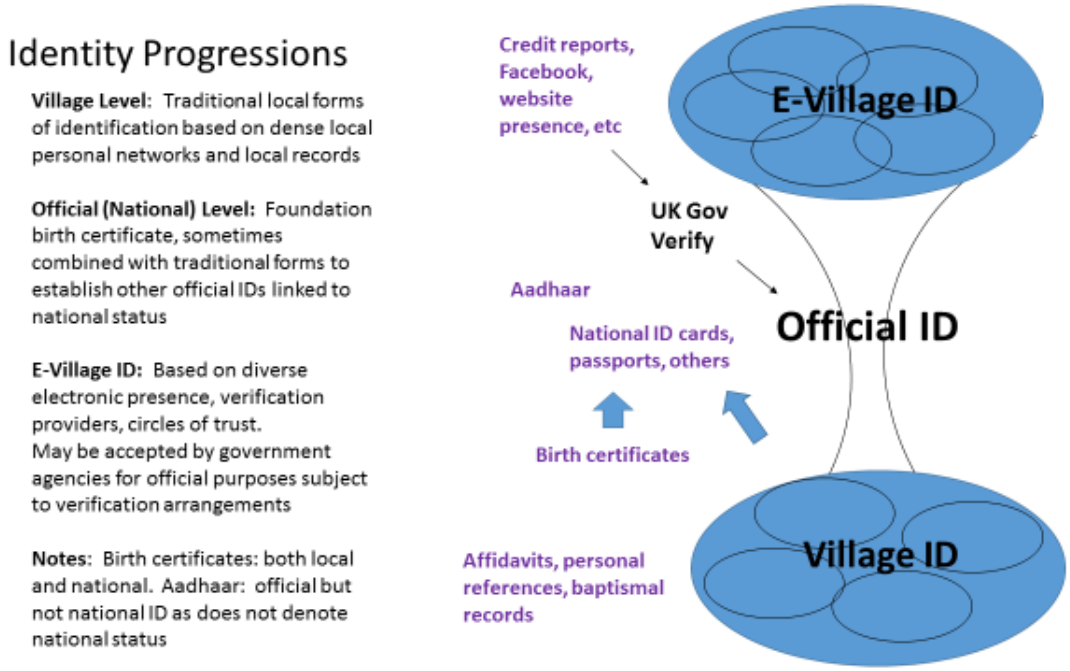
Figure 1 provides a broad sweep on identification distinguishing three phases:

Village ID. In the earliest "village" phase, local officials, religious leaders, communal elders or family members confirm identities and authenticate individuals against them through a written affidavit or oral testimony. Identification systems rely primarily on who you know and who knows you. As societies and economies become more complex and geographically dispersed, identification shifts from local identification based on personal familiarity towards more standardized records and databases.

Although countries have shifted towards top-down and National ID (NID) programs, the personal "village" model remains important in many of them. "Family book" systems in countries like Indonesia and Ethiopia are managed within local administrative units. Local attestation (such as the "introducer" in Aadhaar enrollment) often underpins the identity baseline for "top-down" ID programs. Tanzania, where only around 10% of the population holds a national ID card, offers another example. Especially in rural areas, local testimonials based on personal knowledge are still a key element of identification provided by

individuals seeking to register SIM cards for mobile services. Local identification is also widely used for voter registration in poor countries (see Box 1, Section 2 on Togo).

Figure 1
Three Phases of ID

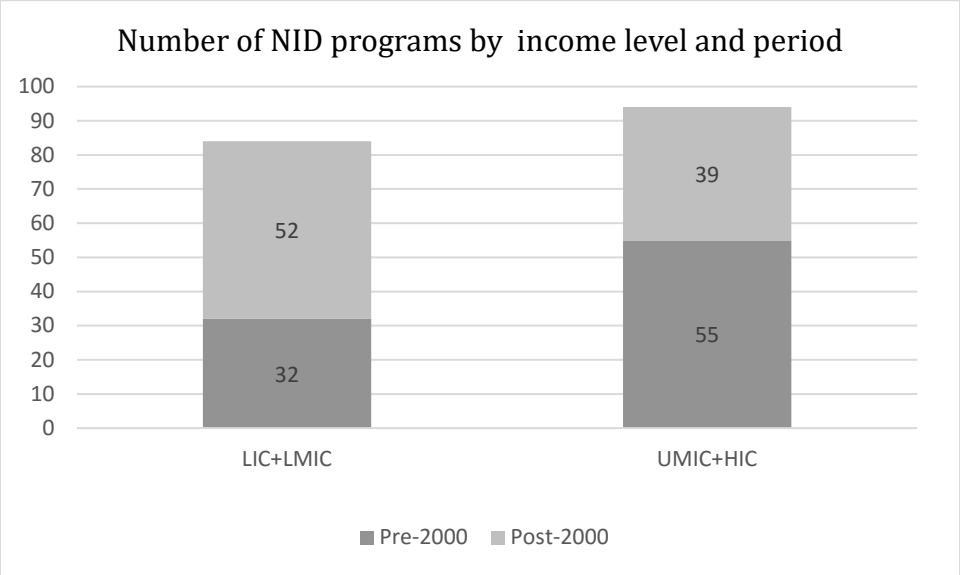


Top-Down ID. In response to the challenge of increasingly mobile populations detached from traditional communities, identity management tends to move to the second phase of centralized national-level programs. Most of these have their origins in local church or civil registration processes. The extensive system of national registration and identification in Peru, for example, has roots long before independence in the local registration of births by the Catholic Church. Modern identification systems often combine all three identification factors - registration and authentication via a biometric identifier, issuance of a physical token, and access to sensitive information via a PIN or password. Estonia (see section 5) represents the pinnacle of this model, with a central e-ID system that provides all citizens and residents (as well as enrolled non-residents) with a full digital identity.

Many of the better-established NID programs are included in Bennett and Lyon (2008) and the database maintained by www.identity-cards.net but the coverage of smaller and more recent programs is incomplete. With these caveats in mind, Figure 2 offers a broad global picture of the spread of nation-level identification programs based on ongoing work by the World Bank ID4D Program. Not all of them are fully operational -- at least 15 are in the

process of development.[11] Nevertheless, the figure suggests that NID programs have proliferated after 2000 to the point that almost all countries have a national-level program. More than half of the programs in low and lower-middle income countries have been initiated in the last 15 years. Most of those in high and upper-middle income countries were initiated before 2000. This difference is partly due to Latin America, which has a strong tradition of civil registration and national ID.

Figure 2
The Spread of National-Level ID Programs



Source: World Bank ID4D

"Federated ID" or the "e-Village". Access to the Internet has become quasi-universal in most of the developed states and is expanding rapidly in developing countries. Close to 35% of those living in developing countries use the Internet regularly, with the share of the population on-line rising by about 10% each year (ITU, 2015).

Increasing connectivity and online presence opens up the third potential phase of ID services, towards the use of third-party credentials provided by trusted identity providers as in the case of "federated ID". This can be considered as an "e-village" model where an identity is established by documentation and a record of existence and interactions. The trusted agent verifies the identity and authenticates individual against that identity. The most advanced case of this model for providing official ID appears to be Gov.UK Verify, now in Beta test mode. Commercial entities with large client bases, such as Facebook, Google,

[11] The number is probably higher: the estimate is based on a comparison of a dataset produced at CGD with the dataset from the World Bank and considered only non-matched cases where the assessments differed on the existence of a NID.

Amazon and Yahoo are also beginning to emerge as third-party providers of identification services in a limited sense.

From ID to eID. Countries are transitioning away from traditional paper-based IDs to eIDs. One study of ongoing programs and plans by IRIS Corporation estimated a decline in the number of traditional national ID programs from 59 to 26 and an increase in the number of eID programs from 67 to 114 over 2010—2015. Another assessment of ongoing market trends in the ID card industry by Acuity estimated that the ratio of the issuance of eID credentials relative to that of traditional IDs increased from 1:1 in 2010 to 4:1 by 2014. (Refs)

The e-credentials themselves are varied. Countries like Peru, Chile and Pakistan have quite lengthy records of the use of a foundational eID across a wide range of applications. Malaysia offers an early example of experience with a multi-purpose national eID card. MyKad, the compulsory identity document for Malaysian citizens aged 12 and above, was introduced in 2001and was followed by MyKid for younger children in 2003. The card includes digital photo and fingerprints. As well as serving as proof of nationality, it includes many applications that can be activated by the user, including driver's license, ATM card, e-wallet and provision for PKI – users can now select out of a menu of 50 applications. A number of other administrations including for example Macao and Hong Kong, have moved in the direction of multi-purpose cards. Some countries offer the option of integrating ID into a mobile (mobile ID). Others prefer to separate out applications from the core ID function of the card or – in the case of India's UID system -- to dispense with cards altogether.

There are signs that eIDs may be starting to converge towards compatibility with the ICAO standard for machine-readable passports[12]. Many countries now collect fingerprint and face biometrics that conform to this standard. Such a development could enhance inter-operability and personal mobility, including across the many borders in Africa.

2.2 How do ID Systems Evolve?

Enrolling people, protecting and maintaining data systems, checking for fraud, updating entries, and authenticating identities requires effort, time and money. ID services are therefore always provided in response to an actual or perceived need. This may relate to national security or to a program of national re-integration, or to an urgent need to improve the management of public programs. However, the uses of particular ID systems may not correspond to the original reason for introducing them. Even as foundational systems are used for particular functional applications (the national ID card is presented

[12] Some of the many examples include Pakistan, Greece, Cape Verde, Hong Kong and Macao. http://www.icao.int/security/mrtd/Pages/default.aspx

for KYC purposes to open a bank account), functional systems sometimes evolve into multi-purpose ones. For example:

- In the US, the social security number is used for a far wider range of purposes than originally intended because of the absence of a national ID system. In addition, since the events of 9/11 the state-issued driver's license (held by about 80% of adults) has been transitioning towards the dominant form of state-issued ID.

- Bangladesh is building on voter ID to create a national ID system. [13]

- South Africa's comprehensive registration program was developed for the particular purpose of controlling population movement during the Apartheid era. It was re-purposed to underpin the extensive system of social grants that emerged after the political transition in 1994 (Breckenridge 2005). The recent rollout of its eID card was mainly impelled by security concerns (widespread use of counterfeit or stolen ID books and some 5 million undocumented migrants) but it is also used to reduce financial fraud and will underpin a comprehensive system of health insurance.

ID systems developed for one purpose can therefore evolve to be used for others that were not envisaged when the system was initiated.[14] They can spur demand for new social programs and services as previously invisible segments of the population are made visible to the state and other service providers. The provision of ID services can thus create a virtuous circle that strengthens both the demand for identification systems and development.

At the same time, the experience of countries such as Ghana, Nigeria and others shows that programs can languish at low levels of coverage if they are not seen to provide useful services. Despite years of effort, Nigeria's national ID coverage stands at barely 7 million, a fraction of the 69 million voters who were registered for the 2015 elections. The same is true for birth registration -- the challenge is not only to make it easier for administrators – though this is needed and is happening through the use of ICT – but to incentivize parents to want to register their children. South Africa rapidly increased its registration rate, from 40% to over 95% in less than a decade, by requiring birth certificates to access a generous program of child grants (Statistics South Africa, 2012).

As ID systems evolve, it is important that point of service (POS) infrastructure follow suit to enable the appropriate use of the ID provided. There is little point in issuing sophisticated eID credentials with chips and biometric identifiers if the only way to authenticate the holders at points of service is through visual inspection.

[13] For more discussion of paths towards identity systems see Gelb and Clark (2013a).

[14] This can make it difficult to operationalize the principle of informed consent -- that personal data provided by an individual to such a system is used only for the purposes that were originally intended (section 6).

This is not to say that all applications need to be able to use the full identification capability enables by the system[15]. Visual inspection of a card photo and its holder may be adequate for many purposes depending on the level of identity verification needed. Some cards include both barcodes and chips to enable a wider range of use.

2.3 Legal Identity or "Official" Identity?

Harbitz and Molina (2010) define legal identity as "legal civil status obtained through birth registration and civil identification that recognizes the individual as a subject of law and protection of the state." However, identification, as used in the broader sense, may or may not imply any particular legal status, in particular citizenship or nationality or even legal residence.[16] Identification can be seen from two perspectives – supporting individual rights and claims (the need of the individual to be recognized and authenticated), and supporting administrative requirements (the needs of the state or another entity requiring that the individual be identified). Many of these claims and requirements are based on a particular status but not all are, especially when we consider the wide range of development programs that require accurate identification to function well.

Gelb and Clark (2013a) therefore develop a broader concept of "official identity" which is defined to include the various forms of identification that individuals can use to identify themselves for interactions with formal institutions, such as government agencies and programs or employers or banks. Official identity may or may not be associated with legal status. A passport or a national ID card will be bundled with the particular ID+ attribute of nationality. Nationality is included as one of the basic rights set out in the Universal Declaration of Human Rights and the Convention on the Rights of the Child because of its critical importance for accessing many other rights and privileges. But the acceptability of official identity for a particular purpose depends on the particular requirements at hand –

[15] As an example of the POS infrastructure lag, while there is an ICAO standard on digital passports, there is no similar standard for their use at border crossings because not all posts are similarly equipped. One approach to the POS problem is to allow for interim technology. For example, the issue of Israel's secure chip-based eID card was accompanied by the issue of Senior Citizen cards with less secure barcode technology to enable holders to access a wide range of services. Combining the chip and barcode in one card risks undermining the extra security provided by the former. Nevertheless, South Africa does combine these technologies in its new National eID card because not all POS are equipped to handle chip technology. Sources: presentations by Ofer Ishai ("eID Services, eSignatures, eDocuments - The Road Map of Israel") and Professor A.D. Mbewu ("The South African Smart ID Card Project: Restoring Dignity and Identity to all South Africans - Next Steps") at the eID Conference, 7th Edition, Washington DC 28-29 September 2015.

[16] At least 10 US states permit undocumented aliens to hold driving permits because of the desire to encourage them to pass a test and be insured. These permits have no bearing on their legal status and are differentiated from regular ones that serve as the most common type of ID. Estonia's recent e-Residency program is another example: "An e-resident will be a physical person who has received the e-resident's digital identity (smart ID-card) from the Republic of Estonia. This will not entail full legal residency or citizenship or right of entry to Estonia." (E-Estonia 2014). India's Aadhaar is accepted for KYC purposes but confers no right of citizenship or legal residence.

not necessarily "who are you?" but "are you entitled to perform this transaction?" Sometimes it is simply necessary to ascertain that an individual has passed a driving test, or is consistently identified through a course of vaccinations or to be reasonably certain that the student who actually sits a test is the same person who enrolled for the examination.[17] We therefore use "official identity" in preference to "legal identity" to separate identification and status.

What counts as 'official' identity? Countries are not always consistent in their treatment of identity credentials. Some are considered as evidence of status while others are seen as facilitating the administration of particular programs. Birth certificates do not convey the same rights in all countries. Except in the relatively few that automatically grant citizenship on the basis of birthright *(jus soli)*, they do not constitute proof of national status.[18] In many countries candidates for a national registration have to go through an additional process of screening, usually by local officials and prominent members of their communities. In Kenya (especially in border areas), Nigeria and Somaliland, such screening requires proof of ancestry, sometimes several generations back. [19] These processes, and the decisions taken by officials, have become the effective adjudicators of claims to nationality.

At the opposite end of the spectrum, enrolment for the Aadhaar – now the largest ID system in the world with a gallery of almost 950 million -- requires only minimal personal data: name, age and address. It is recognized by the Reserve Bank of India as valid identification for opening a bank account but cannot on its own support the issue of a passport[20] as it is issued equally to citizens and others who claim to be resident.[21] Aadhaar may qualify as official identity but it does not confer legal identity in the sense generally understood.

Voting is one of the most fundamental rights of citizens so that voter cards ought logically to be evidence of full legal identity. However, elections are often conducted on the basis of

[17] Concern over widespread examination fraud caused the introduction of mobile biometric identification before examinations by the West African Examination Council, Nigeria. Candidates are enrolled when registering for the examination, and their details are included into a mobile database provided to examiners. The system checks attendance and validates identities.

[18] Only around 30 countries grant citizenship on the basis of jus soli, mainly in the Americas (Feere, 2010).

[19] The extent of the screening process and the number of supporting documents required also differs for different groups within countries. In Kenya, for example, Kenyan-Somalis and Nubians have to undergo additional 'vetting' to obtain their ID documents (KNCHR 2007; Oppenheim and Powell 2015)

[20] The Aadhaar may still be used to improve the management of the passport system but this is an administrative purpose: http://passportindia.gov.in/AppOnlineProject/pdf/Aadhaar_Passport_Seva.pdf.

[21] The US Social Security Number is another example of a credential issued to citizens and residents, even those such as G4 visa holders who do not participate in the social security system. Most countries do of course issue identity credentials to non-citizens but often they are differentiated.

voter credentials that are not otherwise accepted as full evidence of national status.[22] Indonesia's Constitutional Court has ruled that only a birth certificate or passport provide evidence of existence as a citizen, but many people do not have either of these credentials. The more widely-held e-KTP or electronic ID card is accepted as a credential for voting. It is based on the ubiquitous family card system and national civil administration database (SIAK) which is considered as administrative data rather than providing evidence of identity (Sumner 2015). Togo provides a further example of the continuing importance of local attestation and the complexity associated with the determination of nationality (Box 1).

Box 1. The Complexity of Nationality in Togo

A review of Togo's electoral roll ahead of its 2015 elections revealed that the identity of over 75% of its 3.5 million registered voters has been verified exclusively through testimonies of village chiefs without any 'official' (state-issued) proof of identity or nationality (CENI, 2015). While being allowed to vote represents de facto recognition of Togolese nationality, those who seek to hold a Togolese ID card in addition to their voter ID, first need to obtain an official certificate of nationality. This, in turn, is conditional on the applicant holding a birth certificate or being able to present a birth certificate of a close relative (La Cour d'Appel de Lome, 2015) -- a condition that many Togolese cannot fulfil. UNICEF estimates that about 22% of births of children under the age of 5 have not been registered, while the share of adults without a birth certificate is considerably higher. Deficient birth registration coupled with the combined cost of $16.5 for the certificate of nationality and the ID card prevents most Togolese from obtaining these credentials (median daily income in 2011 was $1.25). In contrast, voter cards are free and cover almost all of the country's adult population.

Entities may require a higher degree of identity assurance than is provided by existing government-issued credentials. They may establish costly ID systems, not so much as to verify status but to be sure that individuals are uniquely identified. Faced with escalating identity fraud, banks in some Latin American countries have established consortia to pool ID data from an industry-wide fingerprint-based system. The complete re-registration by SASSA in South Africa of 16 million recipients of social transfers to weed out duplicates and ghosts is another example (Bruni forthcoming). These cases show the high value placed on robust official ID and also the problem that having many separate systems can escalate the costs of accurate identification.

Official identity therefore can include a rich variety of credentials, each with particular historical and legal underpinnings and issued by institutions with particular mandates. This diversity does not help efforts to validate credentials. One study identified over 14,000 different versions of birth certificates, issued by some 6,000 entities (Department of

[22] Following the recent decision of India's Supreme Court that the Aadhaar should be seen in a similar way. http://timesofindia.indiatimes.com/india/Supreme-Court-allows-linking-Aadhaar-with-PDS-and-LPG-subsidies/articleshow/48444953.cms

Health and Human Services, 2000). Few embodied security features. Not surprisingly, the great variation constituted a severe impediment for officials seeking to assess the validity of a certificate. Some countries, such as Mexico, have since taken steps to develop a standardized birth certificate including a digital stamp, but the only current global standard for identity documents is that for the ICAO e-Passport.[23]

3 Who Has "Official Identity"?

Because of the diversity of credentials and incomplete data on live coverage, it is not straightforward to enumerate the number of people who have official identity and the number that does not. We first summarize estimates of children whose births have not been registered and of individuals without either a birth certificate or a widely-held credential such as a national ID card or number. We then present estimates of the coverage of voter rolls. All of these data are subject to considerable error and do not allow for the quality of the identity, but provide an initial perspective on countries that are more or less advanced in providing civil registration and identity services.

3.1 Birth and Death Registration

Registration of birth and the issuance of a birth certificate are usually the first steps towards establishing an official identity. A birth certificate is often required to access public services, such as education or to sit examinations or receive social grants. In the traditional "OECD model", it is the breeder document for the additional identity credentials such as voter cards, national identity cards, or passports that enable full participation in a modern society and economy.

Data on registration rates in developing countries is only collected periodically (about every five years) through Demographic and Health Surveys and Multiple Indicator Cluster Surveys. Thus global estimates released in any given year can reflect the state of birth registration in some countries up to a decade before the date of publication, and there can be large year-on-year revisions in published estimates as new survey results are released. Not all countries have been covered in all periods. With these caveats, Table 1 shows a positive trend in the registration of children aged 0 – 5 over the last 15 years. A number of developing countries have been making strides towards more comprehensive registration. According to UNICEF data, India has more than doubled the share of children under 5 years registered at birth in under a decade: from 41% in 2006 (reported in 2013) to over 83% in 2011 (reported in 2014). Globally, birth registration coverage rose from 58% in 2000 to 65% in about 2010 (an average of survey dates as reported in 2013) and to 72% as reported in 2014, with relatively large gains in South Asia (driven by India), and Latin America.

[23] See: http://www.icao.int/security/mrtd/Pages/default.aspx

In the least developed countries registration increased from 30% to 38%. However, Sub-Saharan Africa is lagging, with very little change, on average, over the last decade and a half. Some countries have performed remarkably well: Niger doubled registration rates from 32% to 64%, Mozambique increased coverage from 31% to 48% and Benin from 60% to 80%. Others, such as Zimbabwe, have seen marked declines in registration in the last ten years; Nigeria had an uptick around 2011 reaching over 41% coverage and then a fall back to 30% in 2013.

Table 1
Birth registration rates 0-5 years by region

	Birth registration rate (under 5s)[24]		
Region	**2000 estimates**	**2013 estimates**	**2014 estimates**
Sub-Saharan Africa	42%	44%	41%
Eastern and Southern Africa	37%	38%	36%
West and Central Africa	43%	47%	44%
South Asia	31%	39%	71%
East Asia and the Pacific	No data	No data	79%
Middle East and North Africa	No data	87%	87%
Latin America and the Caribbean	83%	92%	92%
CEE/CIS	92%	98%	98%
World	**58%**	**65%**	**72%**

Source: UNICEF 2013; UNICEF 2014

How many children are not registered? Based on the 2013 UNICEF estimates Dunning, Gelb, and Raghavan (2014) estimated some 750 million children under the age of 16. The 2014 data would bring this down to about 650 million. UNICEF (2014) estimated that there were over 2 billion individuals whose births had not been registered. Even among those whose births have been registered, many do not receive a birth certificate: 70 million in the 0-5 age group according to UNICEF (2013). They thus lack a key building block for legal and official identity.

