Identification for Development: The Biometrics Revolution

Alan Gelb and Julia Clark

Abstract

Formal identification is a prerequisite for development in the modern world. The inability to authenticate oneself when interacting with the state—or with private entities such as banks—inhibits access to basic rights and services, including education, formal employment, financial services, voting, social transfers, and more. Unfortunately, underdocumentation is pervasive in the developing world. Civil registration systems are often absent or cover only a fraction of the population. In contrast, people in rich countries are almost all well identified from birth. This "identity gap" is increasingly recognized as not only a symptom of underdevelopment but as a factor that makes development more difficult and less inclusive.

Many programs now aim to provide individuals in poor countries with more robust official identity, often in the context of the delivery of particular services. Many of these programs use digital biometric identification technology that distinguish physical or behavioral features, such as fingerprints or iris scans, to help "leapfrog" traditional paper-based identity systems. The technology cannot do everything, but recent advances enable it to be used far more accurately than previously, to provide identification (who are you?) and authentication (are you who you claim to be?). Technology costs are falling rapidly, and it is now possible to ensure unique identity in populations of at least several hundred million with little error.

This paper surveys 160 cases where biometric identification has been used for economic, political, and social purposes in developing countries. About half of these cases have been supported by donors. Recognizing the need for more rigorous assessments and more open data on performance, the paper draws some conclusions about identification and development and the use of biometric technology. Some cases suggest large returns to its use, with potential gains in inclusion, efficiency, and governance. In others, costly technology has been ineffective or, combined with the formalization of identity, has increased the risk of exclusion.

One primary conclusion is that identification should be considered as a component of development policy, rather than being seen as just a cost on a program-by-program basis. Within such a strategic framework, countries and donors can work to close the identification gap, and in the process improve both inclusion and the efficiency of many programs.

JEL Codes: H80, J10, O33, O38, Z18

Keywords: biometric identification, civil registry, voter registration, G2P, financial inclusion, transfers.

Center for Global Development
www.cgdev.org

Working Paper 315
January 2013

Identification for Development: The Biometrics Revolution

Alan Gelb
Center for Global Development

Julia Clark
Center for Global Development

The authors thank Charles Kenny, Roberto Palacios, Wyly Wade, and Frances Zelazny for helpful comments as well as participants at the 2012 World Bank / IIT Conference on Implementing Social Programs: "Better Processes, Better Technology, Better Results," in Bangalore, India, and the 2012 Biometrics Consortium Convention in Tampa, Florida. Caroline Decker contributed to early drafts of this paper. All errors of interpretation or omission are the responsibility of the authors.

CGD is grateful for contributions from the UK Department for International Development and the William and Flora Hewlett Foundation in support of this work.

Alan Gelb and Julia Clark. 2013. "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development. http://www.cgdev.org/content/publications/detail/1426862

Center for Global Development
1800 Massachusetts Ave., NW
Washington, DC 20036

202.416.4000
(f) 202.416.4050

www.cgdev.org

Contents

Abbreviations ii
Figures and Graphs iii
1. Introduction 1
2. Identification, development, and biometrics 5
    2.1. Official Identity and the identity gap 5
    2.2. The Technology revolution and its limits 8
    2.3. Perspectives and concerns 12
3. Survey of Biometric identification Applications 19
    3.1. Overview 19
    3.2. Functional Applications 23
    3.3. Foundational Applications 35
    3.4. Pathways to a National Identity System 38
4. Emerging Trends and implications 44
    4.1. Successes 44
    4.2. Failures and risks 46
    4.3. Strategy 49
    4.4. Role of donors 51
5. Conclusion 52
References 54
Appendix 1: Key Concepts in Biometrics 62
    Biometric basics 62
    Accuracy and Error Rates 64
    Industry Growth 66
Appendix 2: Referenced Cases 67

Abbreviations

4Ps	Pantawid Pamilyang Pilipino Program (Philippines)
AFIS	automated fingerprint identification system
AHR	advanced human recognition
ARV	antiretroviral
ATM	automatic teller machine
BEVS	Biometric Electronic Voting System (Philippines)
BIS	biometric information system (Yemen)
BISP	Benzir Income Support Program (Pakistan)
BOM	*Banco Oportunidade de Moçambique* (Opportunity Bank of Mozambique)
CCT	conditional cash transfer
CDC	Centers for Disease Control and Prevention (United States)
CLARCIEV	*Consejo Latinoamericano y del Caribe de Registro Civil, Identidad y Estadísticas Vitales* (Latin American and Caribbean Council for Civil Registration, Identity and Vital Statistics)
CNAMGS	*Caisse Nationale d'Assurance Maladie et de Garantie Sociale* (National Health Insurance and Social Welfare Fund, Gabon)
CNPSS	*Comisión Nacional de Protección Social en Salud* (National Commission of Social Protection in Health, Mexico)
DECT	Dowa Emergency Cash Transfer project (Malawi)
DGRCIC	*Dirección General de Registro Civil, Identificación y Cedulación* (General Directorate of Civil Registry, Identification, and ID Cards, Ecuador)
DRC	Democratic Republic of Congo
EBIRS	Employee Biometric Identification & Records System (Liberia)
EEG	electroencephalography (brain waves)
EHR	electronic health record
ELECT	Enhancing Legal & Electoral Capacity for Tomorrow (Afghanistan)
EU	European Union
HANIS	Home Affairs National Identification System (South Africa)
HDSS	health and demographic surveillance system
ICT	information and communication(s) technology
ID	identity document
IDB	Inter-American Development Bank
IDP	internally-displaced person
IFC	International Finance Corporation
ILO	International Labor Organization
J-PAL	Abdul Latif Jameel Poverty Action Lab
KYC	know your customer
MCC	Millennium Challenge Corporation
NADRA	National Database and Registration Authority (Pakistan)
NGO	non-governmental organization

OAS	Organization of American States
PDS	Public Distribution System (India)
PIN	personal identification number
POS	point of sale
PUICA	Universal Civil Identity Program in the Americas
RCT	randomized controlled trial
RENAPER	*Registro Nacional de las Personas* (National Registry of Persons, Argentina)
RENIEC	*Registro Nacional de Identificación y Estado Civil* (National Registry for Identification and Civil Status, Peru)
RSBY	*Rashtriya Swasthya Bima Yojna* (National Health Insurance Program, India)
SIBIOS	*Sistema de Identificación Biométrica para la Seguridad Pública* (Federal Biometric Identification System, Argentina)
SINOS	*Sistema Nominal en Salud* (Nominal Health System, Mexico)
SINTyS	*Sistema de Identificación Nacional Tributario y Social* (Argentina)
SIUBEN	*Sistema Único de Beneficiarios* (Unique Beneficiary System, Dominican Republic)
SSN	Social Security number (United States)
STRs	short tandem repeats
TB	tuberculosis
UID	Unique Identification number (India)
UIDAI	Unique Identification Authority of India
UNDP	United Nations Development Program
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
USAID	United States Agency for International Development

Figures and Graphs

Figure 1. Survey of the Use of Biometrics Technology for Development, Low-Middle Income Countries (2012) 2
Figure 2. Common identification model 6
Figure 3. Different Contexts and Uses of Biometric Technology 13

Graph 1. Sample of developmental biometric cases by region 20
Graph 2. Sample of developmental biometric cases by type and region 21
Graph 3. Estimated population covered in sample cases by region 22

1. Introduction

Rich and poor countries differ in many ways, including the provision of identity services to their citizens. Most wealthy nations have robust identification systems based on strong basic official documentation such as birth certificates.[1] These traditional, paper-based systems—though susceptible to fraud on an individual level--are sufficient for most purposes and can reasonably ensure uniqueness within a population. Citizens in rich countries can generally "prove" who they are to acceptable standards, whether for interactions with the state (voting, claiming social security payments, obtaining passports) or with non-state institutions (opening a bank account, buying a house).

Conversely, many people living in poor countries lack any official documentation (UNICEF, 2005). In a sense, these individuals do not formally exist, and are therefore excluded from the many points of engagement between a modern state and its citizens. They cannot open bank accounts or register property. There is no easy way to confirm that they have received the public transfers or services to which they are entitled. Traditional social structures may provide local recognition, but communal systems of identification break down with internal migration and urbanization. For many poor people, this "identity gap" severely limits opportunities for economic, social and political development.

Robust identification services are urgently needed to close this gap, but identity management systems have historically taken centuries to develop and mature in industrialized countries (Higgs, 2011). Biometric identification technology is a potential solution. In one sense, the approach is hardly new. Individuals have identified each other by their appearances or their actions since the dawn of humanity. Fingerprints were embossed on seals centuries ago, and employed more systematically by law enforcement agencies beginning in the 19th century, when they displaced complex systems based on multiple body measurements. These approaches were useful in law enforcement, but had serious limitations. They were labor-intensive, requiring expert analysts to spend hours measuring and comparing minute details. The precision of manual comparisons was hampered by human error and poor quality records. No expert could reliably recognize or verify a particular individual among a population of millions, let alone billions, and the data was not robust enough to ensure that each individual was uniquely identifiable.