Registries in many countries are in poor condition. Many are yet to be digitized – a task that can involve scanning entries in hundreds of thousands of volumes and entering the information into a database. The cost can be high, especially if the information is decentralized and held in many local registries.[25] Without knowing the birth number of an

[24] Estimates reflect latest data available in given year, which may be up to a decade old, but it usually reflects surveys results between 1-5 years prior to publication. Large year-on-year revisions in published estimates (as seen for South Asia between 2013 and 2014, for example) thus reflect changes over periods up to a decade long.
[25] For Morocco it is estimated to cost $0.90 to digitize each existing entry in addition to the costs of shifting new entries from paper-based to digital format (J. Atick, Presentation to Connect:ID, Washington DC, September 2015).

entry it can be difficult to locate it. This can prompt duplicate registrations as people find it easier to create a new entry than locate the original one. Conflict has destroyed the birth records in some countries. This undermines the value of any paper-based credentials that have been issued, as it is not possible to verify them against a register.

Barriers to birth registration: poverty and geography. Within countries, rates of birth registration are higher for institutional births than for births at home and sometimes differ across ethnic or religious groups. Income is a major factor: globally, on average those born to the poorest quintile of households are about a third less likely to be registered than those to the richest. The gap between rural and urban households is similarly large. In Pakistan and Sudan rural registration rates are as much as 35 percentage points lower than those in urban areas and children in the poorest families are over two-thirds less likely to be registered as those in the top income quintile (Table 2). Registration rates between male and female births differ in some countries but not usually by much. However, relative equality in birth registration rates across the sexes does not accurately reflect barriers to other forms of ID later in life.

Table 2
Countries with the greatest income-based differences in Under 5 birth registration

	Birth registration rate		
	Poorest 20%	**Richest 20%**	**Income-based difference**
Sudan	26%	98%	-72.0%
Pakistan	5%	71.4%	-66.4%
Cameroon	27.9%	88.7%	-60.8%
Nigeria	6.7%	64.9%	-58.2%
Mauritania	32.6%	84.4%	-51.8%
Tanzania	4.40%	55.8%	-51.4%
Guinea	37.6%	88.8%	-51.2%
Senegal	46%	94.1%	-48.1%
Yemen	3.3%	51.2%	-47.9%
Indonesia	40.5%	87.9%	-46%

Source: UNICEF 2014

While birth registration is critically important, its absence does not necessarily mean that a child is not officially known to exist. In Indonesia, children not registered at birth are often recorded on family cards, which list the name, address, date and place of birth the head of the household and all family members. This information is entered in the SIAK population database. However, the children remain vulnerable to the discretion of local officials as the birth certificate (or passport that requires one) is the only legally recognized evidence of citizenship and is required to attend school, for government employment and other purposes (Gelb, 2015, Sumner 2015).

Death registration is crucial for measuring actual ID coverage, yet data are incomplete for many low-income countries. The most recent figures cited may go back two decades and be reported within a wide and not very meaningful range, such as 'under 90%'. The United Nations provides point estimates for death registration in only 11 low -income countries[26] and 33 lower middle income countries[27] (UNSD, 2014). The median death registration rate among these low-income economies is only 14%, ranging from 2% in Niger to 51% in Rwanda. The median death registration rate for the lower-middle income states is a more encouraging 68%, ranging from 5% in Sudan to close to complete coverage (over 95%) in post-Soviet states such as Armenia, Kyrgyzstan, and Ukraine. There are also large variations between sources and years: India's death registration is reported at 48% by the UN as of 1994 (the most recent report from that source), but at only 8% by the WHO in 2012.

3.2 Civil Identification: Coverage of National ID and Similar Programs

Few developing countries have reliable data on the share of the adult population with a national identity card. Even if data exists on the number of cards issued and outstanding, the number of living card holders remains uncertain if death registration rates are low. Kenya –where ID cards are mandatory above the age of 18 - has issued some 24 million ID cards to date, with 1.2 million new registrations each year. This is close to the country's estimated adult population but the number of active holders cannot be determined -- only 46% of deaths have been registered so that many IDs issued in previous years have not been de-activated.[28] Low death registration coverage, coupled with missing data, poses a challenge for assessing live ID coverage in many developing countries.[29] Estimates of coverage by the World Bank's ID4D program as well as by others[30] indicate that coverage can be over 90% in some countries like Peru, Chile or Pakistan but less than 20% for others such as Tanzania, Ghana or Nigeria.

Combining estimates of unregistered children with estimates of adults lacking a national ID or similar credential, the World Bank's ID4D program concluded that around 2.4 billion

[26] Niger, Benin, Nepal, Gambia, Liberia, Togo, Uganda, Zimbabwe, Kenya, Rwanda

[27] Sudan, Zambia, Yemen, Lesotho, Morocco, Ghana, Swaziland, Vanuatu, Cameroon, Pakistan, Senegal, Republic of the Congo, India, Honduras, Samoa, Paraguay, Nicaragua, Solomon Islands, Syria, Kiribati, El Salvador, Uzbekistan, Sri Lanka, Guyana, Georgia, Philippines, Republic of Moldova, Guatemala, Egypt, Kyrgyzstan, Ukraine, Mongolia, Armenia

[28] On the basis of the cumulative number of adult deaths since the last comprehensive re-registration in 1995, live coverage of Kenya's ID might be on the order of 88%. It is known to be lower --around 50%-- in the sparsely populated Northern areas. ID cards do not expire in Kenya.

[29] India's UID program has no need to cancel the identity of the deceased because authentication is directly on the basis of biometrics, but it is still the case that the number of Aadhaar numbers issued does not necessarily reflect live coverage.

[30] An ongoing review by the University of Washington covers 43 developing countries and 48 programs. Coverage estimates sometimes differ greatly between this source and the World Bank ID4D data.

people lack official ID.[31] This number should only be viewed as a rough assessment but it provides some idea of the scaling-up needed to provide all with core identification.

3.3 Elections and Other Forms of Official Identification

Competitive elections galvanize political parties and movements to register a large share of the population. Nigeria offers one of many examples, with some 70% voter registration during its latest elections contrasting with several different national ID initiatives that have failed to enroll many Nigerians. As in the case of Togo (Box 1 above), governments may enact special provisions to ensure that those lacking official identification are not disenfranchised. Electoral officials often accept witness testimonies about an individual's identity and eligibility from village leaders or relatives (Carter Center 2012)[32]. In Liberia, where less than 5% of the population is registered at birth, the sworn testimony of two other registered voters or a confirmation by a traditional leader is accepted as proof of identity. As noted previously, voter cards are not necessarily accepted by (public and private) service providers as proof of legal identity or eligibility for a service, but they are often the most widely-held ID credentials in low-income countries, and also in some middle-income ones such as Mexico.

Reported voter registration rates are surprisingly high (Figure 3). In low-income countries they vary from around 50% of the voting age population in Cameroon and Ivory Coast to close to full coverage (above 90%) in the DRC, Tanzania, and Sierra Leone[33] (IDEA 2015). Reported coverage is often higher than the rate of birth registration in poor countries – the opposite of the pattern in rich ones. Actual coverage depends of course on the quality of the voter roll. The cleaning of Pakistan's voter roll for the 2013 election found that 45% of the existing roll consisted of "zombie" voters – deceased voters, voters with no valid ID or duplicate voters (Malik 2014). Ghana's 2012 voter roll is similarly suspected of being heavily padded with false entries.[34] The true coverage of some of the programs could therefore be lower than indicated by the data.

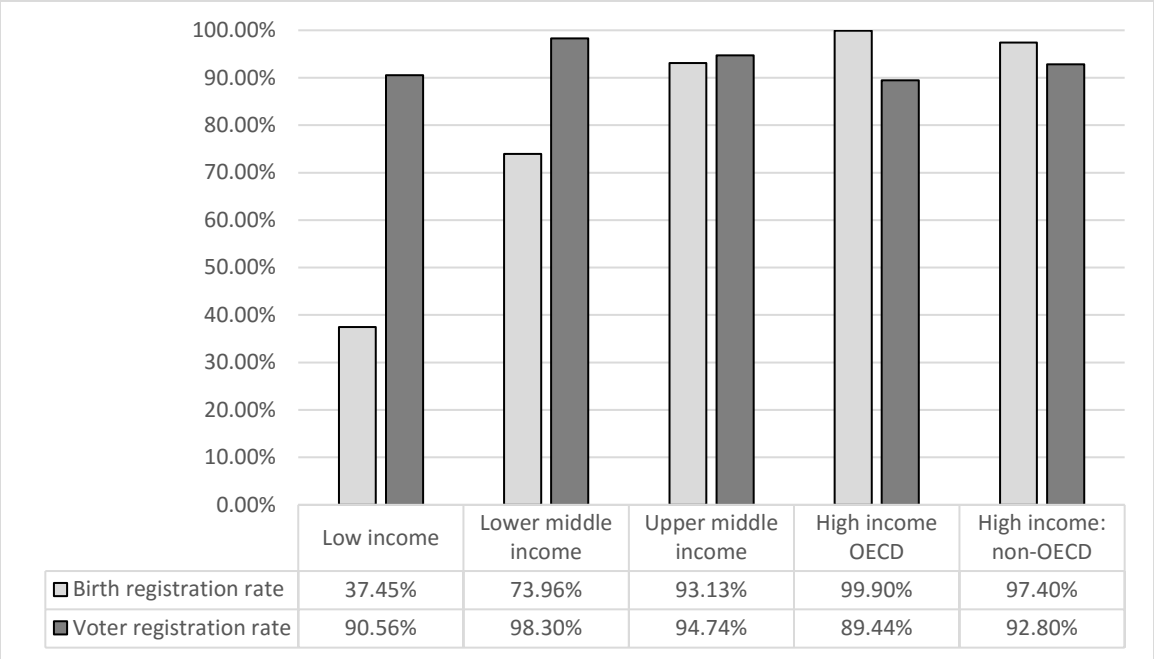
[31] Voter registration was used in some countries where it was not possible to get an estimate of the coverage of a national ID.

[32] Testimonies may also be accepted in lieu of official documentation for registration for national identity cards in countries with deficient civil registration or where records were destroyed due to conflict or natural disasters. For example, in Afghanistan the chief of the village, the imam, or the representative of the district can confirm the identity of applicants for the identity card ('tazkira'). See: http://www.justice.gov/sites/default/files/eoir/legacy/2014/01/16/AFG101176.pdf.

[33] As death registration rates in many low-income countries are very low and voter lists are not updated regularly and reliably in all countries, the number of registered voters (or voter cards issued) and the number of actual, living individuals eligible to vote in the country can differ significantly.

[34] Ghana's case shows that biometric registration may not always result in a clean roll: See: http://www.ghanaweb.com/GhanaHomePage/NewsArchive/Why-Ghana-Has-Probably-the-World-s-Worst-Voters-Register-313424

Figure 3
Average birth- and voter registration rate by country income



	Low income	Lower middle income	Upper middle income	High income OECD	High income: non-OECD
Birth registration rate	37.45%	73.96%	93.13%	99.90%	97.40%
Voter registration rate	90.56%	98.30%	94.74%	89.44%	92.80%

In addition to voter registration, functional ID programs provide many other types of official ID -- (state-issued) health insurance cards, social security cards, family cards, ration cards and many others. Some of these programs can be very large. India's health insurance program for the poor – the Rashtriya Swasthya Bima Yojna (RSBY) – has captured the photographs and fingerprints of over 140 million individuals and issued smart cards to over 36 million families below the poverty line (RSBY 2015). The Philippines' National Health Insurance Program has over 86 million members (87% of the total population) and issues its own ID card, which is considered an official government ID (PhilHealth 2014). In the absence of strong centralized ID management there are often inconsistencies between the different databases of functional ID programs.

The proliferation of ID projects within countries further complicates estimates of the number of people without some form of official ID. In Nigeria, for example, a 2006 report by the Committee on Harmonization of National Identity Cards identified 12 ongoing ID card projects at the time, including 8 with biometric components (Gelb and Clark 2013a). A biometric national ID program was launched in 2003 and registered 37 million citizens but has since been abandoned. In 2014, the country launched a new national e-ID program in cooperation with Mastercard that has enrolled 7 million residents, with plans to enroll a total of 13 million during the pilot phase. This slow progress contrasts with the rapid enrollment of voters in the run up to the 2015 elections.

3.4 Strategies towards providing official identity for all

Efforts to strengthen identity systems and ensure that they contribute to development programs have to take the initial conditions of the country into account. In some cases programs must start from a clean slate. In others the priority is to strengthen the existing system and the POS infrastructure to use it. In still others the task is to move from "confusion to inclusion" and to rationalize multiple programs.

Strengthening the basic civil registration process is a high priority in many countries but it is not the only item on the agenda. Equally important are to better integrate registration and the ID system and ensure that priority applications provide an incentive to register in a way that strengthens, rather than fragments, identity management. As further discussed below, this requires a strategy to develop broad-based engagement to support the use of an ID system to harness momentum for registration. It is important to balance "carrots and sticks". Because of the importance of inclusive development ID should be managed to facilitate access to services rather than be an additional barrier for the poor and marginalized.

4 Architecture and Quality of Official ID Systems

Understanding the choices faced by countries requires a closer look at the quality of official systems and the architecture behind them.

4.1 Institutional Arrangements for Civil Registration and Identification

Institutional arrangements for managing civil registration and national ID programs are depicted in Table 3 for 176 administrations. In about half of the cases the two functions are located in the same entity, usually the Ministry of Home Affairs or the Ministry of Justice. However, this does not necessarily ensure that they are coordinated. Registration and identification can be in different departments of the same ministry, each with a particular legal mandate and with separate processes and data systems. Registration into a family card in Indonesia, for example, does not automatically trigger birth registration, or the other way round.

Otherwise, there are many variants. Civil registration is often managed at state or municipal level or by communes, and on a more decentralized basis than the ID program which is almost always managed at national level. In some countries, civil registration and identification have different networks of decentralized facilities – integrating services could bring substantial savings. In a number of countries, the Election Commission or a similar body is responsible for civil registration and/or for the ID program. This pattern seems to be more prevalent in Latin America and the Caribbean than elsewhere.

Table 3
Institutional Arrangements

		NID organization							
		Min. of Justice	Min. of Interior/ Home Aff.	Min. of Health	Electoral Body/ Org.	Sub-national	Indep. NID org.	Other [35]	Total
Birth registration	Ministry of Justice	12	14	0	4	0	0	1	31
	Ministry of Interior/ Home Aff.	0	48	0	2	3	0	2	55
	Ministry of Health	0	12	0	0	0	1	3	16
	Electoral Body/Org.	0	1	0	5	0	1	0	7
	Sub-national	1	19	0	1	4	2	2	29
	Indep. NID org.	0	0	0	0	0	2	0	2
	Other	2	15	0	1	0	2	13(M) 3 (UM)	36
	Total	15	109	0	13	7	8	24	176

Source: ID4D Preliminary Data.

Please note:
(1) Categories and assignments have been revised from the original ID4D classification.
(2) M =matched (same institution). UM = unmatched (different institution).

Autonomous public ID providers. Several countries task an autonomous agency with the clear objective of providing registration and identification services. Two prominent examples include RENIEC in Peru and NADRA in Pakistan. Both were established as part of nation-building processes.

RENIEC emerged from the breakup of the National Jury of Elections into three entities, the first dealing with registration, the second to organize the elections and the third to rule on electoral processes. An important priority was to re-integrate a country severely disrupted by the Shining Path insurgent movement, which had destroyed much of the civil registration system. This included extending registration to cover indigenous communities, many of which had not been included in national registration. Under the 1993 Constitution, RENIEC acquired autonomous status with a chief officer appointed by open competition for a four-year term. RENIEC does not depend on any ministry but has direct coordination with the Congress, Ministry of Economy and Foreign Affairs (Reyna 2014).

Pakistan's first registration office was established in 1973 at a time when there was little information available to the government of Pakistan on its population. The current form of NADRA as an autonomous organization was created by the "NADRA Ordinance" of 2000, introduced with the aim to accelerate lackluster performance by reducing government interference in the registration of people (Malik 2014). NADRA's chairman and board members are appointed for a statutory term of three years but must retire on attaining the age of 65 years.

Both RENIEC and NADRA have greatly expanded registration. Between 2005 and 2013 RENIEC increased its register by 89%, towards almost total coverage (98%). From 2008 to 2014 NADRA's enrolment grew by 80%, with more rapid growth for women (104%) than men (65%), and towards a high overall coverage level. Both are regarded as technically superior institutions. Both introduced flexible ways of bringing registration services to isolated and excluded groups through connectivity and mobile units including, in the case of NADRA, man-pack registration kits carried by operators to penetrate mountain areas. Registration units for women in sensitive areas were staffed only with female drivers and operators. Both NADRA and RENIEC were able to link registration with access to a variety of programs – transfers, emergency relief and voting – to encourage people to enroll.

Like most other providers of ID services, RENIEC and NADRA charge fees for some services while ensuring that basic registration is available without charge. NADRA has taken this further; it receives no regular budget allocations and funds its operations through charges for fast-track and premium services (such as smart ID cards) to individuals and ID-related services and projects for other parts of government as well as fees from banks and other

entities that need to authenticate clients. It also competes successfully for external contracts and has won many of them, including in Bangladesh, Kenya, Sri Lanka and Sudan. [36] Total revenues tripled over 2008-2013, enabling higher salaries and an increase of 60% in staffing. The proceeds have been used to cross-subsidize outreach to remote communities and the free registration and provision of ID cards to the poor.

The possibility of such a quasi-commercial model – which is made more viable by the growth of demand for e-ID and remote authentication[37] -- raises the question of whether identification should be considered a public good or as a service to be provided subject to cost recovery. The answer is clearly the former if approached from the perspective of human and legal rights and also in terms of the administrative and data externalities from robust identification. However, locating registration and ID services in an independent entity with a clear mandate and some commercial incentives offers three potential advantages:

- It may facilitate a more "technical" approach. Both NADRA and RENIEC are widely regarded as effective institutions with clear mandates to deliver identification services and at least partly insulated from government agencies with particular interests that could create actual or perceived implementation bias.

- Commercial incentives can be useful. NADRA's offices do not follow regular government hours but have autonomy to remain open for longer periods if the employees see opportunities for more business and higher bonuses.

- It may help to integrate civil registration and identification, as well as the system as a whole. ID programs are often more centrally managed than civil registration, and this stronger central direction can be helpful for modernizing the system and introducing new technology. Combining registration and ID facilities could increase access while reducing costs. The approach could also help to integrate voter services. Concern over the independence of a program managed by the Interior or Justice Ministry is sometimes invoked by supporters of an independent election commission to justify a separate – and costly -- voter ID program. The other alternative -- having the commission responsible for the national ID program – risks reducing the incentive to register individuals who are not eligible to vote.

[36] A public company was formed, NADRA Technologies Limited, registered with the Securities and Exchange Commission of Pakistan. It is wholly owned by NADRA and able to bid for contracts outside the country and earn revenues which are plowed back to support operations. Income from foreign projects was $ 17.6 million in 2013 (Malik 2014).

[37] India's massive Unique Identity (UID) Program (almost 900 million enrolled and climbing) is also envisaged to follow such a model in the future, with an increasing share of revenues anticipated to come from charges for authentication services. A National Indian Identification Authority (NIAI) has been proposed as the successor to the Unique Identification Authority of India (UIDAI) which has so far operated under an Executive Order. The NIAI Bill is currently under consideration by parliament.

Whether or not a country delivers ID services through such a model, it is important to ensure that they respond to the demands of potential users – banks, pension funds, social protection -- rather than being biased towards particular narrow interests. This argues for oversight, or at least guidance, by a body or council that includes the views of a range of users as well as providers. Both RENIEC and NADRA have bodies for oversight, and structures to bring together users and providers of ID services have been created in other countries. The Dominican Republic, for example, created a "Social Cabinet" with representatives from a wide range of ministries as well as the election commission to oversee the strengthening of its national ID program (Gelb and Clark 2013a).

4.2 Architecture: Three Dimensions

The methodology developed with the World Bank to assessing the level of development of countries' ID systems classifies them based on three dimensions, as well as the quality of the supporting legal framework (see later): [38]

- **Robustness**: Are the credentials difficult to forge or manipulate? Can they be verified against a register? Can holders be readily authenticated against their claimed identities? Are there controls to ensure uniqueness and prevent one individual from having multiple identities?

- **Coverage**: Is enrollment high across all parts of the population? Or are people and groups excluded, whether by policy, logistical barriers or the cost of obtaining an ID?

- **Integration**: Is a central system used for multiple purposes? Does it provide for integrated identity management, with a common identifier (number) attached to individual records in different program registers?

While the first two attributes are clearly desirable, integration is a more contentious issue. The major concern is the risk to privacy through the use of the unique number to merge individual records across a wide range of registers (economic, social, criminal and security-related) and the potential ability to consolidate a complete record of engagements and track transactions.

Related to this, some argue that that "encouraging", if not mandating, the use of a common identifier as a condition of accessing programs or transfers coerces people, particularly

[38] http://www.worldbank.org/en/topic/socialprotectionlabor/brief/inter-agency-social-protection-assessment-tools

poor people, to enroll in a ubiquitous ID system even if enrollment is not legally obligatory.[39]

A third concern is that the use of a central system can increase vulnerability to hacking and identity theft, especially if data are not strongly protected and encrypted and individuals are not additionally protected through personal "match on card" identifiers. Data protection is lagging in many countries and the last few years have seen some serious breaches.[40]

Objections to integrated systems can also reflect less benevolent motives. An integrated system can be used to strengthen tax and benefit administration by linking databases on property and vehicle registration, possession of bank accounts, travel, and other income-related indicators. Argentina used its national ID system to integrate such databases across its provinces, increasing tax yields and reducing benefit claims (Gelb and Clark 2013a). Those able to benefit from access to multiple programs will be concerned about the potential to rationalize access around each individual user. The strength of the vested interests against such uses of ID is discussed below, with the example of Pakistan showing how a less favorable political economy blocks potentially valuable uses.

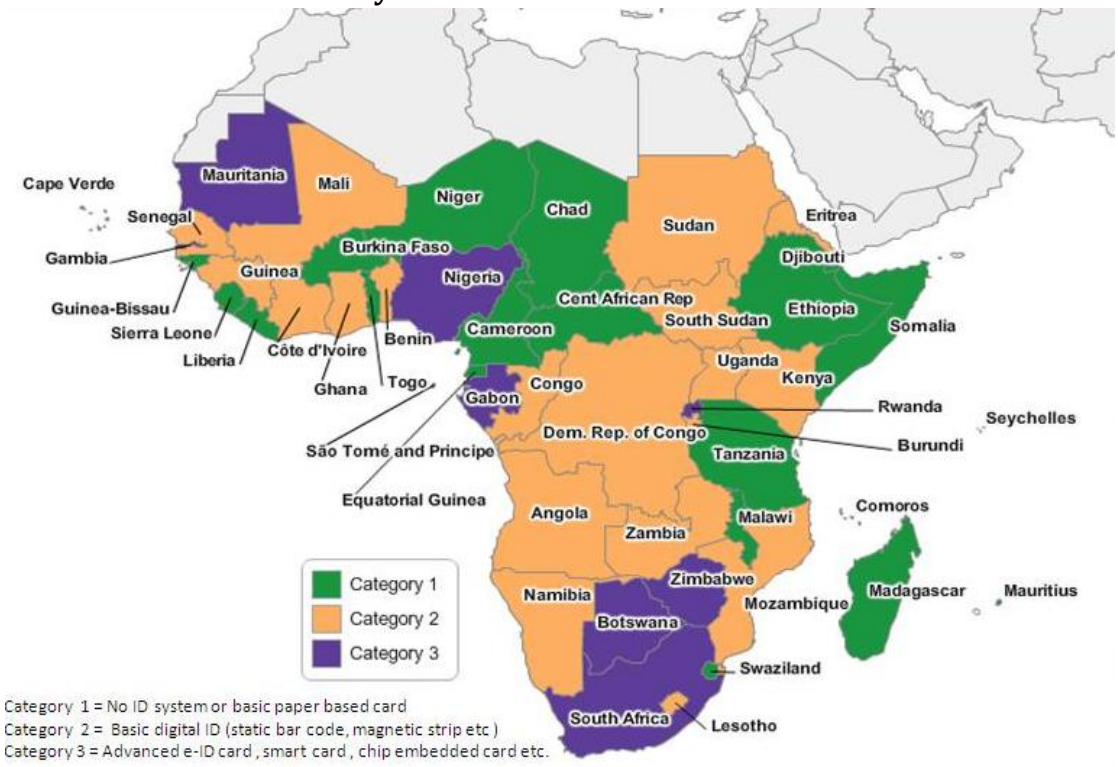
While many countries are making efforts towards stronger core systems, ID integration should therefore be recognized as a social or political choice. Some countries support highly centralized and integrated systems while others are reluctant to implement them.

Figure 4 shows a preliminary summary assessment of the ID systems of Sub-Saharan Africa according to these three criteria. Several, including South Africa, Botswana and Zimbabwe, have relatively advanced systems that score well on all of the dimensions. Others, such as Kenya or Uganda, are classified as intermediate, either because of low civil registration or enrollment rates, less secure credentials, or limited integration. Many other countries have rudimentary systems, scoring low on most, if not all, criteria.

[39] Privacy International, for example, has expressed concern over the integration of social registers across multiple programs, arguing that this coerces poor people to enroll in programs with a wider scope than the particular benefit they are seeking. See Hosein and Nyst (2013). Similar criticisms have been expressed about the Aadhaar program – that pressure to use it in social and other programs is not consistent with its voluntary status. On the other hand, it can be argued that public programs are entitled to require documentation for administrative purposes and that the Aadhaar can be considered in this light.

[40] South Korea faced the need for a comprehensive revision to its system after hackers gained access to ID numbers and other personal data in a massive hack in 2014. The cost implications were estimated at $1 billion. See: http://www.theregister.co.uk/2014/10/14/south_korea_national_identity_system_hacked/. Against this argument, some argue that data protection is likely to be stronger for a well-managed central system than for a system with multiple, dispersed, databases.

Figure 4
ID Systems in Sub-Saharan Africa



More detail on the features of some civil registration/identification systems is shown schematically in Figure 5. The first question is whether the ID system is based on a comprehensive civil registry or whether the system is fractured between registration and identification.

- Most OECD countries, as well as some developing countries, base their identification systems on well-established civil registries with high rates of continuous birth and death registration as well as marriage and divorce.

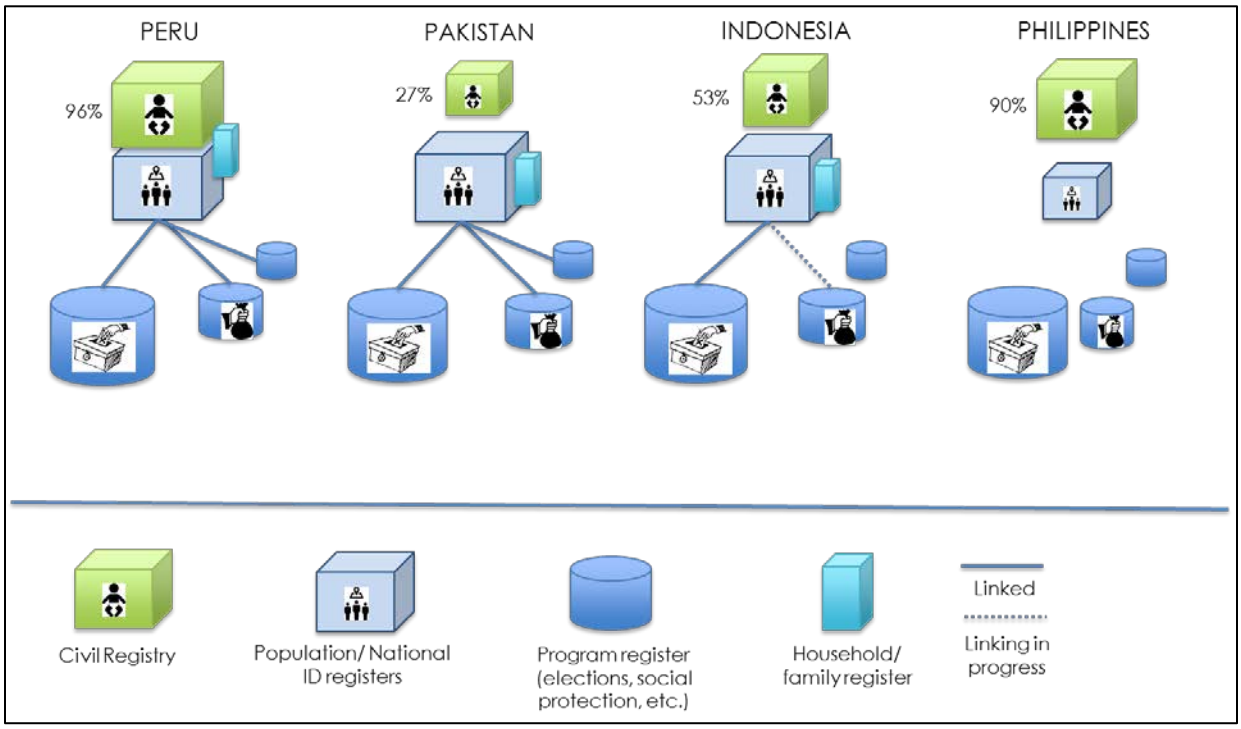
- Pakistan and India are not currently able to do this, and need to conduct separate registration and enrollment exercises. Updating the population register without a continuous record of births and deaths is a challenge. Pakistan maintains three registers – individual, family and household – because the programs supported by NADRA deliver services to all these groupings. To update its registers it uses program interactions such as voter registration drives, emergency relief and social transfers. It also operates a data-sharing protocol, to formalize arrangements to

share data with social and other programs and in turn receive information that can be used to update its own registers.[41]

- Indonesia operates a dual regime with a population registration/national ID system coexisting with an independent and underdeveloped civil registry even though both are in the same ministry. This dual system has led to an inconsistent approach towards identification and considerable difficulties for the poor.[42]

- In the dis-connected picture for the Philippines, the comprehensive birth registry (95% coverage) could constitute an effective basis for a widely held national ID using the birth number as the identifier but – as in the UK and a number of other countries -- concerns over data privacy and surveillance appear to have been important in slowing efforts in this area or blocking a national ID-type program altogether.

Figure 5
Different ID Architectures



[41] India's UID program does enroll children taking biometrics from the age of 5. While it does not provide birth certificates it could be argued that this procedure provides a more robust link between identification and birth identity than traditional paper-based certificates with no security features: see later.
[42] Birth registration is a legal requirement for enrolment into the population register but in practice this has been ignored. Many individuals voting on the basis of identification through the register and the associated ID card therefore lack the only legally valid credential for recognition as an Indonesian citizen, as articulated by the Constitutional Court. At the same time, birth certificates are required for access to certain public services as well as for employment in the civil service (Sumner 2015).

Moving towards identification, Figure 5 shows a number of patterns:

- Peru and Pakistan score strongly in all three dimensions. Both have made particular efforts to register excluded groups and to increase the coverage of their population registers, including through the use of mobile units in remote areas. Both use biometric technology to limit (if not fully prevent) duplicate enrollment and to ensure that each identity is distinguished by a unique number. In both countries the number is required for virtually all engagements between citizen and state as well as for many private transactions.

- Indonesia (e-KTP) and India (Aadhaar) are in an intermediate position. Both have developed core systems using similar advanced enrollment technology, although the e-KTP system involves card-based authentication while the Aadhaar relies on remote biometric authentication against the central database. Both have high, though not yet complete, coverage. Both are in the process of "seeding" their ID numbers into the registers of functional programs to provide subsidies and cash transfers, but integration is far from complete.

- Nigeria and Mexico have still less integrated systems, with some six major systems in Mexico and at least a dozen in Nigeria. [43] The coverage of some of the functional ID programs in such countries can be higher than that of the respective national IDs. Voter registration, in particular, is often de-linked from civil registration/identification with costly registration campaigns managed by the election commission undermining the focus on building up the core system (Section 2).

- Yet another example of a disconnected system is the Philippines. Citizen and civil society resistance to a strong mandatory national ID program in the absence of data protection legislation has slowed movement towards an integrated system and resulted in a disconnected ID architecture. There are reportedly at least 28 separate identification registers and cards in the Philippines although a single individual will hold far fewer of these credentials. [44]

Country assessments under the World Bank's ID4D program have begun to map out the strengths and weaknesses in their ID systems using this analytical framework. Some 10 countries are being assessed each year.

[43] Over the last decade the Nigerian government is estimated to have spent $2 billion on ID programs yet still lacks a coherent system (Reference). A report by the government in 2006 identified 12 ongoing ID card projects, 8 of which included biometrics (Gelb and Clark 2012). Since then there have been more, including the customer identification program launched independently by the banking system (CBN 2015).

[44]. Data privacy legislation approved in the Philippines in 2012 may open the way to a more integrated ID system

5. Towards the Future: Four Frontier Cases.

Identification systems and identity providers face new challenges in today's digital age. Demand for digital identification is rising with an increasingly connected population in emerging economies. Governments are under pressure from better-informed and more vocal voters as well as international donors to cut leakages and improve efficiency. In a survey of 32 emerging and developing nations conducted by the Pew Research Center (2015) about four-in-ten internet users reported going online to get information about government or public services. One-fourth of surveyed respondents in Africa had made or received payments online. As government records and services move online and the number of digital transactions with public and private entities multiply, the creation and verification of trusted digital identities is becoming an increasingly pressing issue.

In response, providers are juggling competing demands for data security, ease of use and privacy. With varied conditions (connectivity, literacy….) as well as different public preferences, digital ID is being provided in different ways by different countries. No one ID system is the most advanced in all possible dimensions. We consider four "frontier" cases of special interest: India (UID-Aadhaar), Estonia, the UK (Gov.UK Verify) and the ID potential of social or professional networks. The first two cases are centralized "top-down" systems with different mechanisms to deliver unique digital identity. The second two cases illustrate the possible shift towards a "federated" or "electronic village" mode of digital identity. At present, the latter models are probably better seen as complements rather than substitutes to "top-down" systems as it is difficult to imagine a full range of identity services being provided through networks. Whether an individual has a Facebook or LinkedIn account and the number of "friends", "likes" or endorsements says nothing about entitlement to a passport or to drive. Nevertheless, the new forms of identity authentication could be quite useful for a range of uses and far superior to older *ad hoc* methods such as basing a determination of identity on one or two references.

5.1 India: The UID Program

The concept of unique identification for all Indians was originally conceived in 2006 but it was not until 2008 that the Planning Commission of India created the Unique Identification Authority (UIDAI). In 2009 it was elevated to a cabinet committee level and Nandan Nilekani, former Chairman of Infosys, was appointed Chairman. Its goal was "to develop and implement the necessary institutional, technical, and legal infrastructure to issue unique identity numbers to residents all across India" and to "issue a unique identification number that can be verified and authenticated in an online, cost effective manner, which is robust enough to eliminate duplicate and fake identities". The prime motivation for the program was to help rationalize India's extensive and complex system of subsidy programs; these represented some 14% of GDP but were poorly implemented and

targeted. Estimates of losses due to leakages and fraud were as high as 71%. A 2008 Planning Commission report demonstrated that, for example, more than one third or 36.7% of grain intended for poor households was instead sold to non-poor households, and that 58% of subsidized grains did not reach intended recipients due to various errors in delivery and identification (Zelazny 2012).

Since the program was launched the remarkable number of almost 950 million people have so far enrolled. The unit cost, at $1.16 per enrollment, is the lowest of any identification program in the world. Some 190 million new bank accounts have been created using UID-issued identification to satisfy KYC requirements, ready to serve as vehicles for MNREGA[45] and other payments. The unique Aadhaar number is beginning to be seeded into program databases; some 60 applications are now estimated to be in process, many at state level. Initial reports suggested that the most developed application, the PaHAL program for reforming LPG subsidies, would save enough over one year to cover the entire cost of the UID program to date (below).

The UID program has attracted great attention and had a major impact on thinking about ID programs and also on the biometrics industry. It is a "frontier" case in several dimensions:

Identity First. UID is a mechanism, an infrastructure designed to establish a person's identity, not to confer rights and privileges. Disputes in this area are misguided, notably with the National Population Register (NPR) that has the mandate to establish citizenship with all its associated rights and obligations. The concern expressed by the Supreme Court that Aadhaar numbers could be issued to undocumented residents reflects a similar misunderstanding of the Aadhaar. This aspect of UID reflects the need to build an identity foundation in the face of the reality that most individuals had only fragmentary and often inconsistent ID credentials.

At the same time the absence of any legislative basis for UID and its undefined scope of application makes it a unique program. It differs from all others in the world (mandatory or voluntary) that are either linked to specific purposes (driver's license) or to status as a national, resident or refugee. Especially in the absence of a legal framework for data privacy this has led to intense debate on whether such a voluntary credential (a status re-confirmed by the Supreme Court) can be required to access subsidies, transfers and public services, pay taxes, register property, obtain a passport or for the many other applications commonly served by nation-wide identity programs. [46] Should the Aadhaar be linked to criminal databases or to border entry? Biometric information is taken in these areas even in countries like the US and UK that reject national ID systems.

Pending a decision on the NIAI Bill (2011) the legal status of UID is not settled. It could become the foundation for a national identity system along the lines of those implemented

[45] The Mahatma Gandhi National Rural Employment Guarantee Act of 2005

[46] It is notable that an Aadhaar number is not essential to participate in PaHAL if the individual has a bank account.

by many other countries. It could also be constrained to the status of a social security credential, providing a unified identity baseline to rationalize the systems of subsidies and social protection and to satisfy KYC requirements for access to basic financial services. Even in this more restricted role its potential benefit is immense.

Biometrics as the Base for Identity. UID collects a minimum of biographic data, relying on biometrics for online identification and authentication. Fused fingerprints, iris and now face are used to de-duplicate enrollments across India's massive population, including children down to the age of 5. At the start of the program it was not guaranteed that this would be possible because of the vast number of pair-wise comparisons necessary and the poor quality of fingerprint images for many manual laborers. Performance data released by the program in 2012 (discussed later) indicate that de-duplication is possible with a high degree of precision. This is only possible with tight quality control including at the point of capture of biometric data. UID's technology has been adopted by Indonesia and is potentially of great benefit to other countries.

UID is also distinctive in that no card is issued for local identity verification. This was a deliberate choice, to save the cost of issuing and managing cards and also to avoid the problems associated with forged credentials. Even though the central database is strongly encrypted, it could be argued that this renders the system more vulnerable to data breaches, in the unlikely event that they should occur, than the match-on-card approach used by Estonia (below). However, once the primary identity of the holder is verified by in-person authentication there is nothing to stop the issue of secondary or derived IDs secured by tokens, PINs or other biometrics. This would be normal, for example, for transactional IDs issued to higher-value customers by financial institutions. The aim of an ID system should be to build on a strong primary identity to enable as wide a range of authentication mechanisms as possible. [47]

Standards-Based Implementation. The third distinctive feature of UID is its certification process, implemented by the Standardization Testing and Quality Certification (STQC) Directorate. Technology suppliers have to submit documentation and three sets of biometric devices for testing. Once approved, certificates have a 3-year validity. Coupled with the large size of the UID program, this has created competition, opened up the biometrics industry, helped to move it towards a "commodity" industry and greatly reduced costs. Computing equipment is off-the-shelf. Proprietary technology is used only in the area of de-duplication, where three providers compete with each other for market share.

In addition, UID has decentralized enrollment. States and territories identify Registrars who then outsource the function to Enrolling Agencies to create some 50,000 enrolment points. This is only possible with tight quality monitoring. In addition to biometric and

[47] Cultural factors can also play a part in technology choice. PINs are routinely shared within Indian families, raising a question about the feasibility of adopting an approach like Estonia's. Even there, it requires constant message reinforcement to ensure that PINs are kept confidential.

biographic data, an enrollment package includes detailed information on the process, including the time taken and the number of repeat takes needed to capture biometrics. The three types of information are processed at the center. This provides continual feedback on the performance of different devices and also on operators.

5.2 Estonia: e-ID and digital identity pioneer

Launched in 2002, Estonia's e-ID system provides citizens and residents with the most comprehensive digital access to government services in the world.[48] In a complex geo-political space, Estonia needed to consolidate its national identity and to demonstrate the ability of its new government to provide services economically and efficiently, including in rural areas. It had the advantage of starting "from the ground up" with a highly educated population skilled in science and engineering. In 2014 close to 83% of all households had a computer and internet connection at home, and 84% of the 16-74 age group were reported to have used the internet in that year.

Estonia's system is underpinned by a state-held population database (national register), which provides all citizens and other residents with an 11-digit unique personal identifier. The database contains each person's name, date of birth, gender, address history, citizenship, and legally recognized relationships. Each person is also issued an email account to provide an electronic address. The personal identifier is used universally by state agencies and by a number of private entities to identify users and link them to their records within their respective systems (medical history, police records and others).

Enrollment is compulsory for citizens and residents at the age of 15. Biometrics (face and 10 fingerprints) are taken to ensure against duplicate enrollments but they are not used for authentication. This is through a smart ID card containing a microchip with two digital certificates: one for authenticating the holder with a PIN called PIN1, and the other for digital signing which requires a separate PIN2. PIN1 is a minimum 4-digit number and PIN2 is a minimum 5-digit number. Both are completely under the control of the user. Authentication is match-on-card rather than against the central database. Digital signatures and authentication are legally equivalent to handwritten signatures and face-to-face identification in Estonia and between partners upon agreement anywhere around the world.

Full Digital Identity. A digital person is then the combination of three things: the PINs, the card and its digital certificates and the database against which their validity is verified at the time of using the card. If the card is lost or the PINs are compromised, the certificates can be cancelled and the holder can re-register for the issue of a new card. Estonia's system therefore uses all three identifying factors: something you have (card), know

[48] Sources: www.e-estonia.com, other refs

(PINs) and are (initial biometrics for registration). Users are protected against breaches of the central database because their identity credentials are under their control. This feature could also reduce incentives to hack into the national register.

Users can verify their identity online by connecting their physical ID via a smartcard reader to their computer or (since 2007) by using a personalized digital ID-linked SIM card in their mobile phone. Residents can view all relevant personal records online, including medical, education, and employment history, register changes in their legal status, file taxes, and complete many other administrative tasks. Since 2005 Estonian e-IDs have also been used for online voting in Estonia's parliamentary and European Parliament elections, with close to a third of voters casting their votes online in the last election.

Since late 2014, Estonia has also allowed for those non-physically resident on its territory to obtain a government-issued digital identity, in the form of an e-Residency. This is the first such initiative for a state to issue identity as a "third party" to individuals with no direct relationship to the country. Applicants need to fill in an online application and provide their biometric data and a proof of identity in person at an Estonian police and border guard office or embassy (E-Estonia, 2014). The fee for establishing a state-verified digital identity is 50 euros. E-residency enables the holder to perform a wide range of transactions in Estonia. It remains to be seen how widely it is accepted as a credential in other countries.

Use of Estonia's ID. While the Estonian e-ID system is anchored in the national population register, databases are decentralized, with each government agency and service provider storing only the user data necessary for their own purposes. The databases are linked through a data exchange layer called X-Road, which allows for the exchange of relevant information between the state's information systems as well as links between private entities (such as banks or employers) and the user's digital identity. It also enables users to query several different databases after authenticating themselves. The system is designed to provide residents with maximum access and control over their data. Estonians can verify what information about them is held in each government system and the reason why this information is retained (Herlihy, 2013). They can also check who has accessed their data and when, with the exception of queries related to criminal behavior and national security. Unwarranted snooping by public officials is punishable by imprisonment.

The 1.25 million active Estonian e-ID cards in use have facilitated over 386 million electronic authentications and over 245 million digital signatures (ID.ee 2015); on average each cardholder makes 50 e-signatures per year. Based on time savings, online access to government services and digital signatures are estimated to have saved over $140 million for Estonians and Estonian companies (Arm, 2014). Another estimate is that digital access saves a typical citizen around 40 hours per year in physical travel and waiting time (Annus 2014). The government has no comprehensive assessment of savings from the ID system

(or additional expenses), but it cites a number of partial figures, including over $2 million in savings for the Estonian Road Administration from using paperless services in 2011 (E-Estonia, 2013). In the last elections, savings from e-voting are estimated at 11,000 working days and 500,000 euros (E-Estonia, 2015).

5.3 "Federated" ID: GOV.UK Verify.

Governments can act as both identity providers and verifiers, as is the case in Estonia and India. They can also certify other digital identity providers and be the primary (or first) users of their services. This is the case in Britain's pilot UK.Gov Verify program. It points to the possibility that ID provision may evolve from 'top-down' systems towards more decentralized or 'federated' models including, perhaps, towards a marketplace for privately-provided identity services. [49]

In state-anchored programs such as GOV.UK Verify, the government defines the key parameters of the identification and verification process but the identity itself is verified (or 'facilitated') through a number of providers who draw on a variety of information from state registries and databases as well as from private databases to authenticate users. GOV.UK Verify uses certified private companies to provide identity assurance in a decentralized manner, enabling users to access a number of government services. The provision of identity and the provision of services are separate so that the service organization has no knowledge of the supporting evidence for identity accessed by the provider. The scheme forms the backbone of the British government's 'digital-by-default' strategy for future public service provision. This aims to build on the high share of Internet users among the population: over 91% in 2014 (ITU 2015).