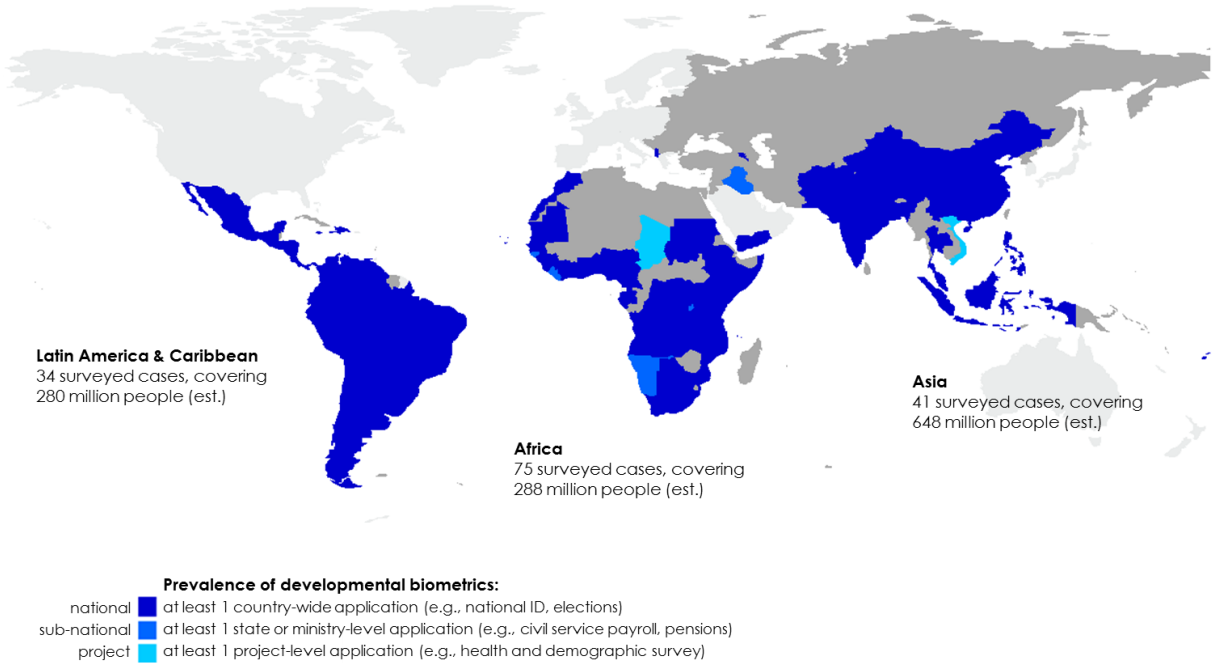
Yet recent advances in digital biometric identification—advanced human recognition (AHR)—have broken these barriers.[2] These technologies now offer the most accurate tool available for identification (who are you?) and authentication (are you who you claim to be?). The biometrics industry is booming, with an estimated annual growth rate of 28 percent for 2005-2010. At 34 percent, annual growth rates have been even higher in developing regions,

[1] Sometimes referred to as "breeder" documentation.

[2] For the purposes of this paper, "biometrics" will refer to digitized biometric data unless otherwise specified.

which are now major markets for the industry.[3] In India alone, the biometrics market is projected to grow by over 40 percent from 2010 to 2014 (TechNavio, 2012). Conservative estimations suggest that over 1 billion people in developing countries have had their biometrics taken for one or more purposes, and this number is growing (see Figure 1).

Figure 1. Survey of the Use of Biometrics Technology for Development, Low-Middle Income Countries (2012)



This rapid growth has been spurred by a variety of uses for the technology. Rich countries have long used biometrics for forensics and security but fewer have incorporated them into their national identity systems or used them to underpin public service delivery. In contrast, we have seen a proliferation of non-security applications in low- and middle-income countries, from civil registries to voter rolls, health records to social transfers, public payrolls to pension payments and beyond. This divergence in purpose partly reflects the different identification baselines in rich and poor countries—the identity gap.

Of course, identification and identity management are not synonymous with biometrics, which is simply one instrument among many for identifying and authenticating individuals. But the technology is worth examining because it represents a potential revolution for developing countries. At a basic level, biometrics can strengthen core identity systems like civil registries and national ID cards, which legitimize and facilitate developmental

[3] Africa, South America, the Middle East and India accounted for 31 percent of global sales in 2010, up from 25 percent in 2005. The most rapid growth (37 percent over 2005-2010) has been in Africa. See Appendix 1 for details.

interactions between states and formerly "invisible" citizens. Beyond these "foundational" applications, especially when combined with other advances in information and communications technology (ICT), it can also be leveraged for more "functional" purposes (voting, transfers or enabling financial access or health insurance markets) that further inclusion, facilitate access to rights and services, and strengthen public accountability. Rather like the explosion of mobile telephony in the face of limited fixed-line systems, it can be harnessed to leapfrog traditional systems.[4]

Despite the growing adoption of biometric technology by developing country governments, donors and non-governmental organizations (NGOs), little analytical work has been done to answer important questions comprehensively and from a developmental perspective:

- How does the question of identification relate to development? Should it be a focus for development policy and assistance?
- Where, how and why is biometric technology being used? Can poor countries really use biometrics to leapfrog rich ones in identity management, including for public service delivery?
- What is known of its impact on economic, political and institutional development? Is it cost effective? Where are the gains and potential pitfalls of general identification and biometric technology in particular? How can governments—and donors—develop strategies to use this technology effectively?

This paper explores these issues by synthesizing experiences from a survey of over 160 cases. Some are modest, covering beneficiaries of small projects, while others are national in scope, covering millions or hundreds of millions. Taken together, the applications exhibit some patterns, including two different supply-demand "pathways" toward national identification. In some cases, supply leads demand: governments create foundational identity systems with the intention to link them to social applications. In others, demand drives supply: multi-purpose national identification systems (mostly *de jure* but sometimes *de facto*) evolve out of functional applications that began with narrower scopes.

We draw some general conclusions regarding the expanding use of biometric identification in poor countries. New technology cannot do everything. In particular, it cannot directly substitute for the lack of essential documents like birth certificates which establish legal identity and citizenship.[5] As with any technology, the developmental impact of biometric identification depends largely on the political, technological, and legal context in which it is used. Some cases suggest large returns on biometric identification in economic and social programs, with potential gains in efficiency, governance, and inclusion. Yet there are also

---

[4] The mobile phones analogy suggests that the value of this technology is potentially greatest in the poorest countries, where need is high and other forms of identification are weak.

[5] As discussed below, very recent advances in DNA-based identification offer the new possibility of genuinely biometric birth certificates but these are not likely to be available on a large scale in the medium-term due to cost .

problematic cases where the technology has been costly but ineffective or, even worse, where more robust identification has increased the risk of exclusion. While more evaluation is needed, evidence to date suggests that—despite its theoretical advantages—using biometrics for periodic voter registration in very difficult environments may impose more costs than benefits.

These findings have implications for countries and for donors, who are involved in funding many of these applications and advising national governments on the adoption of biometric technology. One key conclusion is that identification services should become a standard element of development planning, including to deliver social services. Rather than funding one-off applications, donors should work to strengthen on-going identity management systems with multiple possible uses.

This survey remains a work in progress. Cases are evolving as rapidly as the technology. There are few rigorous evaluations of the merits of an identity-driven approach to development, and in particular the use of biometrics. More research is needed to assess and add to the impressions given in this paper.

Section 2 considers the relationship between identification and development, and how the lack of official documentation can inhibit the rights of poor people. It then gives an overview of advances in biometric technology that make it attractive to countries looking to rapidly close this identity gap, and some of the limits to technology. It concludes with a brief discussion of common concerns related to biometric identification, distinguishing them from those related to any other reasonably robust individual identifier. In Section 3, we summarize the findings of our survey on the evolving use of biometric technology in developing countries, discussing regional trends and applications in specific sectors. This section also includes a typology of some different supply-demand pathways that countries have taken, or plan to take, in developing their identity systems. Section 4 draws some implications from these cases that could inform future approaches to developmental identification. Section 5 offers some concluding thoughts.

2. Identification, development, and biometrics

"Identity" and "identification" are nebulous and subjective concepts. Each of us is a sum of our many personal and psychological traits, physical features, life experiences, circumstances and preferences. These identities play a key role in our societies. Many—including gender, poverty level, nationality, religion, etc.—are of central relevance for development. Identities are also increasingly represented in digital form, such as Facebook pages and databases maintained by large internet providers such as Google. These "digital identities", partly self-made and partly imposed on individuals without their explicit consent, raise some important issues and concerns. For the purposes of this paper, however, we will consider a narrower set of core attributes and characteristics—"official identity."

This section outlines the importance of official identification for development in light of the identity gap that exists in many poor countries. It then discusses the specific use of biometric technology for identification, including common concerns regarding exclusion, privacy and oversight.