Gov.UK Verify is motivated by a concern to protect the privacy of users and the integrity of their personal data. As explained by Verify:

"Within the UK there is no official or statutory attribute or set of attributes that are used to uniquely identify individuals across Government. Neither is there a single official or statutory issued document whose primary purpose is that of identifying an individual. Without such attributes or documentation it is difficult for any person to be absolutely certain of the identity of another. […] a combination of the breadth of evidence provided, the strength of the evidence itself, the validation and verification processes conducted and a history of activity can provide various levels of assurance around the legitimacy of an identity". (CESG, 2014)

Prospective users need to provide their name, address, and date of birth at registration. The identity providers can then query databases of government agencies to check the

[49] A study of GOV.UK Verify has been commissioned to provide further detail. For the US the NSTIC (National Strategy for Trusted Identities in Cyberspace) project seeks to establish the basis for such an ID market. http://www.nist.gov/nstic/

validity of passports or driving licenses provided as part of the verification process. They are able to draw on other government sources, such as police databases, to check against fraudulent documents. They can also access records from the private sector, including information from financial institutions and credit reference agencies. While the state has an important role in issuing and maintaining records of the identification that underlies the online verification process, the use of private identity providers enables the government to authenticate residents online in a decentralized manner. This is considered to protect users' privacy and personal data better than having data centralized or using a single unique identifier, such as a number, to access all services (Hughes 2014a).

Identity evidence is collected across three data categories: information on the citizen, information of a financial nature, and evidence of a living identity. The process uses a potentially wide range of documents that can encompass more than one category at a time. They include government-issued identity documents, such as birth certificates, passports, and marriage certificates as well as privately provided evidence such as of a bank savings account, property or car insurance or a contract for a mobile phone account (CESG, 2014). Many of these non-government proofs of identity do require some form of government-issued ID when first established, such as when opening a UK bank account, so that the approach builds on, rather than substitutes for, more conventional forms of official ID.[50]

The number and types of evidence needed for online verification depend on the level of assurance required by the service to be accessed. As set out in Table 4, three of four identity levels distinguished by GOV.UK Verify are currently provided: Level 1 (the most basic identity account); Level 2 ("on the balance of probability" someone is who they claim to be) and Level 3 (the person is who they say they are "beyond reasonable doubt"). The program does not yet support level 4 identity assurance. The verification process for the identity itself has five elements: the identity actually exists; evidence of identity is valid (matching against records); the person owns the claimed identity (verification questions); the identity is not known to be fraudulent; and the identity is active (recent transaction history) (Hughes 2014b). Once an applicant's identity is verified, they can access a variety of government records and services, including driving license records and online tax filing. Access to additional services, such as health records and child maintenance is expected to be available by the end of 2016 (McEvoy 2015).

[50] Gov.UK Verify is increasing the range of supporting documentation to extend the demographic coverage of the system. The process still appears to rely heavily on official identification, confirming its role as a complement to official ID rather than a substitute. See: https://identityassurance.blog.gov.uk/2015/10/20/making-gov-uk-verify-available-to-more-people/

Table 4
Levels of Identity Assurance

Level 1 Identity At Level 1 there is no requirement for the identity of the Applicant to be proven. The Applicant has provided an Identifier that can be used to confirm an individual as the Applicant. The Identifier has been checked to ensure that it is in the possession and/or control of the Applicant.
Level 2 Identity A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings.
Level 3 Identity A Level 3 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of criminal proceedings.
Level 4 identity A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of Biometrics, to further protect the identity from impersonation or fabrication. This is intended for those persons who may be in a position of trust or situations where compromise could represent a danger to life.

Source: CESG (2014)

The program is still in public beta status, with improvements being made to the system regularly. By mid-October 2015 a total of 297,000 verified accounts had been recorded along with 185,000 basic level 1 accounts; for the latter access to each service will be contingent upon answering additional security questions (GOV.UK Verify 2015). The proportion of visits where users have been able to verify their identity online has been on the rise, reaching around 80% in the last three months. The transition to digital identification for government services is expected to save about $1.6 billion from the first 25 pilot services alone (Arthur 2014). The government is planning to take the system 'live' by April 2016.

While the initial roll-out is focused on access to government services, it is possible that the private sector will also be able to make use of this state-approved verified digital identity program at some point in the future. That step will require addressing a number of further issues, including the question of how to assign and limit legal liability for errors in identification. As the sole client so far, government can agree to waive or limit its claims.

Something similar will no doubt be needed if private entities are to take on the service for private clients. [51]

5.4 Social and Professional Networks and Crowd-Sourced Digital Identities

Private companies such as social or professional networks maintain extensive databases that include personal information on users and their lifestyles. This information could also play a future role in providing official digital identity. The role of networks has been limited to date. Decisions on eligibility for government services and access are likely to remain anchored in state-based identities, possibly validated by authorized non-state identity providers as in GOV.UK Verify. However, some private companies may see value in network-based or 'crowd-sourced' identification processes. These bear some parallels to the local peer-based identification used before the emergence of centralized registries where much of the verification process was based on who you knew and who knew you, but extending beyond the physical constraints of 'village-ID' into digital communities.

Members of online communities can now have their identities verified through their connections and activities in the 'e-village'. For example, through OpenID a large number of websites and applications are already relying on third parties -- Google, LinkedIn, Facebook, Yahoo and others – to authenticate users. This benefits the third parties who need features to drive more users to their sites. It benefits the users, who no longer need to memorize multiple passwords but can sign in to multiple applications with a single username and password. It also benefits the client websites and app developers, who no longer need to provide for their own password management systems and who would not anyway have needed stronger authentication than provided by the third party providers.

Private companies have started to use social networks as at least supporting identity providers. Fidor, a registered online bank in Germany, allows new customers to complete its initial registration process using Facebook Connect although customers do need to verify their identity by submitting a state-issued ID and proof of address for full account functionality (Economia 2013). Another example is Lenddo, which has been providing small loans to individuals in the Philippines, Mexico, and Colombia using data from social networks to determine their creditworthiness (Groenfeldt 2015). It is now selling its algorithm, called the Lenddo Score, to financial institutions to facilitate the use of social networks for credit assessment more broadly. If this is indeed helpful, it could possibly encourage financial inclusion in emerging economies where credit reference facilities do not exist or cover only a small fraction of the population.

[51] The issue is less pressing when ID is issued by government since its agencies and staff enjoy broad immunity but could become an important question for ID certification performed as a business by private entities

Facebook offers one example of identification through social media. With 1.5 billion active users worldwide, it has the largest social network data base in the world. About 900 million of its active users live outside of the US, Canada, and Europe making Facebook perhaps the best-positioned potential provider of digital identity in the developing world. Many of its members may not have state-issued identification. Its current identity management processes are far from rigorous, however, and it is also not clear whether a formal identity provision function is compatible with an inclusive business model that depends on having as many users as possible to maximize network externalities.

Official Facebook policy allows only the use of one's real identity. Users are required to submit their authentic name and birthday when registering for an account for the first time. Nevertheless, Facebook does not require new users to submit any specific form of identification when signing up -- verification is solely by the email address or the mobile number provided. There is no need to provide a photo of the user. As well as cats, dogs or other non-persons, users can post pictures of celebrities provided that the clear intent is not to impersonate another individual. If it suspects that the identity provided at registration is not genuine, or that the user is under 13 (the minimum age for a Facebook account,) Facebook can ask the owner of an account for further confirmation of their identity. Users may be asked to submit a copy of a photo ID, with a wide range of both government- and privately-issued ID types accepted. If they cannot comply or are unwilling to do so, their account may be deleted.

This light approach towards identity management reflects the need of a social network to be inclusive while at the same time protecting its business model against the manufacture of fake identities with the purpose, for example to enable a large number of "likes" to be artificially registered to boost a product, service or reputation.[52] As a result of this balance, the number of accounts believed not to be uniquely linked to an authentic identity can be relatively high. In 2012, Facebook released data indicating that about 8.7% or 83 million of its accounts were duplicates or fakes (Kelly, 2012). Duplicates accounted for about 45.8 million accounts, 'non-human' accounts that were created for pets, companies, etc. made up about 22.9 million while about 14.3 million accounts were set up to distribute spam and for other illicit commercial activities. While the social networking site has stepped up efforts to eliminate fake sites in the last three years, its 2014 Annual Report puts the share of fake accounts between 5.5% and 11.2% (between 67.5 million and 138 million).[53]

Even if Facebook credentials are sufficient for many other web applications, such a level of false identities would make it difficult for the company to become a trusted and widely accepted provider of digital identity services. It is also not clear that this function would be

[52] Amazon has recently initiated lawsuits against fake reviewers: http://krqe.com/2015/10/25/amazon-sues-to-stop-phony-product-reviews/

[53] We have sent Facebook a questionnaire asking how they estimate the number of fake or duplicate accounts and whether they use algorithms such as SibylRank or other approaches. We are awaiting a response.

compatible with the social networking function, since tightening up identification requirements would alienate many users and cause them to shift allegiance to other social networks. It is also not clear how Facebook (or any comparable network) would handle the liability issues associated with formally providing identity assurance to third parties. Offering this on a wide basis could also create additional incentives for users to manufacture fake identities that could be very difficult to detect.

With the number of in-person services and transactions advertised (and contracted) online on the rise, online service providers are increasingly interested in verifying both the on-line and the off-line identities of their users. This could involve accessing their public profiles or conceivably by requiring prospective clients to "befriend them" so that they can have full access to their social networks.[54] Airbnb, a website that connects users seeking to rent out their lodging with those looking for a place to stay has recently introduced a 'Verified ID' process on their website, whereby users are authenticated through both their online or offline presence. Online identities can be verified via existing Airbnb reviews and Linkedin, Google, or Facebook profiles (Airbnb 2013). User accounts need not only exist on one of these social networks, but the user must also have a sufficient amount of connections (100 friends on Facebook, for example) to satisfy Airbnb's verification requirements. If users cannot fulfill this requirement, they may upload a video with a personal introduction. Offline identities are normally verified by scanning and submitting an official photo ID.

Another aspect of the new 'sharing economy' is that a growing number of individuals are providing some kind of personal-interaction based service, whether renting out their apartment or sharing their cars. Facilitated by web-based applications, the rise of 'micro-entrepreneurship' has resulted in a large number of personal reviews that can provide proof of existence and -to a lesser extent - proof of location (residence) and other potentially useful data for identification purposes. Professional networking sites such as LinkedIn allow users to endorse their connections for certain skills and to post longer references on each other's profiles. While primarily a developed country trend, e-village testimonies open additional avenues for private service providers, for example in the financial sector, to refer to users' online presence and social networks to verify their identities and validate claims about their creditworthiness – much as a local banker might draw on personal knowledge about a loan applicant and her/his family. However, while an increasing number of service providers draw on data derived from the e-village, most of them also rely on 'traditional' methods of identity verification, requiring users to present official, state-issued IDs to enable access to sensitive information and to be able to transact online. To what extent online communities can act as official (digital) identity providers therefore remains to be seen.

[54] Interviews with Facebook suggest that while this may contravene the spirit of user policy there is no clear way to prevent it.

6. Issues for implementation: costs, biometrics, and the enrolment of children

6.1 Benchmarking ID Costs against Savings

The costs of ID systems differ between countries and depend on many factors: size and the ability to reap scale economies, the approach (high-security cards, low-security cards, no cards), institutional capacity and the detail of data captured by the system. Registration costs also differ within countries being higher in sparsely-populated and remote areas: Reyna (2014) offers estimates for Peru. Table 5 suggests that a reasonable cost range for providing nation-wide ID might be in the region of $3 -$6 per enrolment. India's UID program, which is very large scale, collects a minimum of personal biographic information and does not issue cards, is unusually inexpensive at around $1.16 per head to date: the total projected budget is only $2.2 billion for a potential coverage of 1.3 million people.[55] Maintaining and updating the database typically costs an additional 15%- 25% while the costs of each ID card varies greatly depending on the material and embedded features.

These costs do not include those of the POS infrastructure needed to use the capabilities of the eID. In many cases this will be supplied by users, such as banks, who benefit from reduced levels of identity-related fraud provided by accurate ID. In other cases it may need to be supported by public funding. In determining the mix between on-line and off-line authentication, much depends on the level of connectivity.

Table 5
Costs of eID Systems

Component	Description	Investment
Enrollment	Capturing identifiers at points of enrollment including biometric and biographic data	$3 - $6 per person (Aadhaar low case, $1.16)
Register Maintenance	Database management and maintenance, updates, deduplication, other checks	+15% – 25% per year
Authentication Services	Mechanisms for verifying identity such as smart electronic cards that contain credentials on a chip (PINs, biometrics, PKI certificates) or online verification services	$1.15 - $5 per ID card depending on features +$0.50 for digital certificates +$0.05 - $0.10 per year per card for maintenance

Source: Atick (2014).

[55] See: http://articles.economictimes.indiatimes.com/2015-03-13/news/60086261_1_aadhaar-project-aadhaar-numbers-uidai-project.

One-off voter registration costs are usually far higher than these estimates. They can range from around $15 per head (Bolivia) to $21-$22 in Afghanistan (Gelb and Clark 2013a) and Kenya. The cost of biometric voter ID technology used in these exercises appears to be around one third of the total (Diofasi and Gelb forthcoming). The high costs can reflect several factors. Highly politicized registration processes often involve hasty or corrupt procurement. The need to purchase enough hardware to register all voters within a short timeframe escalates costs. Kenya's 2013 election required the purchase of 15,000 sophisticated biometric voter kits while Tanzania's 2015 election involves 8,000 kits as well as printers to enable cards to be produced on the spot.[56] In each case, the number of enrollment stations was far more than the number available to the civil registration authorities. Such wasteful exercises do not necessarily ensure trust in the election results (although there are cases when they appear to have made an important contribution) and leave little or nothing behind in terms of stronger permanent registries.

Moving to continuous civil registration as the basis for a national ID register would be highly cost-effective based on the estimates of World Bank/WHO (2014),[57] but it should be noted that these do not include the additional costs of providing and managing robust ID credentials. In many countries it will take time before it is possible to continuously update the range of data needed to implement many programs, such as *de facto* family and household structures in countries where many marriages and divorces are still traditional or religious rather than registered.[58] It may therefore be some time before civil registration processes can supplant survey and engagement--based approaches to updating population, family and household registers[59]. However, modernizing the civil registry as a base for civil identification is clearly the way forward for the future.

Costs versus Savings. Based on the estimates in Table 5, the cost of registration and maintenance for an ID system in a country with 100 million registered inhabitants and with 5 million new enrollments each year could be around $112 million per year. Adding in

[56] Kenya is a particularly egregious case as the pre-existing National ID actually formed the basis for voter registration. For a critical assessment of the procurement process for Kenya's 2013 election see Office of the Auditor General (2014). "Special Audit on Procurement of Electronic voting devices for the 2013 General Election by the Independent Elections and Boundaries Commission". 6 June.

[57] Applying these estimates to Indonesia would yield development and recurrent costs to improve birth and death registration of around $2.08 distributed over a ten-year period (Sumner 2015).

[58] Another option, as in the case of the UID program, would be to limit the role of the identity register to individual authentication with other information collected by programs in line with their requirements.

[59] In Pakistan for example, entries are updated in the course of implementing relief and transfer programs, at the time of ID card renewal and also through periodic surveys to establish entitlement to social programs. The National Social and Economic Registry (NSER) has established a data-sharing protocol to enable social programs to both use information and contribute to it The NSER is managed by BISP, a shared venture that includes NADRA and the Ministry of Finance (BISP 2011).

cards could increase this to $ 134 million.[60] For an average low-income country (income per head $670), this would represent 0.2% of GDP.

To put these costs in perspective, civil service salaries are typically on the order of 6% of GDP (they can be considerably higher, as in Ghana) and general government wages around 9% of GDP (World Bank 2011). To this must be added pensions (the number of civil service pensioners can exceed the number of civil servants as in Kenya) and social transfers -- in South Africa the latter represent some 3.5% of GDP (Bruni forthcoming). Total public cash payments will therefore usually be at least in the range of 10-15% of GDP. An effective system of registration and identification will cover its costs if it succeeds in eliminating leakages or corrupt payments to ghost recipients equal to around 2% of the total value of payments. This is a modest goal relative to the savings seen in the application of strong ID systems to payroll and transfer reform in several countries (Gelb and Clark 2013a). India's PaHAL program (see Section 7) offers an ongoing case for assessment.

6.2 Biometrics and their Limitations

Although biometric technology is moving towards a "commodity industry" it is still in a phase of intense innovation. In addition to fingerprints, face and iris -- the standard and well-tested biometrics commonly used in ID programs – recent years have seen the development of a widening range of physical and behavioral biometrics, including vein patterns, lip movements, DNA, voice, smell, ECG, EEG, gait, dynamic signature and keystroke patterns. Some of these are well established. Vein patterns are used extensively by Japanese banks to authenticate clients at ATMs. Voice is reportedly in use for various purposes in about 140 countries, including to provide "proof of liveness" for companies providing pension and similar payments. Voice may be used overtly, or less transparently as "background" to customers' conversations with an operator to provide backup assurance. It is reported that after about 30 seconds of conversation it is often possible to confirm that the caller on the phone is actually the intended customer with a low margin of error (Warman 2013). Its use in this way is reportedly becoming quite common practice especially as such calls are openly and routinely "recorded to monitor service quality".

Biometric technology has been central to the rollout of ID programs. Considering a sample of 122 established national programs, we found that slightly over half (62) used biometric technology. Since 2008 at least 22 countries have added biometrics, either to existing or to new programs. In addition, at least 16 countries have changed the type or count of biometric identifiers. Typically, they have moved from the incorporation of one or two fingerprints to taking the full set of ten, and/or included other modalities such as iris or digital face-prints to enable de-duplication of identities. Most new programs appear to be incorporating this technology. It is the only known approach to the problem of how to

[60] For comparison, with a registration of 100 million NADRA's revenues and costs in 2013 were around $120 million. Some $17 million in revenue came from international contracts. There will, of course, be additional costs for equipment needed to read cards and authenticate identities but most will not be incurred by the ID system.

ensure "unique" identities within large populations. Its costs have fallen sharply with increased standardization and competition among suppliers (encouraged also by competitive procurement by the Aadhaar program) and continue to do so.

Distressingly little public data is available on the field performance of some of these biometrics and the programs that use them – for example, whether they actually do de-duplicate enrollments as they claim. Vendor claims are sometimes unrealistic and the careful assessments by NIST that provide baseline performance benchmarks are only available for a limited number of technologies and vendor products.[61] In addition, many factors can cause field performance results to differ from those of controlled tests especially if the population has different characteristics, such as a greater proportion of laborers and farmers with worn fingerprints. Biometrics are sensitive to ambient conditions, such as humidity (fingerprints), lighting (face), band-width and connection quality and language (voice). High quality data capture is essential for these technologies to work as expected.

Should Performance Data Be Public? Considering the association of the industry with law enforcement and security, a degree of secrecy over the capabilities of biometrics and the performance of the ID programs that use them is perhaps not unexpected. There may be an element of self-fulfilling prophecy in the mystique of high accuracy: the fewer are the people who try to cheat the system because it is considered infallible, the lower will be the percentage of errors. This "placebo" effect is even occasionally acknowledged, for example when referring to the practice of fingerprinting of infants in Uruguay as a deterrent to child abduction and trafficking.[62]

However, this does raise complications when it comes to dealing with actual errors as the onus falls heavily on those affected to prove a supposedly "infallible" system wrong. All systems need to provide for parallel mechanisms for those unable to provide biometrics of adequate quality. They also need to have strong grievance mechanisms in place, even if (or especially if) they are considered highly accurate. More transparency in this area would be highly desirable, both for the public and also for donors that are asked to support such programs. The use of an open standards-based approach, as exemplified by India's UID program could accelerate the process.

Field Performance on Enrollment. In a series of papers in 2012, the UID program released performance data on the inclusiveness and accuracy of enrolment for a gallery of 84 million people using fused scores from a combination of fingerprint and iris (UIDAI 2012c), and followed this up with large-scale studies of authentication (UIDAI 2012a,b).

[61] NIST assessments have mostly covered fingerprints, iris and face. A major assessment of voice biometrics is soon to start.

[62] This deterrent effect was discussed by Ms. Cristina Tello, Project Coordinator at the Office of Planning and Budget in the Presidency of the Republic of Uruguay, during a seminar at the World Bank on September 17, 2015 and the link to child abduction is also mentioned in a video about Uruguay's civil registry on the Inter-American Development Bank's website (Accessible via: http://www.iadb.org/en/news/webstories/2011-09-19/uruguay-strengthens-civil-registry,9539.html)

These findings are of interest to many countries as providing performance standards, or perhaps lower bounds as technology is continually improving. We can illustrate them by scaling to a more representative-sized population than that of India, with total enrolment of around 30 million (Gelb and Clark 2013b) and summarizing performance in terms of three probabilities: failure to capture biometrics (FTC), False Accept Rate (FAR – also known as the false non-match rate for enrollment) and False Reject Rate (FRR – also known as the false match rate). [63]

- FTC: out of 30 million people around 42,000 people would not be able to provide high-quality images to enroll biometrically, and would need to be enrolled using biographic data.

- FAR: the number of people with dual identities would depend on how many people tried to enroll twice, despite the low probability of success of 3.5 in 100,000. If as many as 1 in 100 attempted duplicate enrolment the number of dual identities would be only about 100.

- FRR: the probability of a false match in a 1:1 comparison would be only 6.7E-12 or about 7 in one trillion. Enrolment would result in only some 3,000 cases of mistaken false rejection (an erroneous indication that the subject had already enrolled) requiring manual follow-up.

These encouraging results on enrollment, which relied on strong quality control at the point of data capture and throughout the program, are supported by less formally released results for Indonesia's program that used the same technology. Including face as a third biometric (not used when the UID tests were performed) would reduce all of these failure probabilities considerably.

UNHCR has begun to roll out a comprehensive program to register refugees, including the use of 10 fingerprints, face and iris. The aim is to be able to provide continuous identity, including in the case of individuals transferring between camps as they frequently do. Hopkins and Hughes (2014) report on the ability to capture fingerprint, iris and face biometrics in a challenging refugee environment in Malawi, including for young children. Total enrollment in these field tests was 16,849 through 16 stations. Regarding ease of use and speed iris was clearly preferred to fingerprints by both operators and participants. Among the latter, 80% considered iris as "easy" relative to only 15% for fingerprints. Thirty five percent of participants rated fingerprints as "difficult" versus none for iris. Face occupied an intermediate position.[64] Failure-to-capture results are reported below.

[63] The parameters can be tuned to enable a tradeoff between the FAR and the FRR (the Detection Error Tradeoff or DET curve). The combined performance is sometimes expressed as the equal error rate or ERR, the point on the DET curve where the probability of the two types of errors are equal.