2.1. Official Identity and the identity gap

Official identity includes those attributes (both static and mutable) that individuals can use to identify themselves when interacting with formal institutions like governments, employers and banks.[6] This often includes name, place and date of birth, sex, current address, nationality, familial relationships such as parents, spouses and children or other information needed to determine individuals' rights and responsibilities vis-à-vis these institutions.

Because names, birthdays and addresses are shared by many people, official identification normally necessitates unique identifiers—data points or characteristics that are unique to each individual.[7] This is often a number (such as a Social Security number or SSN), which is then associated with a persons' other official identity information and documentation. Biometrics identifiers are unique within a population and can be used to link identification numbers and other records.[8] Identification (or registration) is the process whereby an

---

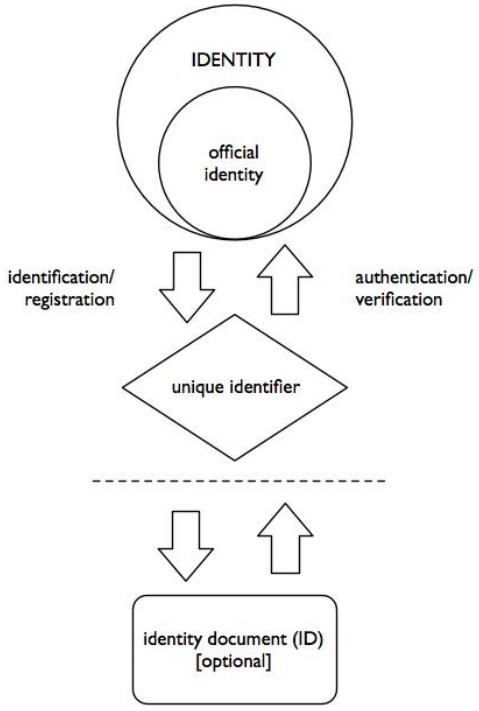
[6] The term "identity" probably derives from the Latin "identidem" meaning "over and over" or "the same." In this sense it is more appropriate to the relatively restricted concept used in this paper. Though often associated with national ID cards, official identity is a broader concept. US Social Security numbers and drivers' licenses, for example, are provided to both nationals and residents, including some who are not part of the Social Security system. India's unique identifier (see below) is also issued to all residents and authenticates against a database rather than a card.

[7] For example, the number of individuals named "John Smith" in the United States along is estimated at around 50,000, and around 5 million Americans are named "John" (see http://howmanyofme.com/). Worldwide, around 150 million people answer to some variant of the name "Muhammad."

[8] In practice, "unique" must be understood in a statistical or probabilistic sense as an extremely low probability that any two random individuals will be recorded as having the same identifier or that a single person will have more than one. The uniqueness of a biometric measurement within a given population depends on the

institution creates and/or records an individual's official identity. Often, though not always, this process includes issuing identity documents (IDs) or other tokens. Once an official identity exists and has been recorded, individuals can then authenticate or verify their identities using their unique identifiers or documents (see Figure 2 below for a common model of identification).

Figure 2. Common identification model



Birth registration, for example, is the process of officially recording a newborn's name, date of birth and parents in a database or other system (a type of *identification*). It normally generates a birth certificate (*ID*) which can then be used as proof of official identity to open a bank account, enroll in school, obtain a drivers' license, etc. (*verification* or *authentication*). A country's *identification system* normally consists of a series of databases (such as civil, voter and driver registries) along with any documents or tokens issued, such as ID cards or personal identification numbers (PINs).

Having an official identity and being able to verify it is such a mundane feature of life in rich countries that most citizens take it for granted—unless faced with an exceptional situation such as identity theft. In general, wealthy countries have well-functioning national register and identification systems that have developed and adapted over centuries. Official identity is established for nearly all citizens at birth, and a birth certificate then allows access to the

---

quality of data and precision of measurements but the uniqueness hurdle set by other identifiers is not very high (see above footnote).

rights and responsibilities that come with citizenship. Typically, over 98 percent of people in rich countries have birth certificates, meaning that the majority are "included" from an identification perspective (UNICEF Innocenti Research Centre, 2002).[9]

In contrast, many poor countries do not have robust identification regimes, ones that include almost all of the population and provide them with highly credible identification services. Modernization and internal migration have rendered traditional systems less useful, yet formal systems are weak. Some individuals have no recognized formal identification, or may carry a variety of often inconsistent documents such as affidavits, residence permits, and old voting or ration cards. Often, bribes are needed to acquire even these deficient IDs.

The foundation for other forms of official identification is usually a birth certificate; the only document that can ostensibly prove age, nationality and parentage. Yet, estimates of the rate of unregistered births in many parts of the world are sobering. According to a UNICEF analysis, in 2000 some 36 percent of children worldwide and 40 percent of children in the developing world were not registered at birth. South Asia had the highest percentage of unregistered births (63 percent), followed by Sub-Saharan Africa (55 percent) and Central and Eastern Europe (23 percent). Among the least-developed countries, under-registration was 71 percent (UNICEF, 2005; UNICEF Innocenti Research Centre). Even for those that are registered, birth certificates are often difficult to access due to poor record keeping, lack of mobility or corruption.[10]

Within countries, under-registration is also highly correlated with income distribution and the urban-rural divide. In the Dominican Republic, only 3 percent of the highest income quintile was unregistered at birth, compared with 40 percent of the lowest quintile (World Bank, 2007). Undocumented individuals in the Dominican Republic faced a host of problems, including being barred from post-primary education. Children of unregistered citizens were unable to be registered themselves, creating an intergenerational cycle of exclusion. Disenfranchisement caused by a lack of official documentation is often compounded by economic and political crises that force migration. The United Nations High Commissioner for Refugees (UNHCR) estimates that around 12 million people are affected by statelessness, many of whom lack formal identification (2012).

---

[9] Still, even established systems have to cope with substantial identity fraud. The US Federal Trade Commission estimates that some 10 million Americans have their identities stolen each year—though it does not distinguish between people who steal SSNs so they can work from those who seek to commit fraud. Most formally employed illegal immigrants—which, according to the Pew Hispanic Center account for 1 in every 20 US workers—are working under fraudulent social security numbers (Leland, 2006). A substantial proportion of compromised Social Security numbers belong to children.

[10] Ten years later, inadequate identification continues to pose myriad problems. In one high-profile (though perhaps not development-crucial) example, a Ugandan team bound for the 2011 Little League World Series (the first African team ever to qualify) was refused entry visas to the United States due to unreliable birth records. Fortunately, the Ugandan team that qualified for the 2012 Series has received their visas (Post, 2012).

At the same time, governments in poor countries are asked to carry out many functions that were not expected of more advanced governments until relatively recent times, including providing universal access to healthcare and education, implementing know your customer (KYC) rules for financial institutions, and administering a wide variety of transfer programs.[11] Each of these functions services requires state–citizen interactions that often rely on formal identification to ensure eligibility.

This "identity gap" has profound implications for development, particularly when viewed from a human rights perspective.[12] Development goals for a nation can be equally seen as development aspirations for its citizens; from there it is but a step towards enshrining aspirations as rights, although some doubt the practicality of this approach. Identification is basic to many of the rights set out in the UN Declaration on Human Rights and the Convention of the Rights of the Child. They include rights to: a name, an identity with family ties, nationality, recognition before the law, participation in electing government, take part in government, own property, and to equal access to public services as well as social security.[13] Many of these rights, which are also related to development goals, cannot be exercised on a national scale by individuals who lack basic national identity documentation. While official identification is of course not enough to ensure these rights—some countries cannot or will not deliver services even to citizens with IDs—it is often a prerequisite.[14]

2.2. The Technology revolution and its limits

Technological innovations have opened up new possibilities for creating, managing, and using identity systems. This includes biometrics, which can be defined as "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual"(Woodward, Orlans, & Higgins, 2003). In addition to the commonly-used fingerprints, face prints and iris scans, recent years have seen an increasing range of such features used for identification, including voice prints, retinal scans, vein patterns, tongue prints, lip movements, ear patterns, gait,

---

[11] For example, education for all only emerged as a policy goal in Europe after the start of the 18th century, though instruction had long been provided to some through church schools; see http://en.wikipedia.org/wiki/History_of_education.

[12] Human rights are closely linked with development and have been incorporated into mainstream development practice since the 1990s. The rights approach considers human rights both a development goal and an instrument for progress. An extensive review of the human rights approach to development is beyond the scope of this paper: for a good overview, see Alston and Robinson (2005), or Piron and O'Neil (2005).

[13] Notably, however, the rights to birth registration or a birth certificate are not among these.

[14] Individual identification should not always be a prerequisite for service delivery. In particular, it is counterproductive to link access to identification for services that generate large externalities—such as vaccinations—unless there are strong arguments against a degree of duplicate provision.

dynamic signature, DNA, brain waves (EEG) and even butt prints, with the latter two still at an experimental stage.[15]

Biometrics can be used for two identity-related purposes: 1) *identifying* an individual within a large population to determine if she is unique (one-to-many or 1:N matching), and 2) *authenticating* an individual against a record to determine if she is who she claims to be (one-to-one or 1:1 matching). These functions, combined with other digital technology, can enable individuals to authenticate themselves remotely against a database rather than require them to carry cards. They can improve accuracy and security, facilitate fast data processing and collection, and create auditable transaction records; all of which have the potential to prevent fraud, improve service delivery, and aid development planning. But do these new technologies to identify and authenticate individuals actually work? How accurate are they?

The first instance where biometric technology may face accuracy difficulties is a *failure to enroll*. Some individuals may have biometrics that are hard to capture, either due to faulty equipment or physical characteristics. The latter can include, for example, worn fingerprints for rural and manual workers, or unreadable prints for the very old. Cataract surgery can stymie iris recognition.

For those that can enroll, the technology can then match an individual's biometric against other stored data record. Comparing one template to another ("one-to-one" or 1:1 matching) allows for authentication (e.g., verifying a person against their ID card). Comparing one template to an entire database of enrolled records ("one-to-many" or 1:N matching) identifies whether or not that individual has already been enrolled (i.e., is she unique?). One-to-many matching can "de-duplicate" the enrolled population to produce, for example, a clean voter roll. Though biometrics may be statistically unique, errors can still occur during these comparisons. A "false negative" occurs when the system *does not identify* a match when it should (e.g., it fails to recognize a person that has already enrolled). A "false positive" occurs when the system *does identify* a match when it should not (e.g., it recognizes a person that has not yet enrolled).[16]

In large populations, the main difficulty is with 1:N comparisons: there must be enough data (that is, multiple, high quality measurements) to ensure that the probability of a false positive is very small. With insufficient points of comparison, large databases yield a high number of false matches that is too great to be resolved through other methods such as manual checking of demographic details. For example, using a single fingerprint to de-duplicate a voter roll of 1 million people would require a half a trillion comparisons between individuals. With an error rate of just 0.01 percent, 50 million of these comparisons will yield false

---

[15] For a useful short overview of biometrics, see Jain et al (2004); some essential information is also summarized in Appendix 1.

[16] Different applications dictate the importance of minimizing one type of effort over the other. It may be vital, for example, to exclude every unauthorized person into a nuclear facility but more important to include applicants for health services than to exclude them.

positive matches (50 per person), far too many to be useful. Frustratingly little information has historically been available on the performance of biometric identification in the field—unsurprising since the industry is dominated by large companies with proprietary systems. A lack of transparency allows these companies to hide behind the mystique of an "almost infallible" technology, rather than being forthcoming about its limitations.

The Unique Identification Authority of India (UIDAI), broke new ground in March 2012 when it released performance data on its processing of 84 million Unique Identification numbers (UIDs)—part of India's ambitious project to biometrically identify some 1.2 billion residents (UIDAI, 2012c). This has created a precedent for future data openness, and the information contained in the UIDAI report raises the bar for future biometric applications in a number of respects. Its standards-based model increases competition between technology suppliers, greatly lowering costs.[17] And, the UID approach towards data quality offers a central lesson for other countries.

The UID program is unusually demanding. It uses data provided by 10 finger scans and two iris scans, and also applies stringent quality controls at the point of registration (Zelazny, 2012). Combining (or "fusing") the 12 measurements resulted in a low biometric failure-to-enroll ratio of 0.14 percent, even in a population where many rural and manual workers are not able to provide high-quality fingerprints. The probability that a duplicate entry will not be caught (a false negative) was estimated at only 0.035 percent. The probability that an entry would be erroneously classified as a duplicate (a false positive) against the gallery of 84 million was estimated at 0.057 percent. Applying the UID system to a much smaller country like Haiti, with some 10 million people, suggests that comparable enrollment standards and procedures would result in only some 340 duplicate cases for further manual examination. For a large country like Nigeria, with about 100 million people, the number of erroneous duplicates would be 34,000, still quite manageable.[18] UID has also released two reports on authentication (UIDAI, 2012a, 2012b). These indicate that advances in technology enable the authentication of all but a very few individuals (or for individuals to authenticate themselves), provided that enough high-quality biometric data is taken. With sufficient high-quality data, individuals can therefore be uniquely identified with a high degree of precision, even in large populations.

---

[17] The price of iris scanners has fallen dramatically over the past few years, down from thousands of dollars to US$100 or less (Steiner, 2010). This reflects both mass production (including for UID itself) and a transition from military to normal civilian specifications.

[18] To yield the UID result, the corresponding probability of a false positive in a bilateral 1:1 comparison would have to be extremely small, approximately 6.8×10^{-12} or 7 in one trillion. Extrapolating the probability to a population of 1 billion for India would yield a total number of false positives of 3.4 million. UIDAI aims to reduce the number by applying tighter quality controls to minimize enrollment errors identified in the first stage of testing, and also by adjusting the match parameters to reduce the probability of a false positive by allowing a slight increase in the probability of a false negative. Since parameters can be adjusted to enable a tradeoff between false positive and false negative error rates, it is possible to reduce the number of false positives by accepting a somewhat higher probability of not picking up a genuine duplicate registration. The tradeoff is better with iris technology than with fingerprints. For more details on the UID performance results, see Gelb and Clark (2013).

Research into digital recognition, as well as the wide availability of information on the internet, is also forcing a more transparent and realistic look at the pros and cons of biometric identification technology. The widely held belief that irises remain unchanged after stabilization has been challenged by the finding that ageing results in small but perceptible changes to the iris that can degrade matching over time (Bowyer et al., 2009; Bowyer & Fenker, 2012). A recent experiment by Javier Galbally et al (2012) has called the security of irises into question by using a genetic algorithm to generate computer-produced, fake irises good enough to fool a scanner most of the time. Cracking "foolproof" high-tech ID cards has become something of a cult. The struggle between those seeking to increase the security of their technology—for instance by including "liveness" detection in fingerprint and iris readers—and those seeking to spoof it will only continue.

This dialectic should not undermine the use of biometric identification on a wide scale, including to de-duplicate large datasets—an area where it has some unique advantages—and support authentication for a high volume of relatively low-value transactions. At the same time, there is a growing trend for high-value and security authentication applications to use towards action-based or "hidden" biometrics such as voice and lip movement recognition, patterns of computer keyboard and mouse movements, infrared vein technology (widely used in Japan for ATMs), DNA and brain waves (EEGs). Many of these biometrics are not likely to be useful on a mass scale to underpin basic official identity systems. However, no system of official identification can itself cover all authentication needs. Once identified for the purposes of opening an account, a bank client may require additional identification for secure transactions which might not involve standard biometrics at all.[19] Whatever the technology, implementers must be aware of the limitations.

Among the new biometrics being developed, rapid DNA analysis deserves special mention from a development perspective. Because DNA is the only biometric that can be taken at birth and is stable over a lifetime, it offers the possibility that individuals can be definitively linked to the primary documentation of their existence—the birth certificate.[20] Recent breakthroughs have made this option more practical; sequencing a series of short tandem repeats (STRs) is now possible within about one hour. The biometric markers used by this technology reportedly convey little or none of the personal details encoded in DNA, and are therefore no more intrusive than any other physical attribute such as fingerprints. However, rapid DNA assessment is still costly and not yet deployable on a mass scale.

---

[19] Non-biometric approaches to authentication (photos, passwords, PINs) are often used for banking but are less secure and present greater opportunities for fraud. In a recent competition organized by the US Defense Advanced Research Projects Agency (DARPA) to crack 52,000 passwords, the winner had solved over 37,000 of them within 48 hours. It made little difference whether passwords were simple or complex (Guidorizzi, 2012).

[20] Newborns cannot provide good fingerprints; the iris is not stable until several months after birth and is also difficult to capture in very young children. Studies of identical twins show that DNA itself mutates very slightly over time, so that an individual of 60 is not precisely the same as she or he was at birth, but the changes do not appear substantial enough to have practical impact (Atick, 2012; Casselman, 2008).

Biometric technology is of course only one approach to bolstering official documentation. Identification programs do not require advanced technology either for enrollment or authentication. Countries with strong civil registries have managed—within limits—to ensure their integrity without relying on biometrics as the main identifier. Estonia's comprehensive identity system, for example, plays a fundamental role in linking to a variety of economic, social and political applications without biometrics.[21] Instead, it relies on a sound system of birth registration and the use of PINs (ePractice.eu, 2012). But Estonia is a small country, with good data on its highly literate and connected population. Poor countries appear to have fewer viable alternatives for creating robust identity management systems quickly and efficiently.

2.3. Perspectives and concerns

For many—refugees, potential voters or pensioners—some form of official documentation can be an essential step towards security, freedom, entitlement and inclusion. For others, identification raises concerns about government encroachment on citizen's rights and is associated with victimization, oppression and exclusion.[22] Biometric-enabled identification elicits similarly opposing viewpoints; some see it as a means to improve services, others associate it with an Orwellian dystopia. This divide is not surprising. Technology is neutral; it opens up new possibilities that can be used for good or for ill. The utility and morality of identity systems and technologies depend largely on context, perspective and need.