[64] For a status report on UNHCR's program see Gina Jordan, "United Nations Global Biometrics System Streamlines Relief to Refugees". Re:ID Issue 42, Summer 2015.

Authentication. UID's reports on authentication indicate that this is also possible with high accuracy in field conditions but display a number of less favorable results. Single-finger authentication, for example, yielded a 5% total rejection rate (the sum of FRR + FTC) for an FAR of 0.01%. Iris was far more successful, with dual-capture showing a total rejection rate of only 0.55% for the same FAR.

These results suggest -- in line with some of the reported difficulties in validating voters at the polls using fingerprints -- that simple biometric approaches to rapid and convenient authentication have limitations unless more sophisticated multi-modal technology is used. In a recent audit in Andhra Pradesh of five ration shops[65] with Aadhaar-based point-of-sale identity verification about half of those beneficiaries who did not collect their rations cited non-matching fingerprints as the reason (Scroll, 2015). Once a base identity is securely and uniquely established, it may be convenient to have a wider range of alternative options for routine authentication, such as tokens, PINs, OTPs or a wider choice of biometrics. Even though the cost of hardware is falling this could still raise costs if readers are to be dispersed on a wide scale – the breakthrough will come when reliable fingerprint and iris scanners are incorporated into mobile devices.

Mobile authentication. Mobile or remote authentication remains something of a frontier in general. Passwords and PINS are still dominant, despite widespread concerns that they are vulnerable, especially as actually used by convenience-seeking users. There is therefore a substantial ongoing effort to find effective substitutes, including through biometrics. Convenience applications such as unlocking an iPhone have done a great deal to shift the image of biometrics away from its association with law enforcement and towards a facilitating technology. Fingerprint readers can easily be linked with tablets and smartphones (for example, in Malawi to identify farmers in rural credit programs). However, fingerprint capture on personal mobiles frequently has to contend with dirty environments, scratched screens and other problems that degrade the image. The situation should change as technology improves and iris technology (with liveness detection) is incorporated into mobiles. Several developers are actively engaged with mobile producers; once rolled out, this innovation will sharply reduce the cost of readers.

Alternative biometrics are competing for a share of the growing market for remote digital authentication, including face and voice. Each has the promise of convenience as well as vulnerabilities – the quality of lighting, expression and positioning for face, and language, the quality of transmission and background noise for voice. The combination of such biometrics can be more powerful than either in isolation. One study by Wells Fargo Bank (Ref) reported on the results of testing the fusion of voice and face captured on mobiles. The equal error rate or EER reported for voice alone was 2% and that for face alone was 1%, but for the fused score the reported EER was only 0.2%. Such a level of accuracy, if

[65]Also known as fair price shops, where eligible beneficiaries can purchase grains at subsidized prices

proven more widely, would be adequate for many applications including, for example, to provide proof-of-life for pensions and other social payments. [66] Moreover, the approach requires no special biometric readers or other equipment than the mobile. Since the mobile is also identifiable, this provides two+ factor authentication (something you have and two biometrics).

At the inconvenience and expense of carrying another device, the recently-developed NYMI band offers the prospect of still higher security, authenticating its wearer through monitoring her/his ECG. Combining these systems with a PIN or password would yield full three-factor authentication.

Not all of the existing biometrics or those that come on line in the future are likely to be used in large-scale ID programs in developing countries. However, continued innovation, especially in the area of remote authentication, points to a wide range of future possibilities once the base or primary identity is established by in-person enrollment. The biometrics used most widely in the future might not be those that are most familiar today. Remote authentication is a frontier area for identification in developed and developing countries as e-government and the e-economy expand and mobiles become almost universal.

Vulnerability. Standard error data do not convey the level of resilience of the technology to possible "spoofing" attacks through the creation of artificial fingerprints or irises. This can be done in several ways without the cooperation of the subject, through recent advances in "capture at a distance" technology for face and more recently fingerprints and iris, through the lifting of latent fingerprint images or the re-engineering of a synthetic iris from a stolen iris template. The last process was widely believed to be impossible until Javier Galbally and his colleagues succeeded in re-engineering such an iris using a genetic algorithm in 2012 (Zetter 2012). [67] Unlike the hacking of data stored in a central facility, the spoofing of an individual biometric is a time-consuming process requiring specialized skills so that it is not likely to be undertaken on a mass scale, but vulnerability has led to several developments[68]:

- The incorporation of liveness detection in more sophisticated readers, for example by measuring the dilation of the pupil in response to slight changes in lighting, or by combining fingerprints with infrared finger vein recognition.

[66] In addition to its extensive studies on fingerprints, iris and face, NIST is embarking on a large-scale test of voice biometrics. The results could be of interest for many developing countries because of the potential to verify that recipients of transfer programs are still living. Voice biometric algorithms are sensitive to language however. This could be a useful frontier area for research, possibly coordinated with NIST.

[67] The synthetic iris need not resemble the original one; it simply has to have the ability to generate a close match to the template when processed similarly. The problem may be addressed by revoking the template and re-issuing a different one. If of course the actual iris image is retained in the database and stolen, it becomes impossible to revoke it.

[68] The Biometrics Institute provides guidelines on many issues relating to biometrics including privacy and vulnerability to spoofing. See: http://www.biometricsinstitute.org/.

- Greater interest in "hidden" biometrics such as infrared vein pattern recognition, EEG and ECG that cannot be remotely lifted without the knowledge of the subject and also embody automatic liveness detection.

- The storing of biometric data "on card" and under the control of the user rather than in a central database. This enables the individual to be authenticated against the card but raises the problem that there is then no way to de-duplicate enrollment

- Ongoing efforts to develop "revocable biometrics" where the template can be cancelled and re-issued in the event of compromise and approaches to develop encrypted templates that still permit matching. [69]

Acceptability. Attitudes to the taking of biometric data vary across countries and in some cases within them. While there has not been a comprehensive global survey, the technology itself appears to be widely acceptable although there can still be stigma attached to the technology because of its association with law enforcement. In a relatively few cases opposition reflects longstanding religious and social traditions that can sometimes be accommodated through special administrative arrangements. One example, in Muslim countries, is the deployment of female-staffed enrolment facilities for women. Opposition often relates not to the technology itself but rather to concerns about the (mis)use of the personal data that is collected and the purpose of the identity system supported by biometrics. However, on balance people appear to judge biometric image capture – like other technology-- in a pragmatic way. If it is expected to enhance safety and convenience – for example, to unlock mobile phones -- and improve the delivery of services it is a plus. If not, it becomes seen as an obstacle.

One study related to border management by Accenture (2015) covered 3000 people in several European countries.[70] Overall, 80% were willing to share at least one form of biometric; 82% for British travelers -- this from a country that has strongly opposed proposals to develop any type of national identity system. German respondents were the least supportive, but even so 74% responded positively. Security and convenience were both factors: 73% said that biometric capture of everyone crossing the border would make their country more secure. Favorable responses were higher for those that had used e-Gates than for those that had not; most of the former had found them faster than manual gates. The study also indicated the importance of having an effective mechanism to deal with failures of the technology. Travelers were comfortable with automated e-Gates provided that an attendant would be on hand to respond to any problems.

[69] Unlike PINs, biometrics cannot be matched in encrypted form. Even if templates are encrypted when stored they need to be de-encrypted for matching.

[70] The basis for sample selection is not clear to us so that results are offered only as suggestive.

These considerations have implications for the use of biometrics in developing countries and more broadly for ID systems in general. If they are expected to improve service delivery and to be used for their intended purposes (easier to define for functional IDs than for foundational programs,) they will be accepted, often with hope and even enthusiasm. If not, they will be taken up only with reluctance in the face of official pressure. Their use in programs has to be accompanied by effective grievance processes to resolve failures and errors as well as approaches to deal with those not able to provide biometrics of adequate quality to use the automated systems.

6.3 Beyond the Birth Certificate? Lifetime ID and Young Children.

Birth registration and the issue of certificates – the "breeder document" for identification systems -- have emerged as areas of special vulnerability for ID systems. [71] The neglect of birth and civil registration in many countries is beginning to be addressed by increased focus and finance, collaboration between registrars and health service providers, and new technology. But translating registration into seamless lifetime identification requires further steps.

At the most basic level, the need is simply to increase the coverage and timeliness of birth registration. Coverage is a continuing challenge in many countries (section 3) as is the problem of early registration. By the time a child reaches 5, the age used for the standard indicator of registration coverage, she or he should already have received essential health services such as vaccinations. Some advocate for registration "right from the start" as a human right,[72] while mandating more stringent standards for coverage is seen by others as discouraging countries still low on the standard under-5 indicator. From the perspective of assuring the integrity of identity, the earlier birth registration can be performed the better. Issuing the national identity number at birth can also help to ensure the continuity of identity management over the life cycle. Botswana has done this since 2003, it is also the practice in other countries such as Uruguay.

A second priority is to standardize and secure birth certificates (the "breeder documents" for subsequent identification), improve their security and enable them to be more easily validated against birth registers. Spurred in part by a number of incidents and scandals, many jurisdictions and countries have taken steps in this direction but global progress is still limited. [73]

---

[71] In one assessment, some 10-15% of new French biometric passports were estimated to be held by an unauthorized individual due to forged or substituted supporting documentation (Le Parisien 2011)

[72] See for example: Innocenti Digest, 2002 March 9, "Birth Registration" http://www.childinfo.org/files/birthregistration_Digestenglish.pdf

[73] The problem is not confined to developing countries. In 2010 all birth certificates issued by Puerto Rico were invalidated and reissued with security features in an attempt to curb rampant identify fraud. http://www.documentsecurityalliance.com/news/09-26-2012_1.htm l

The third problem is the continuing technical challenge of authenticating very young individuals against their birth certificates (or national identity credentials if the latter are issued at birth) or against other IDs issued for service-related purposes. Other than identifying children through the IDs of their parents, the only secure possibility is through biometrics.[74] While the normal age for adult registration is usually between 15 and 18 younger children have been successfully enrolled using biometrics. India's UID program takes biometrics from the age of 5, re-registering children at the age of 15. In an initiative to fight child trafficking, Mexico successfully identified some 14 million children from the age of 5 using iris, fingerprints and face.

The frontier problem concerns infants and very young children. DNA is a theoretical possibility. A swab could be taken shortly after birth and markers incorporated into the birth record but the routine use of this option on a wide scale is not practical with current technology. Considering enrollment, the cost has come down but is still around $10 per identity for batch DNA (laboratory time 4-8 weeks) and $100 through rapid DNA (90 minutes). DNA is also not suitable for routine authentications, for example to check whether a child has already been vaccinated, since that too would require costly and time-consuming DNA decoding. In addition, while the few DNA markers used for identification are understood to reveal virtually nothing about the subject's race, health status or other personal characteristics, unlike other types of biometrics like iris or fingerprints DNA can reveal sensitive information on family relationships, for example that paternity differs from that generally assumed.

Iris and fingerprints have been tested on infants and young children, as well as palm and footprints. Jain et al. (2014, 2015) summarize a number of studies. They note that operational efforts to identify children through fingerprints using standard approaches (for example by VaxTrack) have generally reverted to using the fingerprints of the mother because of the difficulty of obtaining high quality prints. The difficulty in registering very young children in a refugee setting is also evident in Hopkins and Hughes (2014). High quality fingerprints (iris) were obtained from only 4% (14%) of children aged 0-3, compared with 87% (98%) of those aged over 4.[75] As in the results reported by UID, iris appears to be a more inclusive technology but neither biometric scores well for young children.

[74] Implanted microchips and digital tattoos are now routinely used to identify pets and are being tested as possible approaches towards electronic human recognition. They might, in principle, work for infants and very young children. However their routine use (if ever) appears to be some time off in the future. See http://abcnews.go.com/Technology/story?id=98077&page=1 and http://www.bbc.com/news/technology-31042477. Another possible technology for the future could be hand bacteria https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7033563&filter%3DAND(p_IS_Number%3A7033542)#article-page-hdr

[75] There was also some slight deterioration in the quality of both fingerprint and iris images for participants over 50.

Jain et al. argue in favor of fingerprints because of the difficulty of securing the cooperation of very young subjects to gaze into a scanner for iris registration. They show that the accuracy of fingerprint recognition for very young children can be improved considerably by technical innovations to scale up prints from their small size and "up-scale" the acquired image to increase the spacing between ridges towards adult dimensions. They also explore the effect of fusing scores from separate fingerprints and enrollment sessions. Using these innovations, they obtain a sizeable improvement in matching accuracy, including in the ability to identify individuals against a large gallery. While these results indicate potential, it is not yet clear that fingerprint based systems or other biometrics have progressed to the point where they can routinely be used under field conditions in 1:N comparisons to identify infants with low error probabilities against large galleries.

However, it may be more feasible to make the less demanding 1-1 comparisons to authenticate children against their own identity and that of their well-identified parents. The UIDAI has recently launched an Android application to register children below the age of 5, taking face and thumbprints and linking them to the Aadhaar number of their parents. The main intent is to strengthen the identity link between parents and children. [76]

Technology is therefore not yet at the point where it can deliver a robust unique identity over the entire lifecycle that can be quickly and easily authenticated at a point of service. However, it is possible to do this from ages that are far younger than those commonly used to enroll individuals into national ID and similar programs (commonly 16-18), and well before the subject becomes legally responsible and has the capacity to commit identity fraud. This means that the integrity of an ID system can be enhanced by earlier biometric enrollment. One approach would be to tie initial enrollment into birth registration, as in Uruguay, and to lock this in through biometric enrollment at around the age of 5 or 6 when the child starts school, with re-registration at around the age of 15.

For infants and younger children the most practical approach is still to ensure that their parents have robust ID and to link their identities to those of their parents. Documentation can be improved to make it more useful, secure and less easy to misplace than a paper certificate. One possibility could be to issue an electronic necklace that includes in its chip the name and particulars of the child as well as a copy of its medical record. These can reportedly be produced for as little as $1 (Akpan, 2014).

[76] See: http://www.dnaindia.com/india/report-aadhaar-authority-develops-android-app-for-easier-registration-of-infants-2126997

7. Functional applications of biometrics

Biometric technology has been introduced in a wide range of disciplines and country settings to strengthen identification, improve service delivery, and increase efficiency. Gelb and Clark (2013a) identified 160 cases of biometric identification of which 115 were considered to be 'functional' – linked to a specific developmental purposes, such as health, financial services or elections. The ID programs can be part of nationwide systems or be 'custom' initiatives that serve the particular applications. Many of the latter have been implemented by NGOs and the private sector as well as state or subnational governments. In these programs biometrics has two different uses: to ensure a clean, de-duplicated register of participants/beneficiaries and to authenticate them at the point of service, but not all applications use them in both these ways. We highlight functional applications in three areas: finance, transfers (including with links to financial inclusion) and health.

7.1. Finance

Biometric identification can facilitate financial inclusion in three ways. It can support the implementation of KYC regulations and reduce the risk of fraud through real-time authentication of users. A robust ID system can also strengthen credit monitoring to help customers build credit histories and access loans.

Reconciling KYC and financial inclusion.[77] Tightened KYC requirements over the last 15 years create a tension with financial inclusion because of the high cost of identifying small clients. This has been recognized, as shown by the consensus that KYC rules those set up within the framework established by the Financial Action Task Force (FATF) should follow a risk-based approach that applies the principle of proportionality: *"to strike the right balance, existing regulations should be carefully analyzed to establish whether their demands on service-providers are proportionate to the risk"*.

In response, many countries, including, for example, South Africa, Peru and India, have graduated their KYC requirements with less extensive documentation required for restricted accounts with maximum limits on balances and transactions. Kenya, similarly, applies a graduated approach to e-money provided through M-Pesa and M-Shwari accounts. The wide availability of a robust ID credential – national IDs in three of the countries and the Aadhaar in India, provides a key element of inclusion by reducing the cost to the banks of the minimal level of KYC required to satisfy regulations. In addition,

[77] This section draws on the Report of the Task Force on Financial Inclusion (Claessens and Rojas-Suarez), 2016 forthcoming.

the ability to uniquely identify account holders makes it possible to detect "smurfing"[78] and enforce limits on international remittances effected through account-account transfers via the growing FINTECH industry. This increases transparency relative to more traditional approaches through money transfer operators.

Authentication for transactions. Fingerprint authentication for banking transactions, including by biometric-enabled ATMs, has been used in a diverse set of countries, such as Bolivia (PRODEM), Mexico (Azteca), Opportunity Bank International (various locations), and Nepal (Siddharta and Everest banks) (Gelb and Clark 2013a). It can serve both as a tool for inclusion among customers without official documentation and for fraud prevention in countries with where financial crimes are prevalent. Biometrics may not be the sole method of authentication but can provide additional security in settings where keeping PINs secret may be difficult for socio-cultural reasons.

Opportunity International was among the first financial institutions to roll out biometrics-supported banking for low-income customers across developing countries. It operates in 28 countries and serves over 3.5 million clients (Opportunity International 2014). In Malawi, where Opportunity International Bank has signed up over 350,000 depositors, fingerprint-based customer registration and verification has been the norm since 2003. New clients are fingerprinted and issued a smartcard including biometric identifiers. Each new registered customer is also checked against the existing database to ensure uniqueness. Clients are authenticated against the fingerprint scan stored on their bankcards at a teller's station or ATM, ensuring that only the account owner can access the funds. Even depositors without formal identification can thus be securely identified for each transaction. Anecdotal evidence shows that women, who were previously unable to stop male relatives from accessing their savings, have gained full control over their funds (Campbell 2010). Not surprisingly, the proportion of female clients is far higher than for the financial system as a whole.

Another early adopter of biometrics in banking, Mexico's Banco Azteca has been using fingerprints to register and authenticate clients since 2001. It registered over 8 million customers biometrically in the first five years and was processing over 200,000 fingerprint matches per day as early as 2006. The bank asserts that the use of biometrics has allowed it provide access to financial services to poor clients without reliable official identification. Brazil's Bradesco bank uses ATM equipped with hand-vein readers to authenticate customers; similarly, China's Bank of Lanzhou uses finger veins for verification (Schmidt 2013; and Dymi 2014). Chinese researches have recently unveiled the first facial

[78] When a person carries out several cash transactions by breaking them into smaller amounts in order to avoid the mandatory threshold reporting and/or customer identification requirements (FATF, 2010)

recognition-based ATM, which is envisioned to match facial data to pictures stored in the central ID database (Middlehurst 2015). More recently, growing interest in remote mobile authentication is prompting increased interest in biometrics, such as combining voice and face either alone or to reinforce other forms of identification (see section 6).

Banks in countries with less-than-adequate ID systems may be forced to take the identification of customers into their own hands. Increasing concerns about financial fraud led the Nigerian financial sector to launch its own biometric identification program, the bank verification number (BVN), in February 2014. The BVN is shared across all Nigerian banks and is required to perform all bank transactions. Enrollment requires some official state-issued ID credential - a passport, driver's license, voter card or national ID card - as well as the capture of the applicant's ten fingerprints and a photo (Central Bank of Nigeria 2014). Registrants are then issued with a unique ID number that must be linked to all their bank accounts, a BVN card with a chip containing the holder's biometric information, and a PIN for additional security. The project is aimed at reducing fraud in the banking sector through unauthorized access as well as ensuring that information on blacklisted customers can be shared across the Nigerian banking system. As of August 2015, about 18 million of 28 million Nigerian bank customers have registered with the BVN project[79] (Planet Biometrics 2015). Similar programs have been initiated by consortia of banks in some Latin American countries, to enable them to verify the identity of clients via checking their biometric records against a shared database. Information sharing about clients is limited to the minimum, but fraudulent identities and those on a blacklist are flagged. While such programs may be necessary to protect the integrity of the banking system, the additional cost is likely to serve as a deterrent to enrolling small clients and expanding access to finance.

Strengthening credit monitoring. The lack of reliable unique identifiers represents a challenge to creating credit records and enabling customers to build up credit histories. Fingerprint registration has been shown to positively affect borrower behavior in low-income communities, reducing credit risk and costs for lending institutions. In a randomized evaluation implemented in rural Malawi, a group of micro-credit applicants were fingerprinted at the time of borrowing and received some basic instruction about how fingerprints can be used for identification purposes (Gine et al. 2012). Fingerprinted applicants were also told that their biometric information would be used by credit providers in the future to check their credit history. The evaluation found higher repayment rates among high-risk applicants and more prudent borrowing when loans were associated with biometric data capture. Improved loan repayments were associated

[79] The BVN expires after 10 years, at which point customers will need to re-enroll, although the number remains the same for life.

with a $1.94 net benefit for the lender per fingerprinted individual and a total benefit-cost ratio of 2.27 (J-PAL 2011).

Kenya has been a pioneer among developing countries in integrating information on the holders of financial accounts. All bank accounts are linked to the ID number of their holder, which has the role of the unique identifier across the system. Financial institutions are required to query the government's database to verify the validity of the ID. Banks are mandated to share data on non-performing loans and more recently also on positive credit history, setting the stage for a credit information system (CIS Kenya 2015). Microfinance and mobile money institutions are similarly mandated to share data on credit experience. Non-bank credit providers, such as utilities, can also join the system on the basis of reciprocity, receiving information and reporting on payment records of customers. The system has been associated with a substantial decline in the share of non-performing loans as well as a decline in the proportion of loans secured by collateral (Kwambai and Wandera 2013). The cost savings for financial institutions due to less risky lending should allow credit services to be extended to a wider clientele. Strong customer identification, including the ability to connect all accounts owned by a single individual, is also critical for effective KYC enforcement and to ensure that Kenyan institutions are able to maintain and build correspondent relations with institutions abroad.

7.2 Transfers

Mobile ATMs equipped with fingerprint readers were used to deliver social grants in rural Kwa-Zulu-Natal as early as the mid-1990s. Since then, biometrics-based transfers have been used in many intervention ranging from disaster and humanitarian relief to longer-term poverty alleviation grants and the reform of price-based subsidies: Gelb and Decker 2011 summarize 19 cases and estimate that even modest reductions in leakages and losses would be sufficient to cover reasonable costs of an enhanced ID system. Biometrics have usually been used both to curb multiple enrolments and to help authenticate recipients at points-of-service.