The identity gap between rich and poor countries also shapes the debate on identification and the specific role of biometric technology. In rich countries, biometric identification is mainly used in areas relating to security and policing. Applications of this type have mushroomed after the events of 9/11, and spurred the growth of the industry. Although a number of rich countries do have national IDs, some with biometric features, many attempts to create such biometric IDs have met with strong resistance.[23] In poor countries, biometrics is more commonly employed in developmental applications.

---

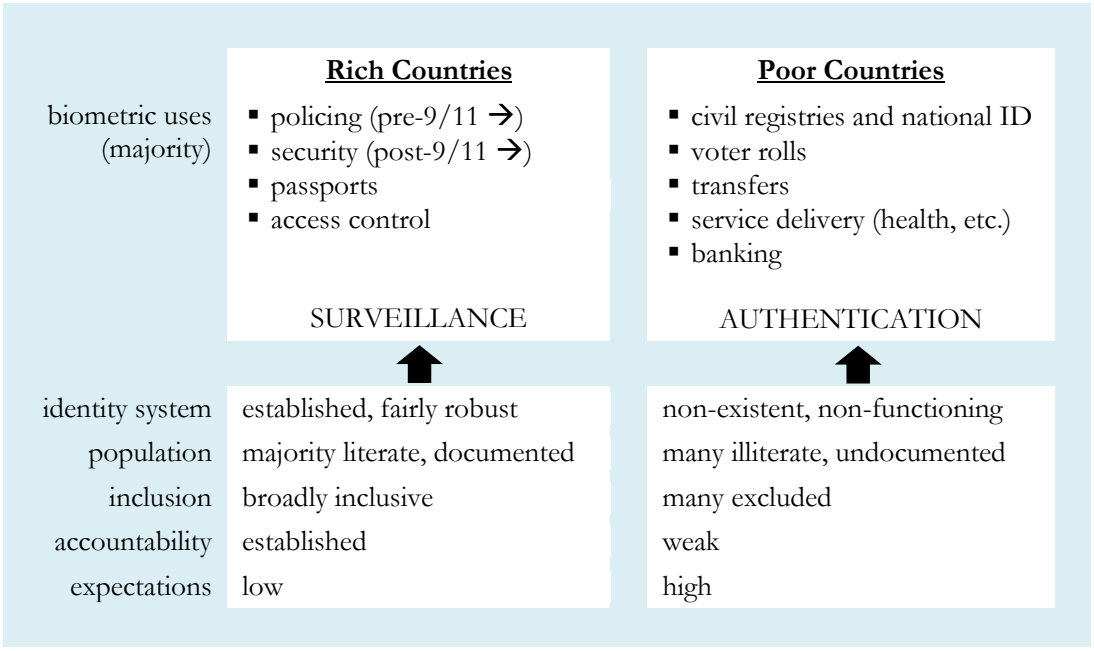
[21] Non-citizens, however, must provide 10 fingerprints, and Estonia now has a biometric passport that also requires fingerprints.

[22] Note, for example, a list of historical identity documents that—because they included group classifications such as "Tutsi"—played a role in ethnic violence and persecution: http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/samples/.

[23] In the US, even though the driver's license and SSN are accepted as *de facto* (though voluntarily held) identifiers, there is strong opposition to introducing a national card for the purpose of identification. While the SSN is not compulsory (and the Amish community has a specific exemption) it is becoming ever more difficult to conduct normal life in the US without one. There are purpose-driven substitutes, such as the taxpayer identification number. Most recently, the introduction of E-Verify and proposals for introducing a national employment verification card have confronted a range of objections (e.g. Froomkin & Weinberg, 2012). Costly national ID card proposals have also floundered under the weight of opposition in the UK and Australia.

This is not always a clear distinction. Some "developmental" identification programs in poorer countries have been influenced or driven by security concerns.[24] Conversely, some rich countries have used biometric identification for broader purposes. Despite strong objections to a national ID, for example, some US states use biometrics to authenticate welfare recipients. However, the overall picture is an emphasis on surveillance in richer countries and an emphasis on authentication or verification in poorer ones (Figure 3).

Figure 3. Different Contexts and Uses of Biometric Technology



The debate on biometrics is also shaped by other contextual differences between rich and poor contexts. In rich countries relatively well-established electoral and oversight processes are usually assumed to allow citizens to hold politicians and bureaucrats to account. A degree of bureaucratic discretion, or "government with a human face" is valued, on the assumption that citizen-state interactions are generally benign. In contrast, many poor countries have only weak mechanisms to enforce public accountability. Interactions with officials are seen

[24] Pakistan's national ID program, for example, was initially introduced for national security purposes but has also been used to underpin a range of social transfers and a new voter roll (see www.nadra.gov.pk). Another example is Argentina's *Sistema de Identificación Biométrica para la Seguridad Pública* (SIBIOS) database, launched in 2011 by the Ministry of Security. SIBIOS uses fingerprint and facial recognition to streamline identification across agencies such as the National Registry of Persons (RENAPER, issuer of national IDs), Federal Police, and Department of Immigration (E-Health Reporter, 2012). Many countries also have biometric passports and border control to comply with ICAO standards and demands from rich countries. Any program to provide unique identification has the potential to help integrate disparate databases as, for example, in India's controversial National Intelligence Grid (NATGRID) program (http://www.thehindu.com/news/national/article3529461.ece).

as exploitative, especially by the poor, and as opportunities for extortion and bribery.[25] Many of the human rights noted above are violated when resources intended for one person's use are diverted to well-connected others by mismanagement and corruption. In these conditions there can be a premium on automating citizen-state interactions to reduce discretion, including establishing a clear audit trail to document them. Especially if linked to functional applications, effective identification services can therefore be seen within the development process as strengthening rights by enabling individuals and formal institutions to interact more effectively.

It is therefore not surprising that much of the resistance to strengthening identification systems and adopting biometrics comes from rich countries; but there are also skeptics in the developing world. To critics, the efficiency gains of biometrics may be marginal compared to concerns regarding data protection and oversight. They argue that the collection of such data by governments will unnecessarily strengthen the power of the state relative to citizens, threaten personal privacy[26] and—by increasing the possibility of exclusion—marginalize the most vulnerable members of society.

There are certainly some particular concerns related to biometrics, as there are with any particular tool or technology. Yet many common fears relate to identification more generally and are *not specific* to biometric technology. Others are simple misconceptions. Disentangling these concerns is important for assessing which should be taken seriously—and which are distractors. We consider three issues: the risk of exclusion, threats to privacy, and cost-efficiency

Exclusion

A first concern is the risk of exclusion. As mentioned in Section 2.2, not everyone is able to provide biometrics, particularly fingerprints. Those who may have difficultly—infants, the elderly, and manual laborers—are often already marginalized within society. This is a limitation of the technology that can indeed lead to exclusion if counter-measures are not put in place. Taking multiple biometrics ("multimodal") can minimize this risk, but all programs need to allow for exceptional failures-to-enroll.

It is also essential to ensure effective means of redress when individuals are hurt by the failure of a system erroneously considered to be "almost infallible." If new systems (for

---

[25] In *Voices of the Poor* (1999, p. 8), Deepa Narayan writes that "Poor people report that their interactions with state representatives are marred by rudeness, humiliation, harassment, and stonewalling. The poor also report vast experience with corruption as they attempt to seek health care, educate their children, claim social assistance or relief assistance, get paid by employers, and seek protection from the police or justice from local authorities."

[26] Privacy concerns are not always consistent. For example, in April 2012 the Supreme Court of Maryland ruled that crime suspects enjoy, together with a presumption of innocence, an expectation of privacy (including from DNA swabs) that outweighed the government's interest in fighting crime. This is despite the fact that suspects are routinely fingerprinted, frisked, handcuffed and even strip-searched during arrest (Washington Post, 2012).

example, voter rolls) are implemented in a hurry, there may be insufficient time or resources to deal with these issues and otherwise eligible people may be overlooked or unable to enroll. By definition, robust identification systems have the virtue of producing fewer errors; but the stronger the system, the greater the presumption that the computer is right and the objecting individual is wrong. Still, errors in data capture are not unique to biometric identification. Regardless of the technology used, all registration and authentication processes must define clear processes and standards for resolving errors and identity disputes—an feature absent in many developing country systems.

Beyond the failure-to-enroll and errors, there is another area where biometric identification projects have risked exclusion. Weak identity systems breed under-documentation that excludes many people. At the same time, their flaws allow space for familial relationships and bureaucratic discretion to offer loopholes and informal identification (usually for a fee) to the undocumented. Formalizing identity can eliminate this grey area and lead to a stronger division between "insiders" and "outsiders," particularly when citizenship and its associated rights are at stake. Countries that have sought to increase the coverage of their national ID systems or social registries to undocumented nationals have been forced to develop substitutes for birth registration. These may rely on local records, such as baptismal records or affidavits from local officials. Without a policy to break the cycle of un-documentation, national identification programs may further marginalize undocumented people—or even increase statelessness (see Section 3 for the example of the Dominican Republic). The possibility of mass de-nationalization is a serious concern, especially when national demographic boundaries are fluid, as in many developing countries.[27] However, the risk of exclusion due to formalization is *not* a biometric-specific concern. Biometric technology may accelerate the development and robustness of identification system, but the same nationality problems can arise with a low-tech identity solution.