Humanitarian crises and emergency relief. Biometric tools have been used to register refugees since 2003 and UNHCR has made the collection of biometric data a regular and routine feature in its registration process since 2010 (UNHCR, 2013).[80] Fingerprint or iris records are incorporated into UNHCR's "proGres" refugee registration database to identify and track refugees in countries like Burundi, Ethiopia, Kenya, Malaysia, Tanzania and Thailand. Registration provides refugees with an official recognition of their status and can

[80] Refugee identification poses some particular sensitivities and risks, including for family members of identified refugees still in their home country. See Privacy International 2011: "Why We Work With Refugee Privacy" July 8.

help prevent their arbitrary detention or forced repatriation; it can also facilitate refugees' freedom of movement by providing them with a recognized and transportable official identification, including in the event that they transit between camps. Biometric registration and verification at the point-of-service in refugee camps can help prevent fraud by ensuring that each refugee is only registered once and receives the allocated aid or cash grants only once. In 2013, the World Food Program linked the distribution of food rations in the Dadaab and Kakuma refugee camps in Kenya to UNHCR's fingerprint records, which resulted in monthly savings of $1.5 million through better targeting of beneficiaries[81] (WFP, 2013). These savings alone were estimated to cover the cost of registration -- at $4.7 million – over a few months. There is ample scope for increasing the use of technology in humanitarian aid. Currently transfers and vouchers make up only 6% of humanitarian aid, even though studies show that switching from in-kind assistance to these direct mechanisms would enable 18% more people to be assisted for the same budget (ODI, 2015). Direct transfers are also often beneficiaries' preferred option for receiving assistance (IRC, 2014).

Pakistan relied on its national biometric database to identify and authenticate citizens eligible for its national emergency cash transfer programs after devastating floods in 2010 destroyed the livelihoods of millions (Gelb and Decker, 2011). The government used the NADRA database to identify citizens eligible for assistance based on their registered address. The identities of targeted heads-of-household were then confirmed by comparing their fingerprints to those in the 96 million-strong database. This proved particularly useful since many living in the flood affected areas had lost all other forms of identification. Over 1 million households were issued a Visa supported Watan debit card, which could be used at numerous points-of-service and ATMs across the country (Visa, 2010, Pasricha, 2011). Beneficiaries received payments quickly and with little diversion. While there were many disputed decisions that required a lengthy grievance redress process, the problems reflected beneficiary selection rather than identification.

Advanced technology can be successfully used even in difficult conditions provided that it is adapted to the available infrastructure. In the Democratic Republic of Congo, iris recognition was used to facilitate the country's DDR (disarmament, demobilization, and reintegration) strategy (Gelb and Decker, 2011). Individuals were enrolled in a cash transfer program to help them adjust to civilian life; following iris scans, 110,000 ex-combatants received an ID card and a PIN number which they could use to collect 13 monthly cash payments from over 8,000 airtime sales agents. In some sparse rural areas

[81] The workings of the biometrics-based food ration system in refugee camps are well illustrated in this video ('UNHCR Kenya Biometric Food Distribution System') by Doug Greene: https://www.youtube.com/watch?v=CunpKKqCvWg

where distribution through airtime vendors proved difficult, mobile teams delivered cash using only iris scans for identification.

Social grants. Biometrics are used in many programs including in Pakistan (Malik 2014) and South Africa. Provincial governments in South Africa have used fingerprint-based biometric ATMs and smartcards since the mid-1990s to deliver pensions and social grants, including in locations with limited connectivity. Scans of each 10 fingers were recorded on a smartcard which also holds that individual's grant information, including payment schedule, amount, and date of last payment received (Gelb and Decker, 2011). The system of social grants now accounts for 3.5% of GDP and serves around a third of the population. Biometric re-registration of over 20 million social grant recipients was completed in 2013 by the South African Social Security Agency (SASSA) in an effort to streamline the recently centralized system. . Even though the system had been able to draw on an extensive identity infrastructure initiated during the apartheid period re-registration enabled SASSA to remove 650,000 social grants going to non-eligible individuals which resulted in savings of over $65 million annually (Ensor, 2014). The new system also ensures that payments cease once a beneficiary has died without having to rely on death registration records: all grant recipients must present a 'proof of life' once a month by scanning their fingerprints or through voice recognition.[82]

Kenya's recently launched National Social Protection Safety Net Policy (NSSP), consisting of five different social assistance programs - seeks to provide social grants to 500,000 recipients. All beneficiary households need a valid national ID card to enroll in the program and the card can be authenticated against records in Kenya's Integrated Population Registration System. As in South Africa and increasingly in other programs (notably in India), payments are delivered through bank or mobile accounts, creating an additional stimulus to financial inclusion while minimizing the cost of creating program-specific delivery mechanisms. The national ID card and number provide the ability to de-duplicate the registry and thus limit fraudulent claims but liveness detection, as in South Africa, remains a problem. Three programs use biometric smartcards for two-factor authentication to ensure the 'liveness' of recipients, but custom technology is implemented by each bank responsible for distributing funds. The systems are not inter-operable so that the programs are locked in. Separate, incompatible systems are costly -- a change in the financial intermediary would necessitate a new and expensive re-enrolment.

[82] The estimated completeness of adult death registration has increased from 89% to 94% over the period 1996-2001. While high, this still leaves the possibility of a large number of cumulative unrecorded deaths, especially among the poorer parts of the population. Statistics South Africa: Statistical Release P0309.3 2011. http://beta2.statssa.gov.za/publications/P03093/P030932011.pdf

Subsidy reform. Price subsidies are massive – the July 2015 IMF Survey estimates that the revenue gain from eliminating energy subsidies alone would be US$2.9 trillion (3.6 percent of global GDP) in 2015.[83] Price subsidies cannot be reformed without adverse impacts on the poor (and on consumers more generally) without some compensatory mechanisms. While compensation could partly be through reducing tax rates in other areas, this is regressive to the extent that very poor consumers may not be subject to direct taxation or consume much that is subject to indirect taxes. The alternative -- shifting to direct transfers -- is not possible without clear identification of the recipients.

India's PaHAL program to eliminate LPG price subsidies to consumers offers an example. LPG cylinders were previously sold at subsidized prices to households, but at market prices to businesses, resulting in a flourishing black market and many fraudulent accounts. The reform shifts the subsidy to direct payments into purchasers' bank accounts. Evidence on the program is still being collected so that financial results will continue to be revised, but based on initial estimates, it would save the Indian government between $1 billion and $2 billion a year (depending on world energy prices), which represents savings of up to 25% based on the costs in previous years (Gelb and Diofasi, 2015). As mentioned above, the status of Aadhaar as a universal, legal requirement for the receipt of transfers is still in limbo after the Indian Supreme Court's ruling against its mandatory use (Anand, 2015). Nevertheless the Aadhaar number is now being introduced as a key identifier in about 60 government programs to provide accurate identification and recording of beneficiaries and curb leakages.[84]

7.3. Health

Biometric ID can support health programs in at least three ways. It can help manage enrolment in large-scale health systems, including health insurance schemes where it is important to accurately identify beneficiaries. It opens up new possibilities for tracking treatment for individuals in health settings where timely dosage is of great importance, such as for TB or HIV patients or the efficient administration of vaccines. It can also be used to ensure timely and diversion-free salary payments to employees in both established health systems and emergency settings, and – with some complications --to monitor the attendance of health care workers.

Healthcare for targeted populations. India's health insurance scheme for the poor, the Rashtriya Swasthya Bima Yojna (RSBY), is an illustrative example of a large-scale health

[83] http://www.imf.org/external/pubs/ft/survey/so/2015/NEW070215A.htm

[84] A recent ruling by the Supreme Court does appear to allow the use of the Aadhaar for particular programs, including the LPG programs, but limits its use for other purposes and still does not appear to endorse the compulsory use of the identifier.

program that has used biometrics to minimize administrative burdens while also maximizing inclusion (Palacios et al 2011). It covers costs of specified procedures for those living below the poverty line – about 47 rupees (about 70 US cents) a day. RSBY covers 36 million families (100 million people) and has subsidized 9.8 million hospital visits to date (RSBY, 2015). Private and public insurance companies compete to service each district. The winner registers eligible families, takes their fingerprints and provides biometric insurance smartcards for a nominal fee (30 rupees) (Gelb 2011). If a beneficiary is hospitalized, the hospital verifies coverage using fingerprints and the smartcard and then submits claims to the insurance company. No cash changes hand and there are no lengthy claims forms to fill in.

Tracking patients and treatment. NGOs are pioneering the use of biometrics in tracking patients for treatments and preventative measures where accurate identification of patients over repeat encounters is crucial for success. Vaxtrac, an NGO dedicated to providing technology-based support to vaccination programs in developing countries has been using fingerprint scanners to register and track the vaccination record of infants in Nepal and Benin. Left and right thumb prints of both the mother and the child are captured and used to verify the vaccinations received during later visits. Given the low success rate in matching children's fingerprints, health workers rely primarily on the mother's biometric data (Jain et al 2015). Preliminary data indicates that biometric tracking has increased the number of children returning for further vaccinations and that parents perceive the programs positively (Reuters 2014).

Tuberculosis (TB) patients of Operation ASHA – an NGO focusing on providing TB treatment to the poor - receive their medication via a biometrics-based treatment administration system, aimed to improve adherence and prevent the spread of multi-drug resistant TB – an equally contagious, but more difficult to treat strain of TB that often develops in patients who skip or miss medication. Patients are registered via their fingerprints as they take their first dose of medication. For each subsequent dose, both the counsellor (the ASHA employee) and the patient are required to give their fingerprint. If the medication has not been dispensed on time, the eCompliance system associated with the biometric terminals issues a warning to the patient, the counsellor, and the medical supervisor (Operation Asha 2015). An interview-based evaluation of the program's implementation in 25 treatment centers across New Delhi and Jaipur reported that biometric monitoring made patients more likely to visit the health centers and take their medication on time and improved patient-health worker relations compared to traditional Directly Observed Therapy, Short Course (DOTS) programs (Bhatnagar et al 2012).

Fingerprint-based tracking of antiretroviral (ARV) drug treatment for HIV patients was piloted in South Africa under the USAID-supported DELIVER project (DELIVER 2007). Both

patients and health care providers were issued with smartcards that were inserted into a smartcard-reader simultaneously during health visits. The patient's identity was than verified via a fingerprint scan that matched them to the information contained on the smartcard. The patient's card also held data on diagnostics, laboratory results, and prescription information, while the provider's card stored details of the patient encounter temporarily and was uploaded to the health care provider's central database at the end of the day. While the system worked, the high cost of the annual per site licensing fee ($1450) for the proprietary software associated with the smartcard technology made the scale-up of the pilot program prohibitively expensive. Biometric registration of 1100 HIV patients was also implemented in 2004 in Malawi's Mzuzu Central Hospital, with support from Taiwanese donors. The digitalized data management process was associated with significant time savings per patient, cutting staff numbers and thus costs (Yu et al. 2005). While these early projects to track ARV patients are promising, we found very little information about current applications or evidence of scale-up.

Incentivizing and monitoring health workers. A third health-related application of biometric ID is to improve the performance of health workers. This has potential to contribute towards better health outcomes, but much depends on the willingness and ability of the implementing agency to provide positive incentives as well as to enforce sanctions. The latter alone can be problematic – the use of fingerprint readers to monitor attendance and combat absenteeism has seen some mixed results. [85]

Dhaliwal and Hanna (2014) show that recording staff attendance via fingerprint readers helped reduce absenteeism among some health workers, but not among doctors in primary health centers (PHCs) in Karnataka state in India. Each participating PHC received a reader and a multi-purpose mobile phone to upload fingerprint data to the state health headquarters, so that supervisors could then monitor attendance in near real time. Staff had to scan their thumbs on arrival and departure; attendance data was uploaded to the central database at the end of the day. While the monitoring system increased the attendance of nurses, lab technicians, and pharmacists by 18 percent, it had no effect on doctors relative to medical staff in PHCs without the intervention. Machine "malfunction" rates were high, with the monitoring system being non-operational in one-third of the cases. There was little evidence that supervisors used the data to monitor and reprimand absent employees, highlighting the limitations of technology where the will to enforce rules within an organization is limited. A similar experiment using non-biometric time/date

[85] Unlike payroll de-duplication, which is clearly directed against fraud, measures to monitor attendance can be interpreted as indicating a lack of trust between management and workers, with consequences for labor relations. Gelb and Clark (2013a) note the example of West Bengal where the introduction of biometric monitoring of health personnel was first used with the highest-grade employees—administrative heads and medical officers—before being extended to lower grade positions.

stamping machines to monitor the attendance of assistant nurse midwives at rural health centers initially reduced absenteeism, but due to a non-enforcement of penalties by the local health administration, absences were back to their original level 16 months after the first implementation of the program (Banerjee et al 2008).

In emergency settings, such as the recent Ebola outbreak in West Africa, keeping track of the number of health workers and ensuring timely payments to the existing and newly recruited workforce poses a great challenge. A UNDP-supported biometric payroll system was introduced for Ebola response workers (ERWs) in Sierra Leone in early 2015, which registered all 30,000 ERWs employed by over 10 different NGOs and government entities (UNDP 2015a). The registration underpinned the roll-out of mobile pay for workers, ensuring that all got paid in a secure and convenient manner, including a 'hazard pay' bonus for those at greatest risk of contracting the disease. These added incentives, coupled with an effective payment system, helped avert strikes and kept workers motivated among very difficult conditions. The new system also helped remove 3,500 duplicate records and identified several ERWs who received payment for the same work by two different entities (UNDP, 2015b).

Similar attendance monitoring and payroll systems are being implemented in developing countries across public service providers and government department outside of the health sector. The World Bank recently supported the roll-out of a biometrics-based payroll for civil servants in Somalia (World Bank, 2014). India introduced a biometric attendance system for bureaucrats in 2014, where the presence of over 160,000 public servants can be tracked online by any interested party in real-time[86] (Raj 2014).

These functional cases suggest the great potential for the use of robust ID systems to improve inclusion and the implementation of a range of programs. They also show the externalities associated with wider programs that avoid the cost of small, fragmented initiatives, even if these programs (as in South Africa's SASSA registration) are not foundational national IDs. They also show the importance of unique ID and of recognizing the ID needs of particular programs, for example proof of liveness for social transfers when developing a strategic approach to identification.

8. Risks of ID Programs and Unintended Consequences

Like other technology-related areas, more advanced ID programs raise areas of concern and involve specific risks. These can be classified into three groups: facilitating the exclusion of vulnerable populations and discrimination, eroding privacy, including through

[86] See: http://attendance.gov.in/ for real-time information.

the misuse of personal data and enhancing surveillance; and failure to deploy new systems in a cost-effective way. These risks are genuine but at the same time they need to be weighed against the potential benefits of such programs and a realistic counterfactual that takes into account the political conditions and institutional capacity of the country.

8.1 Exclusion and Discrimination

The Poverty Barrier. Requirements for ID that is costly or difficult to obtain constitute an additional obstacle to poor and disadvantaged populations. In additional to monetary cost, barriers can include low birth registration coverage, the distance to registration centers and the time required to get there. Some countries have empowered a large number of enrollment agents (about 50,000 for UID) or emphasize mobile units (Pakistan, Peru, Malaysia). The need for prior documentation and a complex process can also constitute impediments to registration. In some countries NGOs have played a facilitating role, intermediating between people and registration authorities and helping them to gather evidence, prepare forms and respond to questions. As an outstanding example, the Female-headed Household Empowerment Program PEKKA[87] has played a key role in supporting civil registration in Indonesia, including by helping to convene "one-stop-shop" rural registration fairs (World Bank 2012; Gelb, 2015, Sumner 2015). Subject to controls against multiple registrations, donors can encourage outreach by funding each additional registration on a pay-for-performance basis. [88]

Programs also need to allow for people who cannot register or authenticate themselves in the normal way, for example by providing biometrics of adequate quality or recalling PINs and other identifiers. Even though the percentage of FTC can be reduced through the use of multi-modal biometrics there will still be a considerable number of such cases. Setting up an appropriate grievance mechanism to address such cases is a crucial element of any program.

The Gender Barrier. Women in many countries face considerable barriers to obtaining official identification, often compounded by poverty barriers (as noted above). Both discriminatory laws and informal local traditions contribute to the exclusion of women from ID programs and from the rights and services conferred by them. While there is little reliable data on women's enrolment rates in national or functional ID programs, a review of legal and administrative requirements and recent survey data can shed some light of the patterns of exclusion along gender lines.

In Nepal, women's access to identification is hindered by both the country's citizenship laws, which limit women's ability to pass on their citizenship to their children and spouse, and customs and administrative regulations that require the presence of male relatives for

[87] Perempuan Kepala Keluarga

[88] For example, support to civil registration in the Dominican Republic included both funding to upgrade the system and $5 per additional registration. Such an incentive scheme requires of course effective measures to prevent multiple registrations.

obtaining official identification. A recent survey of 20,000 Nepalese residents found that only 74 percent of eligible women – compared to 87 percent of eligible men – held citizenship certificates, the country's primary identity document (FWLD 2014). Without a citizenship certificate, women cannot access banking, employment, register land or home ownership, and a range of other public services. The presence or the identification documents of a male relative is required for ID registration in several other countries, including Afghanistan, Iraq, and a number of Middle Eastern states.

Even where women's differential access to ID is not formally regulated, social norms can provide a powerful disincentive for registration, sometimes across generations. Unmarried mothers and their children often face stigmatization when birth certificates are issued without the father's name and thus may opt to not register their children at all (Sumner, 2015). Spouses and other family members may also discourage women from obtaining an official ID for fear that greater access to services and greater financial independence may increase the decision-making power of the female household member or even that it will promote the dissolution of the marriage.

The Nationality Barrier. Programs that define eligibility in terms of citizenship (and also require pre-existing official documentation such as a birth certificate) can also exclude poor and vulnerable people. The case of the Dominican Republic illustrates how tightening criteria for citizenship and documentation requirements – for parents, grandparents, and even earlier generations - can increase the risk of statelessness. A retrospective reinterpretation of "temporary status" in 2004 denied birthright citizenship to children of 'non-residents' who now included persons of Haitian descent who were born in the Dominican Republic or had lived in the country for decades. As a result, many lifelong residents of Haitian descent were refused national identity documents (*cedulas*) if they were not able to provide documentary evidence of legal Dominican residence going back multiple generations. Those without cedulas are routinely denied access to education, political participation, and the justice system, while also being unable to register the birth of their own children (Open Society Institute 2010). A Dominican Constitutional Court ruling from 2013 further entrenched the exclusion of residents of Haitian descent, ordering a review - effectively a repeal - of Dominican citizenship status going back to 1929, which put an estimated 200,000 Dominicans of Haitian descent at risk of statelessness (Blake 2014). While there appears to have been some backtracking on threats of widespread deportations, the situation of many residents is still uncertain.

The uncertainty surrounding citizenship rights in the Dominican Republic is neither unique nor quantitatively the largest. Only about 30 countries, mainly in the Americas, grant citizenship on the basis of *jus soli,* birth on national territory. Nationality laws often have provisions that leave the question of citizenship open for interpretation by local officials; the ID authority thus becomes the de facto court for adjudicating claims to citizenship. Legislation may directly discriminate against certain vulnerable groups, such as ethnic or

religious minorities or women. For instance, twenty-seven countries grant no or only limited rights to women to pass citizenship to their children or spouses (UNHCR 2014).

Increased statelessness therefore looms as a risk from the increasing formalization of identity. The UNHCR's official statistics list 3.5 million stateless persons worldwide, but they estimate the total to be about 10 million due to missing data in many areas. Formally stateless people may not be undocumented, since statelessness is a recognized status, but they are heavily constrained. Many with indeterminate status are unable to obtain any official documentation and are denied access to legal and social protection and to basic public services, such as education and healthcare. In Myanmar, where over 800,000 of the world's stateless population resides, citizenship is divided into three categories, with acceptance to each category relying on a different set of criteria and each category of citizen assigned different rights. Only those with 'full' citizenship can stand for elections or establish political parties. Members of the two other categories - 'associate' citizens and 'naturalized' citizens - are also barred from fourteen liberal professions, including medicine, law, and engineering (UNHCR 2015). Members of the Rohingya minority group in the northern state of Rakhine have for decades been denied any form of citizenship. Some have been issued temporary identification documents – 'white cards' and, more recently, 'green cards' – but these provide no right to state protection or access to public services and further entrench differences between their status and that of recognized citizens (Aung and Mar 2015).

There are two key legal instruments that states can ratify to protect stateless people in their own countries: the 1954 Convention relating to the Status of Stateless Persons and the 1961 Convention on the Reduction of Statelessness. The 1954 convention sets out minimum standards of treatment for the stateless; the 1961 Convention focuses on the prevention of statelessness at birth. Signatories are committed to granting citizenship to those born on national territory is they otherwise would be stateless. Relatively few countries are parties to these conventions: 80 to the 1954 Convention and 55 to the 1961 Convention.

Africa has over 720,000 are formally stateless persons but this is regarded by experts as a dramatic underestimate of the number of people with unclear national status. Nationality laws are exclusionary -- over 20 countries have no provisions regarding a child's right to nationality or a path to citizenship for those with foreign-born parents (Manby 2010). Only a handful of African countries automatically confer citizenship from birth to those born on their territory. Several countries still grant greater rights to men than women to pass citizenship to their children or spouses. Citizenship by naturalization is often almost impossible to obtain in practice and many countries allow naturalized citizenship to be withdrawn on arbitrary grounds. Half of Africa's states even allow revocation of a person's

birth nationality. [89] Recognizing the increasing risk of marginalization, the African Union has called for a Convention on African Nationality in its report "The Right to a Nationality in Africa" (ACHPR 2014). This is an urgent problem that, if left unattended, could complicate the process of formalizing identity and nationality in Africa.

Mitigating the Risks. Minimizing exclusion requires attention to the implementation of programs, including building in incentives for registration, and ensuring that the legal basis is as inclusive as possible. In the short term the only way to approach this in countries with large numbers of people in potentially uncertain legal status is to adopt an "ID-first" strategy, de-linking registration and identification from questions of legal status so that they can at least have access to the programs and services enabled by that identity. This will not be sufficient, however, to ensure that they can fully participate in society and economic activity. The global thrust towards more inclusive registration and stronger identification needs to be complemented by a global push to reform nationality policies.

8.2 Personal Data Privacy

Digital ID systems are only a part of the far wider ICT revolution that has so greatly expanded the volume of all types of personal data. Technology can be seen as an intrinsic risk to privacy or as privacy enhancing depending on the protections built into systems and what is understood by privacy.[90] Gaining access to a service or program by submitting a fingerprint or iris scan may be seen as less intrusive than responding to a long list of questions to confirm identity. One motivation for the use of biometric smartcards to support internally displaced populations in Pakistan was to avoid their humiliation from having to stand in lines for support (Malik 2014). Electronic payment of benefits determined on the basis of a proxy-means-assessment may be less intrusive than community-based support programs that rely on scrutiny by neighborhood committees. Segmenting personal information to respond only to the relevant questions can further help to protect privacy. For example, permission to drink alcohol in the US only requires information on age not name, address or other personal details. To the extent that technology can constrain the range of information to that needed by any service provider it can enhance privacy.

Taking into account the wide range of issues related to ICT, such as whether to permit official access to cellphone records or digital communications to be encrypted, or to grant individuals "the right to be forgotten", national ID-related policy is certainly not the only critical area of concern from the privacy perspective. With their more comprehensive privacy legislation it could be argued that citizens of the EU enjoy greater rights to personal data privacy than those of the US despite the fact that, unlike most EU countries, the latter

[89] Some countries base nationality directly on racial criteria. Citizenship is not possible in Liberia unless the person is of African ancestry.

[90] In the present context "data privacy" is best understood as referring to the right of an individual to have access to and control over the use of her/his personal data. This is different from "anonymity" or the right not to be included in the system at all.

does not have a National ID program. However, in addition to the particular concerns raised by remote face recognition, integrated ID systems do potentially facilitate access to personal information and make it easier to link individual records and transactions across disparate data registers through the use of a common identifier.

Data Privacy Laws: Are They Sufficient? As the number and coverage of identity systems expands, data privacy and data protection measures are also increasing in importance. Greenleaf (2013) cataloged 99 states and territories as having a framework for data privacy legislation in 2011 that conformed to the widely accepted OECD Fair Information Principles for the protection of personal data.[91] This is an evolving picture as more countries are adopting data privacy laws. According to Greenleaf, between 2 and 3 countries have been passing such laws every year since the 1940s, with 5 new laws per year in the 2010s alone. Table 6 shows the percentages of countries with data privacy laws in place in 2011 by income group. As expected, this increases sharply with income level, from 12% of the low-income group to 76% of the high-income group.

Table 6
Data Privacy Laws and Rule of Law by (World Bank) Income Group
(Number of countries and percentage of group)

	LIC	LMIC	UMIC	HIC	TOTAL
Countries with Data Privacy Law	4	15	22	44	85
Percentage of Group	*12%*	*32%*	*41%*	*76%*	
Countries with Data Privacy Law + Rule of Law above mean	0	3	9	42	54
Percentage of Group	*0%*	*6%*	*17%*	*72%*	

A data privacy law might not, however, offer much comfort in a country where the rule of law is generally weak or where there is little political will or technical capacity to implement a data privacy law. Angola and the Kyrgyz Republic, for example, are classed as having data privacy laws but their rule of law indicators are among the lowest in the world. Table 6 also shows the distribution of countries that both have data privacy laws and a rule of law indicator above the global mean. Far fewer lower-income countries pass the threshold under this composite criterion—in 2011 none had both a data privacy law and a rule of law indicator above the global average. It is in this group of countries where the coverage of formal ID systems is expanding most rapidly. The problem of ensuring the privacy of personal data is deeper than simply whether a data privacy law is on the books.

[91] Greenleaf notes a number of differences between the countries, for example whether the data privacy laws apply to the public sector, the private sector or both. Inclusion requires that the country has some identifiable data controller and mechanisms of enforcement, such in addition to the legal framework. For a review of the OECD Principles as applied to identification see Gellman (2013).

In addition, the cross-country distribution of data privacy laws in 2011 is strongly associated with Freedom House measures of the level of political rights and civil liberties: and this association is still significant after controlling for the income group of the country (Table 7). This suggests an uphill implementation struggle as efforts are made to extend the coverage of data privacy laws to a wider range of lower-income countries, many with less democratic governance.

Table 7
Democratic Governance and Data Privacy Laws, 2011
Summary of Probit Regression

	Dependent Variable: Data Privacy Law in 2011	
RHS Variables		
Freedom Score	-0.229***	
HI Dummy	1.395***	
UMI Dummy	0.638	
LMI Dummy	0.532	
Constant	-0.150	
Observations	193	
* p<0.05	** p<0.01	*** p<0.001"

Source: Greenleaf 2013, Freedom House, World Bank.
Notes: Freedom is the average of Political Rights and Civil Liberties score. Income categories follow the World Bank classification. The omitted category is Low Income.

A particular concern in low income countries is the difficulty of operationalizing the principle of "informed consent", especially when access to benefits and transfer programs provides an urgent motivation to enroll in systems that may subsequently be used to cross-reference their use of other programs – something not necessarily made clear at the time of enrollment – or for very different purposes. As noted above, this is flagged by privacy advocates who argue that development aid initiatives are facilitating surveillance in developing countries. A similar argument is made regarding humanitarian aid and the registration of refugees. While registration can support the process of re-creating an identity for refugees and provides certain protections, "electronic refugees" may be particularly vulnerable. It may not be possible for refugee agencies to resist requirements to share personal data with host countries. These data are particularly sensitive because of risks to family members remaining in their countries of origin. [92]

Managing the Tradeoffs. Highly integrated ID systems – while often the most cost-effective and user-friendly –represent a greater risk than multiple incompatible systems

[92] See for example Hosein and Nyst (2014) and Lindskov Jacobsen (2015). Currion (2015) argues that government guarantees of privacy are not useful. He observes that even though the EC promised that its EURODAC database of asylum seekers would be protected in 2012, it allowed Europol and other law enforcement agencies access to the data.

that make it more difficult to link data.[93] However, fragmented systems are more costly and make the rationalization of government programs more difficult. Some ID applications, such as strengthening administration to catch tax evaders, require the ability to consolidate a wide range of information on income, assets and lifestyle from different databases. Fragmented systems may require individuals to submit personal information to multiple systems that could- in some ways - make the fragmented system less secure and more intrusive than a well-managed integrated one.

Countries may seek to combine the advantages of a single unique base identity with segregated functional databases. In Estonia, the databases of each department and service provider are held separately and are connected through the XROAD data exchange layer that manages the exchange of information as needed by each program. Security is further enhanced through the match-on-card identity credentials provided to each person enrolled in the system (section 5). Transparency can be increased—as in Estonia -- by logging each data access request submitted to the system and making the consolidated log available only to the individual concerned. Granting permission to access the data can be directly placed in the identity holder's hands, for example, by requiring a text message-based authorization for each access. The federated model of GOV.UK Verify provides another example of an approach to prevent the unauthorized sharing of personal data and block central access to the logged record of ID verification and transactions.

8.3 Wasteful Deployment

Chaotic Deployment is Costly. Without a strategic plan for their use or sufficient demand – for example, due to the lack of broad-based acceptance - identity projects can quickly disappear, only to be restarted later in a different form. As noted above, as many as 12 ID card projects were recorded in Nigeria during the early 2000s; the country of 173 million is estimated to have spent as much as $2 billion on ID schemes over the last ten years and still lacks a high-coverage national system. In contrast, India's Aadhaar ID program has enrolled over 920 million individuals at a cost to date of slightly more than $ 1 billion.

Multiple small programs are not cost-effective. The Dowa Emergency Cash Transfer (DECT) program in Malawi covered 11,000 rural families; fingerprints were used for initial registration and to verify payments at mobile ATMs in conjunction with smartcards. The program improved recipients' nutritional and health status but an assessment concluded that its small coverage and limited application rendered it uneconomic (Gelb and Clark 2013a). In another example, programs to ensure that Kenyan social protection programs reached their intended beneficiaries have been implemented by the financial institutions

[93] Other approaches can be used, such as phonetic algorithms that do not rely on a common number but compare fields such as names, addresses and other indicators. While they will not be as precise they may enable a fair degree of matching depending on the extent of identifying information available.

responsible for effecting payment. Recipients are therefore locked in to particular banks, and there would be a substantial cost to the program of switching to new intermediaries even if they offered better service. As noted previously, crash programs such as voter registration drives tend to be very costly because of the need to register large populations within a very short timeframe (as well as sometimes corrupt procurement). Separate one-off voter registration drives are probably the single largest wasted opportunity to strengthen countries' registration and identification systems.

These examples do not prove the case for a fully integrated system, but they do show the cost of a highly fragmented program-by-program approach towards the provision of ID services driven by the need to respond rapidly to a series of program demands.

Redundant or Inadequate Technology. The use of unnecessarily expensive technological solutions can raise costs beyond voter registration. The number of ID programs that capture biometric identifiers in addition to biographic data has increased exponentially in the last decade. Yet in many countries the benefits are limited to screening for multiple entries (de-duplication: and as noted above independent evidence on how well this is done is limited). Many countries have not deployed the infrastructure to enable real-time verification of individuals at points of service against their cards or the central database. As a result, day-to-day access to services can remain dependent on less reliable technology or visual authentication. Applications that require more than this, for example, to prove that pension recipients or registered voters are still alive may be forced to introduce their own, costly, programs to authenticate users even if there is a national ID. Before investing in expensive advanced technology, a careful assessment is needed of the expected benefits – in terms of reducing fraud and leakages, better targeting of service delivery, etc. – versus the expected additional costs – from the deployment of high-tech equipment for enrollment and use at service points, software and licensing fees, training of operators, etc.

Political Economy Constraints on the use of ID. While ID systems can be highly cost effective, their ability to fulfill their potential depends on the political economy in which they are implemented. Institutional (or bureaucratic) competition often stands in the way of better system integration. The institutions responsible for different registration and identification programs frequently operate under specific mandates that are invoked to ensure that each agency maintains control of its own facilities, systems and data. Political elites, who are sometimes the greatest beneficiaries of corruption, fraud, and the diversion of public resources, may laud more effective ID systems for certain purposes but stymie them when it comes to protecting their own interests.

Pakistan is one of the most advanced countries in the world in applying a biometric identification program to address development problems. It offers an illuminating example of the political economy constraints on potential applications of technology to strengthen

governance. Pakistan's program has been a remarkable success. Over 2008 – 2014 enrollments increased from 54 to 97 million while the percentage of women rose from 38.4% to 43.6% (Malik 2014). Financial support was provided to 400,000 internally displaced families and reconstruction grants disbursed to 3 million flood-affected families using biometrically linked smartcards. Eligibility for the Benazir Income Support Program (BISP) was put onto a more equitable footing using survey-based PMT tests and funds disbursed through a variety of mechanisms with identification managed through the common national system. A major cleaning of the electoral rolls carried out with the ID agency, NADRA, involved the deletion of 37 million voters: 15 million who were not able to be identified, 9 million duplicates and 13 million with invalid identities, and the inclusion of 36 million voters who had been excluded from the rolls. As explained in Section 4, NADRA operates on the basis of payments for services without budgetary support; its level of expertise is such that it regularly wins contracts to provide ID services in other countries.

Yet Pakistan also demonstrates the difficulties of applying an identification system in ways that impinge on the prerogatives of the elite and run counter to the interests of those in power. Three examples, set out in Malik 2014, illustrate the constraints.

Proxy prisoners. The identification of convicts serving long sentences by NADRA staff revealed that many were not who they purported to be – that they had been hired by wealthy and well-connected Pakistanis to serve out their sentences for them. After a brief outcry over the "proxy prisoners" scandal, no further action was taken.

Tax Evasion. Under a service agreement with the tax authorities, NADRA cross-referenced tax records with records of property and vehicle ownership, travel, and accounts with foreign banks to arrive at an estimated 3.5 million potential taxpayers, about five times the actual number of those paying tax. Despite the fact that Pakistan's tax yield, at around 10% of GDP, is among the lowest in the world, there has so far been no follow-up.[94]

Voter Fraud. Cleaning the voter rolls resulted in a shifting of the locus of election fraud to the polls. In response to challenges from the opposition parties, ex-post verification of fingerprints required on ballot papers revealed evidence of massive voter fraud in key constituencies, including, for example, hundreds of votes by a single male voter at a voting facility reserved exclusively for women. NADRA was pressured by the government to repudiate its findings. After threats to his life and family its Chairman was forced to flee the country.

These risk areas show the importance of a strategic approach towards ID that includes up-front attention to the legal infrastructure, cost-effectiveness and how to ensure wide coverage, as well as a realistic appreciation of how the system is expected to be used.

[94] There has been follow-up in other cases; for Argentina's SINTESIS program see Pessino 2007. For estimates of the potential savings in costs and time from shifting to e-transactions see Secure Identity Alliance 2013.

9 Towards the Future

The last several years have seen some major changes in the landscape around identification and development. ID programs have proliferated, both foundational (national ID or similar) and functional programs serving particular applications, and are using far more advanced technology than previously. Civil registration and capable ID systems are now seen as key elements of development policy and programs. This marks a shift from seeing identification in the narrow context of particular programs towards strategies that strengthen the wider ID system and the birth and civil registration needed to anchor identities.

As part of this process, countries' systems are being assessed in a more comprehensive way as a component of development policy with a view to maximizing benefits and minimizing risks (ID4D). At the same time, two common problems remain:

- Integrating birth and civil registration and identity management so that these work together as a strong unified system. In many countries this will require coordinated efforts to strengthen birth and civil registration and to reinforce core identification services, establishing a robust identity baseline for those previously excluded and integrating the use of ID into programs.
- Reconciling urgent needs for functional identification (elections, transfers, payments, financial access, health, e-Identity) with lagging foundational ID systems in a way that strengthens and integrates the overall system rather than fragments it further.

The challenge will be to resolve these tensions in an effective way, taking into account the different starting-points and legacy systems of particular countries and drawing on best practice and advances in technology. ID systems and technology continue to evolve rapidly, both in terms of establishing identity baselines and especially in mechanisms to authenticate identity to facilitate remote transactions. Developing countries have shown the ability to leapfrog in this area (Malaysia-multi-application ID, India-UID) and can continue to do so. At the same time, ID technology and related ICT have outrun consensus on their use and oversight, and also the social and political processes needed to determine their most appropriate deployment.

Performance benchmarks. Following SDG 16.9, universal birth registration is accepted as a global goal. So is access to identity, although there is no global consensus on the precise measurement of identity (as appropriate to development) or on the ideal ID system. However, identity services can be benchmarked in generally-agreed ways.

- Identities should be robust, unique and continuous over the life-cycle and extend to individuals not just credentials. With the growth of e-Services and the e-Economy, e-Identity is becoming a priority for developing countries as well as for rich ones.

- Credentials should be widely and easily accessible, including for disadvantaged groups. Access to identity should facilitate access to rights and services rather than be a barrier.

- Even if not all agree on the merits of a fully integrated system excessive fragmentation is a problem. Greater inter-operability is desirable: national IDs and resident cards may be moving towards ICAO standard. This could be seen as a relevant goal especially because of the rising level of international travel and migration.

Performance data from India's UID program can help to provide a basis for standards in other countries for registration, uniqueness and authentication. Developing countries, as well as donors who fund a new system or the roll-out of an established system across the population, need to be confident that it is performing as represented. This may call for an independent assessment, for example to ascertain that it does indeed have the capacity to identify individuals against records in its database. It will also be important to understand how the system handles identification errors, makes provision for those unable to provide biometrics of acceptable quality and provides for data privacy and protection. There is not at present such a standards-setting body to help rationalize support to ID programs and encourage their most effective support for development priorities. This could be a useful initiative for major supporters, including the IFIs, UN agencies, industry experts and certain developing country governments.

Improving Access through Integrating Demand and Supply. Countries and development partners have sought to strengthen identity systems through a number of targeted interventions to spur demand and supply, including efforts to extend coverage to excluded groups. Policies to bolster the supply of ID services include the use of mobile units (Pakistan, Peru, Malaysia), new technology (mobile birth registration, as recently introduced in Tanzania[95]), integrating health facilities and registration offices (Uruguay), and involving NGOs to assist with enrollment (Indonesia). On the demand side, policies aimed at incentivizing registration through links to services (access to social grants) have often been critical. Streamlining registration requirements through an "ID-first" approach (India – UID) have also been shown to enable rapid increases in enrolment levels. Providing birth registration and basic ID services without charge helps extend inclusive systems and ID as a public good.

[95] See: Millicom (2013)

Making use of existing registries. In countries where the civil registry is sufficiently well-developed and covers a large share of the population, linking the civil registry and the ID system improves robustness through being better able to trace individuals from their birth throughout their lives. Lifetime identity management can be strengthened by more complete and earlier birth (and death) registration as well as by initiating biometric registration around the age of 5, much earlier than generally done (15-18). Even where the civil registry is incomplete, digitization of paper records serves as a building block in a robust, universal ID program.

Where the quality of civil registry is low, other registries could help provide a foundation for a broad ID system, at least on an interim basis. The rapid rollout of some other programs, notably voter rolls in countries with lagging national ID programs (Nigeria, Tanzania), suggests the potential of building on "credential-lite" programs or enrollments motivated by particular applications to strengthen the ID system as a whole (Bangladesh). For this "functional-to-foundational" path to work, it is important that the functional programs have inter-operability with (if not evolve into) the national program.

Institutional Alternatives. Cases show a wide range of institutional arrangements and architectures for delivering ID services. There is no ideal model, but there may be some advantage for locating registration and identification services in an autonomous entity substantially funded through payments for service. This can clarify the mandate and save on duplicate facilities. It can also help to de-politicize the provision of ID, so encouraging a more integrated system.

Considering the small size of many countries there could be advantage in fewer and stronger ID agencies, perhaps providing services or a mechanism along the lines of UID across economic communities like ECOWAS or the EAC. Estonia's e-Residency may signal the start of such processes to internationalize the provision of ID services. Even if this is politically infeasible in the short term, IDs issued by such groups of countries should be inter-operable (as is increasingly the case in the European Union for national and resident cards) to facilitate mobility.

Technology Choice. The identification technology landscape is changing rapidly, both in terms of ease of registration and the ID integration and management possibilities offered by new systems. Biometric identifiers in the form of fingerprint- and iris scans are now being used for registration and authentication in a large number of functional and foundational ID programs. New technologies, such as voice and hand-vein recognition are currently being tested –primarily by the banking sector – and may prove to be more efficient options in the future. However, the initial choice of biometrics (legacy technologies) for a given ID program will likely constrain the possibilities for adopting of more novel (and perhaps more accurate) identification technologies in the years or even decades to come.

Technology has the potential to enable better ID systems but is of little value without good implementation. Cost-effectiveness is limited where programs lack the necessary point-of-service infrastructure to use the capabilities of the system. The excessive cost of technology has been a particular concern for one-off functional programs, particularly voter registration and authentication. The standards-based nature of the UID program can help to pave the way for more competition and more open, lower-cost, technology.

Integration into Programs. Several countries offer examples of how strengthened identity systems can improve the management of diverse programs, improve service delivery and inclusion and also recover their costs. In the case of India, the decision that the National Population Registry should use the technology developed by the UID program is a major step forward in preventing further fragmentation but all too often data systems remain incompatible between functional and foundational programs.

Programs and government agencies have a natural tendency to defend their own mandates and ID systems, including to preserve control over technology procurement. They will often resist integration on the grounds that this involves transitional costs. Development partners can help by coordinating support to coalitions of users and helping to finance the costs of transitioning to a common ID system as a basis for implementing programs. This could be the national ID (subject to its being of adequate quality) or, if this is not possible, a system to at least identify participants for a broad set of social protection, payments and pension programs.

The evidence on the use of the new ID systems is still largely anecdotal. Relatively few applications have been rigorously assessed to understand the holistic impact of the new systems – on costs, savings, access and quality. The need for more knowledge in this area is emerging at a key issue as the focus moves on from the ID programs themselves towards their use to deliver services.

Integration, Privacy and Data Security. These areas have not been a main focus for this overview, but there will be continued debate on the tradeoffs associated with more integrated versus less integrated ID systems and data registers in general. One model adopted by several countries is to have a single ID system with minimal personal data servicing multiple independent program registers and with strong legal sanctions against unauthorized access and sharing (Estonia, others). Another model, as for GOV.UK Verify, is a “fuzzy” ID system with multiple mechanisms to authenticate users for different programs. This breaks the link between the core ID documentation (passport, driver’s license, etc) and the application data, making it more difficult to consolidate a transactions record.

Fragmented IDs and program databases may appear less worrisome from a privacy and security perspective than more integrated systems. But, especially in countries with lower

levels of capacity, managing and securing multiple systems (and securing data when programs cease to operate) may present a challenge. The tradeoffs include those related to multiple registration, costs, and the capacity to coordinate public services in a user-centric way. These issues go beyond the ID system itself to include a wide range of personal data.

Strategies have to take into account the different starting points of the countries. Institutional mandates and legacy systems set limits on how rapidly countries are prepared to revamp their systems. Countries are continually upgrading their systems but usually initiate a major overhaul in response to urgent needs. Examples include security and national integration (Peru, Pakistan); to clean up a corrupted system (South Africa) and to ease fiscal pressure by reforming massive subsidy programs (India). Governments upgrade to provide important new services, such as to facilitate international travel and transit (Cape Verde ICAO-compliant cards, Macao contactless card) or to facilitate e-Services. Major pushes in functional systems usually respond to urgent needs (clean elections, ensuring that transfer recipients are still living) that the national system cannot be trusted to satisfy. While every country is different we can distinguish three broad cases:

- **Countries without a functioning national-level ID system or where the coverage of the system is very low**. These will typically be the poorest countries, often conflict-affected. In addition to goals of a political nature (security, nation-building and national integration) they usually face severe administrative constraints in the face of urgent development needs – to manage public payroll, pensions and transfers, pay service providers (teachers or health workers in Ebola countries), or provide a basic ID to satisfy KYC requirements.

  These cases suggest the possibility of strengthening the system through a strong focus on applications. There might be a window for rolling out a functional "credential-lite" system or an "ID-first" system like the Aadhaar that could also strengthen a national ID or a similar program. Such a functional ID would be implemented with needs-based priority and scaled up into a first stage (or a component) of a multi-purpose or national ID. For this to work, it would be essential to include a sufficiently broad set of users and donor-supported programs as clients to be sure that the system has enough demand to encourage people to register. It would also be essential to have a clear understanding with the agencies responsible for civil registration and identification on how the accelerated program contributes to the wider ID system as well as the capabilities and quality of the existing system if it is to be the basis for the future one.

  Governments are unlikely to be prepared to outsource the management of the identities of their citizens to private or offshore entities, but they may agree to cooperative arrangements, especially if these include support to strengthen their own data and systems (Pakistan data-sharing protocol; Tanzania health workers

registration, possible enlistment of mobile operators that require SIM registration as enrollment agents or facilitators). Faced with the need to identify their program beneficiaries, it may be more cost-effective for development agencies to support the extension of the national system (if of adequate quality) than to re-invent their own. It could be useful to form a partnership with private service providers to defray part of the cost of rolling out a system but the optics of such arrangements need careful management (Mastercard-Nigeria).

- **Countries with working ID systems that seek to upgrade their functionality**. Such cases may need to improve the capabilities of the system – for example to strengthen its ability to authenticate pension or transfer recipients to ensure that they are still living (Kenya) or to be able to provide more sophisticated ID, mobile ID or multi-purpose smartcards to part of the population to facilitate travel or remote authentication. In some cases it is sufficient to upgrade the card; in others the change may require re-registration. This can proceed as existing credentials need renewal and also on the basis of need (priority re-registration of pension or transfer recipients).

  Upgrading can also involve measures to integrate a high-capability system into a wider set of programs, including the provision of POS technology as necessary to exploit the capabilities of the system (Indonesia). Since the core system already exists, these programs should have a high payoff. Stronger integration provides a key feedback loop, helping to extend the coverage of the core system and update its population data (Pakistan).