Privacy

A second concern is that biometrics violate individual privacy. There are a number of facets to this fear, including the need for data to be securely held and the question of whether or not taking a biometric image is inherently intrusive and an infringement on essential human rights. While such sentiments have been expressed by a few, the last issue is not considered further in this paper. It is not apparent why taking a fingerprint or iris scan with the full knowledge of the subject is inherently more intrusive than any other form of identification, including the commonly accepted standard of requiring photos, signatures or detailed personal information. There is also little evidence that the individuals identified biometrically in developing country applications fear or reject the technology (see Section 4).

Biometric technology does raise some special privacy issues. Digital photography poses a unique challenge as facial recognition is increasingly used for remote surveillance by

[27] Determining nationality is a messy business and has been an issue for many countries in the past century, such as the case of ethnic Germans in Alsace-Lorraine in 1918-20, and the more recent break-up of the Yugoslavia (e.g., in Slovenia: http://preventgenocide.org/europe/slovenia/).

governments and private companies (such as Facebook). Unlike fingerprint and iris scanners, facial recognition can be used without the knowledge of the subject. [28] This is particularly worrying in the context of political and civil liberties, where the ability of governments to identify protestors could hamper free expression (see Freishtat, 2012). Also, like other personal data, there is the question of low long biometric data should be retained, and concern that retention spans may far exceed the period of relevance for the particular application that motivated the data collection.[29]

A more complex privacy concern is the ability to link information from a number of databases using a common biometric identifier. This may increase efficiency, but may also facilitate government overstepping and infringe on the right to confidentiality. The questions of when linkage is appropriate, when it infringes on privacy, and when it should require explicit consent are beyond the scope of this paper—though the answers generally depend on context. Some linkage can be beneficial for development; connecting tax, real property and social service data can be a cost-effective way of reducing fraud and tax evasion. The *Sistema de Identificación Nacional Tributario y Social* (SINTyS) system in Argentina enabled individual records to be linked across 13 databases covering employment, pensions, electoral roll, social beneficiaries, the deceased, real estate registries, auto registries and poor households, along with 24 provincial civil registries—all using a unique identity number. The estimated Phase 1 benefits were US$104 million, mainly through reduced leakages in social spending and tax evasion, relative to an implementation cost of US$10 million (Pessino & Fenochietto, 2007). In other instances, such as voter records and benefits information, linking may be detrimental and infringe on rights. Each country will therefore need to develop appropriate data collection, protection, sharing and retention policies, including in response to questions of national security.[30]

Again, however, it is important to note that privacy concerns regarding linkage are *not* specific to biometrics—any identifier, such as a number like Argentina's, can be used to link records. Nor is a formal identity system necessary to underpin discriminatory or invasive programs. Ethnic discrimination and conflict have endured for centuries, often with no formal identification system at all. Politicians may not need to know who voted for whom; they can favor or disfavor electoral districts based on overall returns. However, regimes with

---

[28] Latent fingerprints, such as those left at a crime scene, can also be collected without the knowledge of the subject. However, they are far less reliable than digitally captured fingerprints (see Dror, Charlton, & Peron, 2006). There have also been recent developments in taking fingerprint scans at a distance (see Roop, 2012), but these are not yet available in the commercial market. In general, these issues are beyond the scope of this development-focused paper except to note, as above, the trend towards "hidden" biometrics for high-value authentication. The US Federal Trade Commission has offered guidelines on the use of face recognition but has not blocked the use of the technology: see http://www.ftc.gov/opa/2012/10/facialrecognition.shtm.

[29] For example, about one third of schools in the UK have used some form of biometric data to manage library borrowings and school meals (BBC, 2012). Will the students' fingerprint records be retained indefinitely, after they leave school?

[30] Some populations have particular sensitivities. Releasing data on the identity of refugees, for example, may expose family members to risk if still in the country of origin (Hosein, 2011).

a common identifier certainly make linkages easier, and facilitate connecting ever-larger volumes of personal information. This may increase incentives to extract such data and save it for periods that may be far longer than the timeframe of the need that originally justified its collection, or to use linked data for nefarious purposes. With any technology, countries must have stringent and transparent standards for data linking and sharing appropriate to their context.

Cost

A third and final concern is that biometric identification is too costly. In some cases the technology has indeed been expensive, especially when high-cost, proprietary packages are chosen instead of cheaper low-tech substitutes. Still, prices are falling, and the unit cost reported for some national ID schemes advocated for rich countries far exceeds the unit cost of those in poor countries, which have typically been around US$5 per head.[31] Where technology is costly, the cost may be passed on to citizens and impose barriers to access. If identification is a prerequisite to exercising citizen rights, including voting, the cost and inconvenience of obtaining acceptable identification should not become an exclusionary barrier.[32] However, biometric technology itself only accounts for a part of the cost of any system of registration and verification. One successful, high-tech registration will be far cheaper than doing it repeatedly, and non-biometric systems may also have expensive security features, such as ID cards with holograms, laser etching, etc., that are in fact more costly than a secure biometric enrollment process (Wade, 2012).

With all these issues, there is also the need to consider the counterfactual. Relative to alternatives, biometric identification can increase inclusion, privacy and efficiency. If documentation of certain details (e.g. nationality, address, etc.) is not needed, identifying people with biometrics can include the undocumented in a way other identifiers cannot. Biometric authentication combined with PINs or numbers conveys no significant personal information. In some cases, this can be preferable to more "human" processes, involving personal knowledge or intrusive questioning. In the absence of a functioning identification system, completing a biometric exercise to create one may be no more costly than a paper-based alternative, and may save greatly in the long run due to more automation and reduced fraud. Many critics of precise identification systems fail to consider these and other counterfactuals. Does biometric technology raise some concerns? Yes, but so do the

---

[31] Estimates of the unit cost of the UK's abortive ID card were reported as being between US$150 and US$600 per head (BBC, 2009). Opponents will naturally want to push for high estimates and supporters for low ones.

[32] This can be an issue in rich countries also, as shown by the controversy over requiring enhanced voter ID in the United States. Whatever the merits of this in principle, the context and timing of proposals left little doubt that they reflected partisan interests rather than a sincere desire that citizens be precisely identified. In addition, the experiences of biometric voter rolls discussed in this paper show that hasty identification schemes often turn out poorly. As the old saying going: "If you want it bad, you'll get it bad." For a summary of ongoing voter ID legislation in the US, see http://www.ncsl.org/legislatures-elections/elections/voter-id.aspx.

alternatives. Is "fuzzy ID" a viable substitute for individuals needing to authenticate themselves within the context of a modern state and economy? Probably not.[33]

[33] In some views, the privacy issues raised by biometrics (other than facial recognition) are less urgent than those raised by other ICTs, including cellular phones, RFID chips and the collection of commercial and personal data through internet and credit cards.

3. Survey of Biometric identification Applications

Biometric technology has underpinned a wide range of efforts to improve identification, democratic participation and service delivery in the developing world. This includes programs to expand financial access for the poor, improve payroll and pension management, reduce fraud and corruption in the civil service, create new voter rolls, provide health services and insurance, verify teacher attendance, and a range of cash and in-kind transfers. In total, we estimate that these projects have biometrically enrolled over one billion people[34] in low and middle-income countries. The landscape of these applications is constantly and rapidly changing. New initiatives are announced around the clock and a deep search into one case inevitably reveals others. Rather than an exhaustive account, this survey should therefore be viewed as a wide sample of existing applications.

We have relied on internet-based primary and secondary sources, project documentation, and interviews with country operators, donors, technical experts and other industry professionals. Nevertheless, information on many programs is often fragmented, and from government, implementer or vendor sources rather than independent assessments. To address this, we have worked to triangulate facts with multiple sources whenever possible. We hope that the publication of this paper will elicit new information and feedback about these applications.

Following a brief overview of the identified cases, this section outlines the particular contribution of biometrics across various sectors and concludes with a snapshot of various pathways that countries have taken in developing nation-wide identity systems.

3.1. Overview

In total, we identified over 230 relevant biometric identification cases spread across more than 80 developing countries.[35] Of these, we have been able to reasonably confirm and research some 160 cases in 73 countries.[36] These are applications where biometric technology has been used to identify a segment of the population for a purpose that could realistically be considered as "developmental." It thus does not include databases used

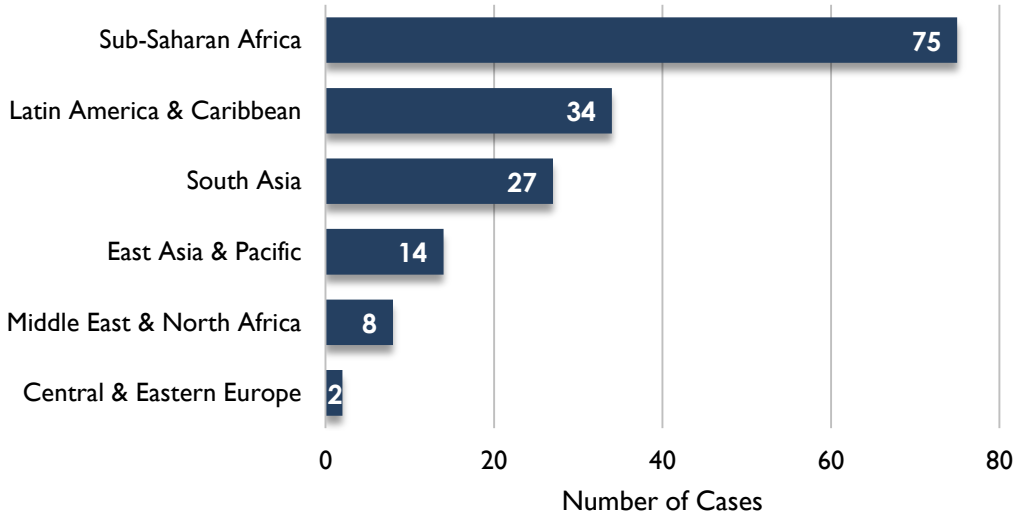
[34] Authors' calculation, based on 92 biometric identification cases (those for which we could obtain coverage data) as reported by official agencies, donors, and or vendors. Some coverage data may be exaggerated, and some individuals may be covered under multiple programs and thus are double-counted. Conversely many more people have likely registered their biometrics since these figures were reported, and the current numbers may thus be much higher. There are also certain cases that presumably have high levels of coverage but for which we have no data. To deal with these uncertainties, we have rounded the reported numbers to the nearest order of magnitude. Adding these rounded numbers yields a total estimate of 1.22 billion people.

[35] We have included only cases from low-to-upper middle income countries, as defined by the World Bank (see http://data.worldbank.org/about/country-classifications). At the time of writing, this includes countries whose GDP per capita is less than US$ 12,476.

[36] For the remainder of this paper, figures and analysis will be based only on those cases where we have reasonably reliably information.

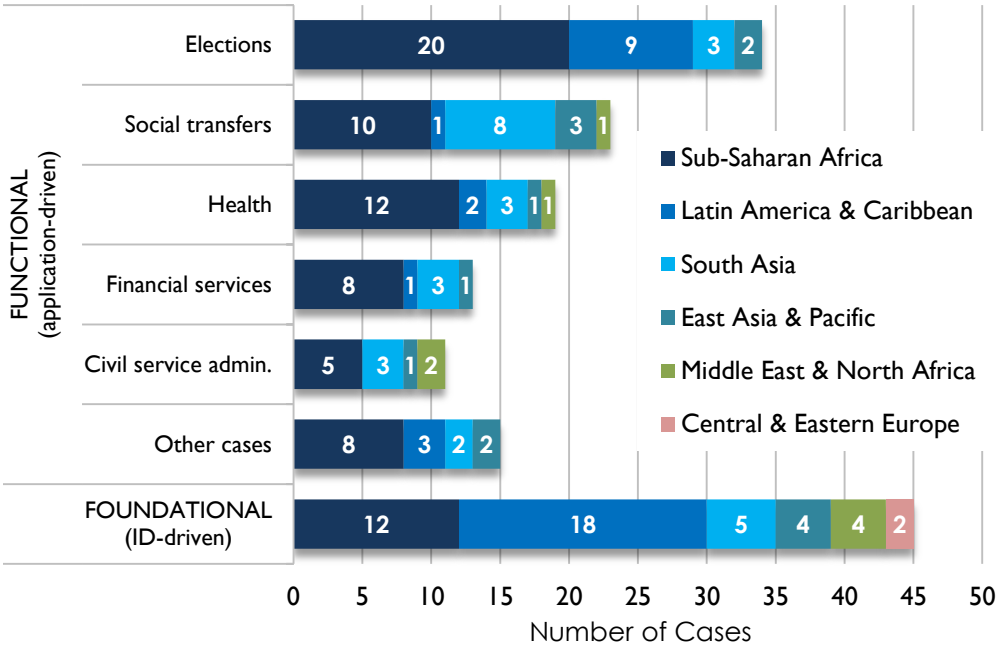
primarily for border control or law enforcement, nor does it include access control to public or private facilities. Graph 1 provides a breakdown of cases by region. Most are "active," in the sense that they are already operational and in use or actively enrolling. A number are also in the early processes of implementation (planning, pilot or procurement phases). To the best of our knowledge, only a few are "inactive" due to delays, cancellation, or project completion.

Graph 1. Sample of developmental biometric cases by region



Most interesting perhaps are the purpose for which countries, donors—at least half of these projects are funded with official development assistance—firms and NGOs have used biometric technology. Using a macro lens, we categorize these cases into two broad types of applications: "foundational" and "functional." The aim of "foundational" programs is to supply general identification for many official and personal uses, most commonly by establishing civil registries and national IDs. Conversely, "functional" identification is introduced in response to a demand for a particular service or transaction, such as voter IDs, health records, bank cards, etc. These two groups are blurred. Forms of identification may evolve from serving a particular purpose to being multi-purposed—sometimes *de jure*, sometimes *de facto*, and not always according to plan. What starts off as a functional application like a ration card may end up meeting the demand for identification in other areas. Nevertheless, we find it useful to loosely distinguish between foundational "ID-supply-driven" cases functional "application-demand-driven" cases. Using this typology, Graph 2 below shows a breakdown of cases by application type and region.

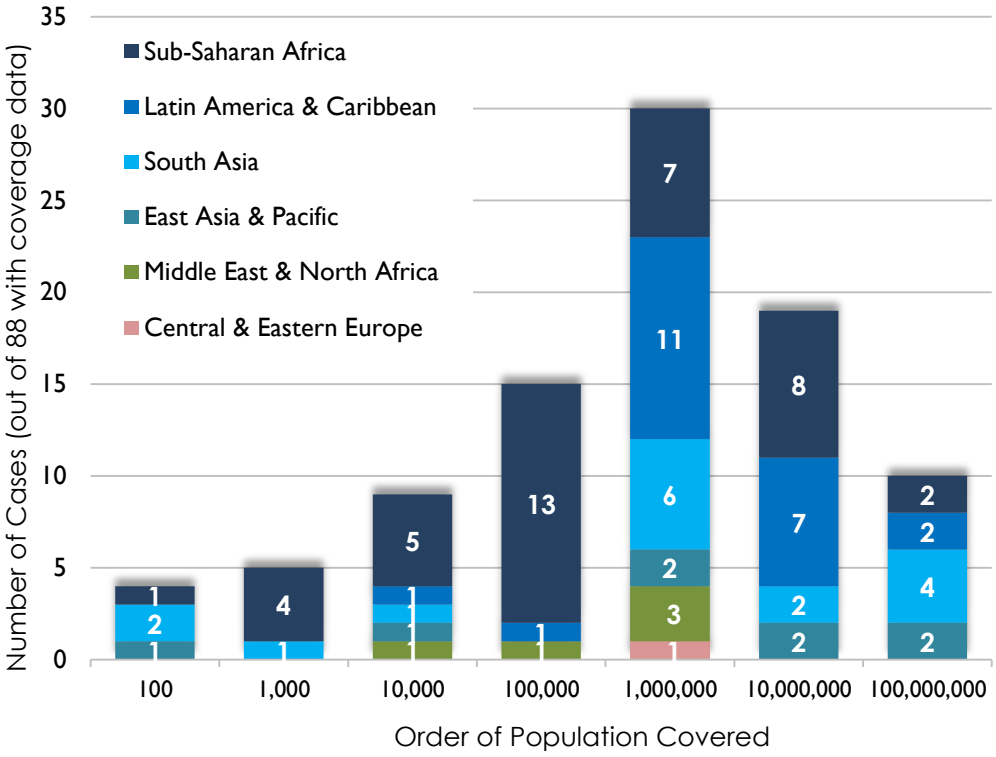
Graph 2. Sample of developmental biometric cases by type and region



At least 37 countries have multiple applications of developmental biometrics. In India, for example, the data include no fewer than 15 instances where a range of actors (central, state and municipal governments, donors, and NGOs) have already or plan to use biometric identification. Nigeria, Mexico, Malawi, Kenya and South Africa also each have five or more cases. In these countries, it is now commonplace for citizens to provide multiple biometrics to different government agencies and sometimes to private firms. As discussed further below, the chaotic proliferation of biometric programs raises many problems and risks.

Even though around half (75) of all sampled developmental biometric applications have taken place in Africa—with the remainder concentrated in Latin America and the Caribbean (34) and South Asia (27), the cases cover only an estimated 288 million Africans, compared with some 281 million people in Latin America and the Caribbean and 426 million South Asians (see Graph 3 below). Many African cases that use biometric technology to promote financial access or facilitate social transfers have tended to be modest in scope (see Graph 3 for a regional breakdown by sector). One field experiment in Malawi measured the impact of fingerprinting on increasing the repayment of rural loans; it covered less than 1,000 people (Giné, Goldberg, & Yang, 2010). The bulk of biometric coverage in Africa has come from voter registration projects (at least 20 to date) and a handful of national ID initiatives, yet many of these are incomplete and still in the enrollment phase.