- **Countries with multiple incompatible systems**. With strong entrenched interests these can present the greatest obstacles to reform (Nigeria). The limited demand for the core system is likely to slow efforts to roll it out. This is more a political problem than a technical one. Approaches to strengthening the system can include providing sustained support to birth and civil registration and to institutional consolidation (such as the ongoing efforts to centralize the management of identity databases in the NIMC) and encouraging registration through introducing at least a "soft" requirement for the common ID in programs where this is possible without creating a barrier.

Some Areas for Further Research. Systematic information on ID systems and their use in development programs is only beginning to be developed. There is a large agenda for fact-finding and research.

- **The comparative architecture of country systems**. With only a limited number of country stems surveyed through a common comparative methodology that covers both the provision of ID services and their use, there is great need to expand

coverage to more cases, including the motivation for systemic innovations and their impact. Integration between civil registration and identification is still a frontier issue for many countries.

- **The use and impact of ID technology and systems.** Many more studies are needed of the implementation of new systems and their impact, particularly on those entitled to the services. Do the new systems facilitate quality and access or do they constitute a barrier? Do they help people to assert rights (including women)? Is there a differential impact on different groups? This is a potentially rich research agenda considering the rollout of new applications in India and elsewhere.

- **Monitoring new ID technology and its deployment**. This can include new biometrics – voice technology, for example, could make a potentially valuable contribution to mobile ID in sparse developing countries – as well as new applications of established biometrics. Federated and network-based identity (or authentication of identity) may not be the most pressing topic for poor countries where many still lack the building-blocks for identity management but may be important for the future. The identification of infants and young children remains a frontier area for research.

- **Incentives and technology to improve CRVS including death registration**. With the increasing number of programs in this area there is scope for useful comparative research, including on the impact of new technology (mobile registration) and the effectiveness of different incentives to register vital events.

- **Standards and interoperability**. The UID program has had a major impact on the ID industry but many technologies are still proprietary. Countries would benefit from guidelines to help ensure that they, not the vendors, retain control over hardware, software and data systems and that they are not locked in to particular providers.

- **Legal frameworks in poor countries**. While there is some useful data on the cross-country spread of data privacy legislation there is less detailed information on the actual situation and the capacity of countries to implement data protection laws. This topic extends beyond identification but is set to become more important with the spread of digital communications and big data, including in developing countries.

Bibliography

ACHPR (2014). *The Right to Nationality in Africa*. Banjul, The Gambia: African Commission on Human and People's Rights.

Accenture (2015). How Can Border Management Solutions Better Meet Citizens' Expectations? Report on the Accenture Citizen Survey on Border Management and Biometrics 2014. Retrieved from: https://www.accenture.com/au-en/insight-border-management-solutions-better-meet-citizens.aspx.

Airbnb (2013). "Introducing Airbnb verified ID". Airbnb blog. Retrieved from: http://blog.airbnb.com/introducing-airbnb-verified-id/.

Akpan, N. (2014). "Baby's Necklace Could End Up Being a Lifesaver". Goats and Soda blog. National Public Radio online. Retrieved from: http://www.npr.org/sections/goatsandsoda/2014/12/05/366405541/babys-necklace-could-end-up-being-a-life-saver.

Anand, U. (2015). "Aadhaar card: SC allows Centre to link Aadhaar with PDS, LPG subsidy". The Indian Express online. Retrieved from: http://indianexpress.com/article/india/india-others/supreme-court-allows-centre-to-link-aadhaar-card-with-social-benefit-schemes/.

Arm, M. (2014). SK: 12+ Years of e-ID in Estonia. *Presentation at the IdentityNorth 2014 conference in Toronto, Canada*. Retrieved from: http://www.identitynorth.ca/wp-content/uploads/2014/06/e-estonia_052014_2-f.pdf.

Arthur, C. (2014). "Gov.uk quietly disrupts the problem of online identity login". Government Digital Service blog via theguardian.com. Retrieved from: http://www.theguardian.com/technology/2014/nov/06/govuk-quietly-disrupts-the-problem-of-online-identity-login.

Atick, J. J. (2014). Digital Identity: The Essential Guide. ID4Africa Identity Forum. Retrieved from: http://www.id4africaforum.com/img/Digital_Identity_The_Essential_Guide.pdf.

Aung, M. T. and Mar, K. (2015). "Myanmar Officials Issue Green Cards to Muslims in Rakhine State". Radio Free Asia online. Retrieved from: http://www.rfa.org/english/news/myanmar/officials-issue-green-cards-to-muslims-in-rakhine-state-06152015145915.html.

Banerjee, A. V., Glennerster, R., and Duflo, E. (2008). Putting a Band-Aid on a Corpse: Incentives for Nurses in the Indian Public Health Care System. *Journal of the European Economic Association*, 6 (2-3), pp. 487-500.

Bennett, C. J. and Lyon, D. (Eds.) (2008). *Playing the Identity Card: Surveillance, Security, and Identification in Global Perspective*. New York, NY: Routledge.

Bhatnagar, N., Sinha, A., Samdaria, N., Gupta, A., Batra, S., Bhardwaj, M. and Thies, W. (2012). Biometric Monitoring as a Persuasive Technology: Ensuring Patients Visit Health Centers in India's Slums. Persuasive Technology. *Design for Health and Safety – 7th International Conference Proceedings*. June 6-8, 2012.

Blake, J. N. (2014). Haiti, the Dominican Republic, and Race-based Statelessness in the Americas. *Georgetown Journal of Law and Modern Critical Race Perspectives*, 6(2), pp. 139-180.

Breckenridge, K. (2005). The Biometric State: The Promise and Peril of Digital Government in the New South Africa. *Journal of Southern African Studies*, 31(2), 267-282.

Breckenridge, K. and Szreter, S. (Eds.) (2012*). Registration and Recognition: Documenting the Person in World History*. Proceedings of the British Academy (182). Oxford, UK: Oxford University Press.

Campbell, B. (2010). "Financial Opportunity". Profit Magazine online. Oracle website. Retrieved from: http://www.oracle.com/us/corporate/profit/archives/092010-oppint-176389.html.

Carson, K. A. (2011). Legibility and Control: Themes in the Work of James C. Scott. Center for a Stateless Society Paper No. 12. Retrieved from: http://c4ss.org/wp-content/uploads/2011/05/James-Scott.pdf.

Carter Center (2012). Voter Identification Requirements and Public International Law: An Examination of Africa and Latin America. Atlanta, GA: Carter Center.

CENI (Commission Electoral Nationale Indépendante) (2015). Rapport general du scrutin du 25 avril 2015. Retrieved from: http://www.ceni-tg.org/?p=4453.

Central Bank of Nigeria (2015). Bank Verification Number website. Retrieved from: http://www.bvn.com.ng/.

CESG (2014). Identity Proofing and Verification of an Individual. Good Practice Guide No. 45. National Technical Authority for Information Assurance. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf.

CIS Kenya (2015). "What is Credit Information Sharing (CIS)". CIS Kenya website. Retrieved from: http://www.ciskenya.co.ke/cis.

Currion, P. (2015). "Eyes Wide Shut: The challenge of humanitarian biometrics." IRIN News. Retrieved from: http://www.irinnews.org/report/101913/eyes-wide-shut-the-challenge-of-humanitarian-biometrics.

Dahan, M. and Gelb, A. (2015a). The Role of Identification in the Post-2015 Development Agenda. Center for Global Development Essay. Washington, DC: Center for Global Development.

Dahan, M. and Gelb, A. (2015b). The Identity Target in the Post-2015 Development Agenda. World Bank Transport & ICT Connections Series, Note 19. Retrieved from: http://pubdocs.worldbank.org/pubdocs/publicdoc/2015/9/553511442506682828/1603399-TransportICT-Newsletter-Note-19.pdf.

DELIVER (2007). *South Africa: Final Country Report*. Arlington, VA: DELIVER, for the U. S. Agency for International Development.

Department of Health and Human Services. (2000). "Birth certificate fraud". Office of the Inspector General. Retrieved from: http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf.

Dhaliwal, I. and Hanna, R. (2014). Deal with the Devil: The Successes and Limitations of Bureaucratic Reform in India. NBER Working Paper 20482. Cambridge, MA: National Bureau of Economic Research.

Dunning, C., Gelb, A., and Raghavan, S. (2014). Birth Registration, Legal Identity, and the Post-2015 Agenda. Center for Global Development Policy Paper 046. Washington, DC: Center for Global Development.

Dymi, A. (2014). "Chinese Bank Deploys ATM with Finger Vein Authentication". American Banker online. Retrieved from: http://www.americanbanker.com/issues/179_37/chinese-bank-deploys-atms-with-finger-vein-authentication-1065809-1.html.

E-Estonia (2013). "Measuring the impact of e-services – case study". E-estonia.com website. Retrieved from: https://e-estonia.com/measuring-impact-e-services-case-study/.

E-Estonia (2014). "Become and Estonian e-Resident" leaflet. Retrieved from: https://e-estonia.com/wp-content/uploads/2014/09/eResident_leaflet.pdf.

E-Estonia (2015). "i-Voting". E-estonia.com website. Retrieved from: https://e-estonia.com/component/i-voting/.

Economia (2013). "Fidor: Banking with friends". Economia website. Retrieved from: http://economia.icaew.com/business/july-2013/fidor-banking-with-friends.

Ensor, L. (2014). "Re-registration of social grant recipients saves R2bn". Business Day live online. Retrieved from: http://www.bdlive.co.za/national/2014/02/05/re-registration-of-social-grant-recipients-saves-r2bn.

Feere, J. (2010). "Birthright Citizenship in the United States: A Global Comparison". Center for Immigration Studies. Retrieved from: http://cis.org/birthright-citizenship.

FWLD (2014). Acquisition of Citizenship Certificate in Nepal. Forum for Women, Law, and Development. Publication No. 169. Retrieved from: http://www.fwld.org/uploads/pdf/Acquisition%20of%20Citizenship%20Certificate%20in%20Nepal%20(Report).pdf.

Frieden, P. (2015). Linking democracy Aid to Public Opinion Research: Findings from Sixteen Countries in Sub-Saharan Africa. *Democracy and Society*, 12(2).

Gelb, A. (2011). "Covering the 7 Billionth Child: Can We Learn from Indian Health Insurance?" Center for Global Development blog. Retrieved from: http://www.cgdev.org/blog/covering-7-billionth-child-can-we-learn-indian-health-insurance.

Gelb, A. (2015). "Labor Pains: Birth and Civil Registration in Indonesia". Center for Global Development blog. Retrieved from: http://www.cgdev.org/blog/labor-pains-birth-and-civil-registration-indonesia.

Gelb, A. and Clark, J. (2013a). Identification for Development: The Biometrics Revolution. CGD Working Paper 315. Washington, DC: Center for Global Development.

Gelb, A. and Clark, J. (2013b). Performance Lessons from India's Universal Identification Program. CGD Policy Paper 020. Washington, DC: Center for Global Development.

Gellman, R. (2013). Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. CGD Policy Paper 028. Washington, DC: Center for Global Development.

GOV.UK Verify (2015). "Total authentications". Gov.uk Verify website. Retrieved from: https://www.gov.uk/performance/govuk-verify/total-authentications.

Greenleaf, G. (2013). Global Data Privacy Laws 2013: 99 Countries and Counting. *Privacy Laws & Business International Report*, June 2013, pp. 10-13.

Groebner, V. (2007). *Who Are You?: Identification, Deception, and Surveillance in Early Modern Europe*. Brooklyn, NY: Zone Books.

Groenfeldt, T. (2015). "Lenddo Creates Credit Scores Using Social Media". Forbes online. Retrieved from: http://www.forbes.com/sites/tomgroenfeldt/2015/01/29/lenddo-creates-credit-scores-using-social-media/.

Harbitz, M. and Molina, J. C. B. (2010). *Civil Registration and Identification Glossary*. Washington, DC: Inter-American Development Bank.

Herlihy, P. (2013). "Government as a data model: what I learned in Estonia". Government Digital Service blog (UK). Retrieved from: https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.

Hopkins, A. and Hughes, J. (2014). Biometrics in a Humanitarian Context. UNHCR. *Presentation at the Connect:ID Conference, March 17-19, 2014*. Retrieved from: http://www.connectidexpo.com/creo_files/expo2014-slides/1700_Hopkins_Hughs.pdf.

Hosein, G. and Nyst, C. (2013). Aiding surveillance: An exploration of how development and humanitarian aid incentives are enabling surveillance in developing countries. Privacy International. Retrieved from: https://www.privacyinternational.org/sites/default/files/Aiding%20Surveillance.pdf.

Hughes, J. (2014a). "What is identity assurance?". Government Digital Service blog. Retrieved from: https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/.

Hughes, J. (2014b). "How does a certified company establish that it's really you?". Identity Assurance and Gov.UK Verify blog. Retrieved from: https://identityassurance.blog.gov.uk/2014/11/21/how-does-a-certified-company-establish-that-its-really-you/.

ID.ee (2015). "Statistics". ID.ee website. Retrieved from: http://www.id.ee/?lang=en.

IDEA. (2015). Voter Turnout Database. International Institute for Democracy and Electoral Assistance website. Retrieved from: http://www.idea.int/vt/viewdata.cfm (last updated August 2015).

IRC (2014). Emergency Economies: The Impact of Cash Assistance in Lebanon. International Rescue Committee report. Retrieved from: https://data.unhcr.org/syrianrefugees/download.php?id=7112.

International Telecommunications Union. (2015). ICT Statistics database 2005-2015. Retrieved from: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Jain, A. K., Cao, K., and Arora, S.S. (2014). Recognizing Infants and Toddlers Using Fingerprints: Increasing the Vaccination Coverage. *Proceedings of the International Joint Conference on Biometrics (IJCB), 29 Sept - 2 Oct, 2014*.

Jain, A. K., Arora, S. S., Best-Rowden, L., and Cao, K. (2015). Biometrics for Child Vaccination and Welfare: Persistence of Fingerprint Recognition for Infants and Toddlers. *MSU Technical Report, MSU-CSE-15-7, 2015*.

Kelly, H. (2012). "83 million Facebook accounts are fakes and dupes". CNN online. Retrieved from: http://www.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/index.html.

KNHCR (2007). An Identity Crisis? A Study on the Issuance of National Identity Cards in Kenya. Kenya National Commision on Human Righs. Retrieved from: http://www.knchr.org/Portals/0/EcosocReports/KNCHR%20Final%20IDs%20Report.pdf

Kwambai, K. D. and Wandera, M. (2013). Effects of Credit Information Sharing on Nonperforming Loans: The Case of Kenya. European Scientific Journal, 9 (13), pp. 168-193.

La Cour d'Appel de Lomé. (2015). "Pieces a fournir pour l 'obtention du certificat de nationalité togolaise". La Cour d'Appel de Lomé website. Retrieved from:

http://lacourdappeldelome.com/pieces-a-fournir-pour-l-obtention-du-certificat-de-nationalite-togolaise/

Le Parisien (2011). "Plus de 10% des passeports biometriques seraient des faux". Le Parisien online. Retrieved from: http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php.

Lindskov Jacobsen, K. (2015). *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity*. New York, NY: Routledge.

Malik, T. (2014). Technology in the Service of Development: The NADRA Story. Center for Global Development Essay. Retrieved from: http://www.cgdev.org/sites/default/files/CGD-Essay-Malik_NADRA-Story_0.pdf.

Manby, B. (2010). *Citizenship Law in Africa*. New York, NY: Open Society Foundations.

McEvoy, J. (2015). "Services that plan to start using GOV.UK Verify". Identity Assurance and GOV.UK Verify blog. Retrieved from: https://identityassurance.blog.gov.uk/2015/07/23/services-that-plan-to-start-using-gov-uk-verify/.

Middlehurst, C. (2015). "China unveils world's first facial recognition ATM". The Telegraph online. Retrieved from: http://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html.

Millicom (2013). "Birth registration in Tanzania". Millicom News Features. Retrieved from: http://www.millicom.com/media/millicom-news-features/birth-registration-in-tanzania/.

ODI (2015). Doing cash differently: How cash transfers can transform humanitarian aid. Report of the High Level Panel on Humanitarian Cash Transfers. London, UK: Overseas Development Institute.

Open Society Institute (2010). Dominicans of Haitian Descent and the Compromised Right to Nationality. *Report presented to the Inter-American Commission on Human Rights on the Occasion of its 140th Session*. Retrieved from: https://www.opensocietyfoundations.org/sites/default/files/Dominican-Republic-Nationality-Report-ENG-20110805.pdf.

Operation ASHA (2015). "eCompliance Biometric Tracking System". Operation ASHA website. Retrieved from: http://www.opasha.org/our-work/ecompliance-innovation-and-health/ecompliance-biometric-tracking-system/

Oppenheim, B. and Powell, B. M. (2015). Legal Identity in the 2030 Agenda for Sustainable Development: Lessons from Kibera, Kenya. Open Society Justice Initiative Policy Paper. New York, NY: Open Society Foundations.

Opportunity International (2014). Annual Report. Retrieved from: http://opportunity.org/annual-report/2014.

Palacios, R., Das, J., and Sun, C. (Eds.). (2011). *India's Health Insurance Scheme for the Poor: Evidence from the Early Experience of the Rashtriya Swasthya Bima Yojana*. New Delhi: Centre for Policy Research.

Pasricha, N. (2011). "G2P Payment for Flood Victims in Pakistan". Consultative Group to Assist the Poor blog. Retrieved from: http://www.cgap.org/blog/g2p-payments-flood-victims-pakistan.

Pew Research Center. (2015). "Internet Seen as Positive Influence of Education but Negative on Morality in Emerging and Developing Nations". Retrieved from: http://www.pewglobal.org/files/2015/03/Pew-Research-Center-Technology-Report-FINAL-March-19-20151.pdf.

PhilHealth (2014). "Issuance and Voluntary Availment of the PhilHealth Health Insurance Card (HIC) by the Members of the Formal Economy". PhilHealth Circular No. 0005 S. 2014. Retrieved from: http://www.philhealth.gov.ph/circulars/2014/TS_circ05_2014.pdf.

Planet Biometrics (2015). "Dermalog tech used to enroll 18m in Nigerian banking initiative". Planet Biometrics website. Retrieved from: http://www.planetbiometrics.com/article-details/i/3434/desc/dermalog-tech-used-to-enrol-18m-in-nigerian-banking-initiative/

Raj, S. (2014). "Tracking India's Bureaucrats Becomes a Digital Dashboard Venture". The New York Times online. Retrieved from: http://www.nytimes.com/2014/10/12/world/asia/in-india-government-tracks-its-own.html.

Reyna, C. (2014). Civil Registration and Identification System in Peru: Key features. *Presentation at the World Bank South-South Social Protection and Learning Forum on March 17, 2014*. Retrieved from: http://www.worldbank.org/content/dam/Worldbank/Event/social-protection/Building_Robust_Identification_Systems_Session_Packet.pdf.

Schmidt, A. (2013). "Brazilian banks lead way on biometrics". Marketplace Tech online. Retrieved from: http://www.marketplace.org/topics/tech/brazilian-banks-lead-way-biometrics

Scott, J. C. (1998). *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale Institution for Social and Policy Studies Series. Binghamton, NY: Vail-Ballou Press.

Sumner, C. (2015). Indonesia's Missing Millions: Erasing Discrimination in Birth Certification in Indonesia. Center for Global Development Policy Paper 064. Washington, DC: Center for Global Development.

UNDP (2015a). "Innovative payment technology for Ebola response workers launched". UNDP Sierra Leone press release, January 28, 2015. Retrieved from: http://www.sl.undp.org/content/sierraleone/en/home/presscenter/pressreleases/2015/01/28/building-transparent-payment-systems-through-deployment-of-innovative-payments-technology-for-ebola-response-workers-.html.

UNDP (2015b). Payments Programme for Ebola Response Workers: Cash at the Front Lines of a Health Crisis. Issue Brief. Retrieved from: http://www.undp.org/content/dam/undp/library/hivaids/English/Payments-Programme-Ebola-Response-Workers.pdf.

UNHCR (2013). "Request for Proposal: No. RFP/2012/507 for the Provision of a Biometric Identity Management System". Retrieved from: http://www.unhcr.org/50c85dd69.pdf.

UNHCR (2014). "Background Note on Gender Equality, Nationality Laws and Statelessness 2014". Retrieved from: http://www.unhcr.org/4f5886306.html

UNHCR (2015). "Citizenship and Statelessness in Myanmar". UNHCR Briefing for the World Bank. September 3, 2015.

UNICEF (2013). *Every Child's Birth Right: Inequities and trends in birth registration*. New York, NY: UNICEF.

UNICEF (2014). Birth registration dataset. UNICEF global databases. Retrieved from: http://data.unicef.org/child-protection/birth-registration.html (last updated: November 2014).

UNSD (2014). Coverage of civil registration system dataset. United Nations Statistics Division website. Retrieved from: http://unstats.un.org/unsd/demographic/CRVS/CR_coverage.htm (last updated: December 2014).

VISA (2010). "Pakistan Flood Victims Receive Government Relief Aid on 'Watan' Visa Cards". Press Release. Retrieved from: http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1468949.

Warman, M. (2013). "Say goodbye to the pin: voice recognition takes over at Barclays Wealth". The Telegraph online. Retrieved from: http://www.telegraph.co.uk/technology/news/10044493/Say-goodbye-to-the-pin-voice-recognition-takes-over-at-Barclays-Wealth.html.

WFP (2013). "WFP Innovative Food Assistance Instruments – The Biometric Project, Kenya". World Food Programme website. Retrieved from: http://documents.wfp.org/stellent/groups/public/documents/resources/wfp271054.pdf

World Bank (2011). Wage Bill and Pay Compression. [Dataset]. Retrieved from: http://data.worldbank.org/data-catalog/wage-bill-pay-compression.

World Bank (2012). Indonesia: Women Headed Household Empowerment Program (PEKKA). World Bank website. Retrieved from: http://www.worldbank.org/en/results/2012/04/19/indonesia-women-headed-household-empowerment-program-pekka.

World Bank (2014). "The World Bank Group in Somalia: Helping to Rebuild State Institutions Piece by Piece". World Bank News. Retrieved from: http://www.worldbank.org/en/news/feature/2014/10/27/the-world-bank-group-in-somalia-helping-to-rebuild-state-institutions-piece-by-piece.

Yu, K-L., Cheng, C-C., Chang, W-S., Juma, H., and Chang, C-S. (2005). Fingerprint identification of AIDS patients on ART. *The Lancet*, 365, p. 1466.

Zelazny, F. (2012). The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. CGD Policy Paper 008. Washington, DC: Center for Global Development.

Zetter, K. (2012). "Reverse-engineered irises look so real, the fool eyes-scanners". Wired magazine online. Retrieved from: http://www.wired.com/2012/07/reverse-engineering-iris-scans/.