Graph 3. Estimated population covered in sample cases by region



While a few Sub-Saharan African countries—e.g. Nigeria, Ghana, South Africa, Angola—have, or are planning, large scale projects to biometrically identify citizens as part of national ID or civil registry projects, biometric-enabled national identity systems are heavily concentrated in Latin America. This is perhaps not surprising, given the fact that many Latin American and Caribbean countries have civil registries that are over 100 years old, in part a legacy of records kept by Catholic Churches since the colonial period.[37] Many of these systems have included inked fingerprints on ID cards for decades. In the past decade, however, the region has seen a strong trend toward collecting digital biometrics (normally 10 fingerprints) as part of national campaigns to increase birth registration and improve personal identification.[38] These might be termed "first generation" cases, where new

[37] See, for example, the variety of records kept by the Catholic Church in Mexico from 1550 to 1935: https://www.familysearch.org/search/collection/show#uri=http://hr-search-api:8080/searchapi/search/collection/1410092

[38] One example is Ecuador's civil registry (*Dirección General de Registro Civil, Identificación y Cedulación*, or DGRCIC), whose forerunner included an inked fingerprint on the national ID card (*cédula unica*) beginning in the 1960s (INEC, 2009). In 2010, DGRCIC began collecting 10 digital fingerprints and issuing chip-based identity cards as one component of an IDB-funded project to modernize the civil registry and increase access to formal documentation and services. This was part of the 2009-2013 national development plan (*Plan Nacional de Desarrollo para el Buen Vivir*), and was preceded by a birth registration campaign (*"¡Al Ecuador ponle tu nombre!"* or "put your

biometrics have enhanced existing identity management systems, both to clean old databases and strengthen authentication. This is in contrast with newer "second generation" systems—like India's UID—that are built around biometrics from the ground up. There are also a number of cases in Latin America where biometrics have been incorporated into elections, but these activities are often linked with existing civil registries or national ID systems; stand-alone biometric voter registries are less common than in other parts of the world.

Like Latin America, most South Asian countries—including India, Pakistan, Bangladesh, Nepal and Afghanistan—either have, are implementing or are planning biometric-based national identification systems. Over 200 million people have already had their biometrics taken as part of India's UID project, and when the project finishes over 1 billion Indian residents will have been biometrically identified. South Asia is also home to many social transfer projects, such as the Benazir Income Support Program in Pakistan (BISP), or the Public Distribution System (PDS) in Andhra Pradesh, India. We have seen comparatively fewer cases in the Middle East, North Africa, East and Central Asia and Eastern Europe. However, there are some notable applications from these regions, including the MyKad card in Malaysia, a pension system and voter registration in the Philippines, banking and cash grants in Indonesia[39], health and civil administration projects in Yemen, and a newly announced national ID in Armenia, among others.

Applications can be difficult to organize; many in the social sector could fit in multiple categories. Should a health-related conditional cash transfer (CCT) be considered a "health" case or a "transfer" case? Still categorization is useful both for looking at macro trends and drawing common lessons. In the sections that follow, we have attempted to group cases based on their initial or primary function or motivation. Thus, a CCT that uses biometrics in distributing cash for reported clinic visits would be found in the social transfers section, since the primary use of biometrics is enabling a payment.

3.2. Functional Applications

Over half of our sample of developmental applications of biometric technology can be classified as "functional," in that they were originally or primarily intended to supply identification and/or authentication services for a specific developmental purpose. This includes financial and banking services intended to expand coverage and access to unbanked groups, social cash and in-kind transfers, civil service administration and reform, health interventions, and electoral management, among other sectors. In this section, we briefly summarize how biometrics are used in each of these functional groups, providing case examples and general trends.

---

name to Ecuador!") supported by UNICEF and Plan International. IDB project documents and more information are available at http://www.iadb.org/en/projects/project,1303.html?id=EC-L1083.

[39] Indonesia is also rolling out a new biometric national ID card (e-KTP) that will have a unique citizen identity number similar to UID. See http://www.e-ktp.com/ (in Indonesian) for details.

Financial services

The 13 cases of biometric identification in the financial sector are only a subset of the growing number of similar applications in developing countries. Relatively simple fingerprint technology has been used for at least 20 years as a means of authentication for commercial transactions, sometimes substituting for other methods (PINs, signatures) and sometimes supplementing them. Recently, more precise, digital biometric technology has paved the way for multi-purpose authentication, in some cases combined with mobile devises to create "biometric money"—secure, cashless transactions.

Fingerprint authentication cases include PRODEM (Bolivia), Azteca (Mexico), Banco Oportunidade de Moçambique (BOM, Mozambique), Siddhartha and Everest Banks (Nepal) and the First Bank of Nigeria, among others. Often, accounts are linked to smartcards that can be used for transactions at biometric-enabled ATMs or POS terminals, in addition to traditional brick and mortar banks. Some applications have been market-driven, others supported by non-profit foundations with the goal of extending financial access to poorer, less literate and often rural clients, while also reducing transactions costs and increasing security. Few studies include comprehensive data on the costs and benefits of the technology, but it appears that increased client bases and lower costs are possible. PRODEM operators claim to have recovered the costs of their biometric system in about a year (Hernandez & Mugica, 2003). While there are reports of occasional frustrations with using smartcards, there is no evidence of customers rejecting the technology. Even though smartcards enable offline transactions and reduce communications costs—ATMs do not need to be online all the time[40]—some minimum level of connectivity is needed to enable data reconciliation several times a day. This has been a problem in some cases such as rural Bolivia. Biometric authentication appears not to be widely used for cell-phone banking.[41]

Ghana's E-Zwich technology marks an evolution towards the use of biometrics beyond authentication towards identification and e-Money (Breckenridge, 2010).[42] Banks are required to record all 10 fingerprints of their clients, which are stored in a centralized, automated fingerprint identification system (AFIS) capable of de-duplicating all account-holders. Accounts are also identified by the national ID number of their holder. Public payrolls must be paid into an ID-linked account, and the Bank of Ghana strongly encourages

---

[40] Estimates made for PRODEM suggested a savings in communications costs of about US$800,000 per year, but this would likely decrease as telecommunications costs fall (Hernandez & Mugica, 2003).

[41] This is probably because of the difficulties of reliably taking high-quality readings for simple biometrics (fingerprints) in the cell-phone environment where devices are often not clean. New and more complex biometrics, such as experimental voice and lip-movement recognition are now being tested for mobile applications. Some cases do merge biometric and mobile phone technologies; for example, authentication against a smartcard can be used by an operator to authenticate the user for a phone-based transaction. In Japan, the largest biometric banking service network in the world relies on infrared vain recognition (Hitachi) in ATMs, but this technology does not seem to have diffused to developing countries.

[42] Notably, this E-Zwich was launched in the same time period that Ghana was rolling out a biometric-based national ID card. The card project, though still active, has been fraught with problems. Had its uptake been quicker, Ghana may not have needed the E-Zwich (Breckenridge, 2010).

larger private employers to do the same rather than paying in cash. One year after the launch of E-Zwich, over 300,000 people had smartcards linked to the system. The banking system then becomes an important mechanism to automate and control the state's payroll, with the capacity to identify ghost workers and expired pensioners. It forms the core of what could potentially become an extensive variation on an identity system—one driven by payments and finance that focuses primary on public and formal sectors. While there are no comprehensive studies of the costs and benefits of E-Zwich, illustrative calculations suggest that the savings, in terms of managing payroll, could be substantial.[43]

Beyond authentication, biometrics have also been used to establish secure identities in order to fulfill KYC requirements for opening bank accounts. For example, the UID Aadhaar number was accepted by the Reserve Bank of India as valid identification for small accounts in January 2011 and for all accounts in September 2012. It is now also accepted as a proof of address for banking purposes (Adajania, 2012).

Social transfers

Biometric technology has been used in a wide variety of social transfers: resettlement and demobilization payments, drought and flood relief, pensions, disability and unemployment compensation, social and universal income grants and public works. We have identified some 23 cases, many of which are described in Gelb and Decker (2011). In most cases, biometrics have been used in creating beneficiary registries and authenticating cash or in-kind transfers at the point of service. Future applications may include using biometrics to verify compliance with transfer conditions (such as school attendance and hospital visits), however we are unaware of any cases where this has been successfully executed to date.

Biometrics, mainly fingerprints and iris, have been used to identify beneficiaries in several ways. At a minimum, they can be used only for payments, without registration. For some resettlement grants in Afghanistan/Pakistan, the goal was simply been to prevent "round-tripping" (i.e., returning to the border crossing again to collect multiple cash grants). No longer-term database was established by the program; applicants were simply de-duplicated against the iris-prints of previous grantees (UNHCR, 2007). More commonly, however, biometric data has been taken to both register and de-duplicate beneficiaries and sometimes used in conjunction with smartcards to authenticate recipients at the point of service delivery.

---

[43] Net-1, the supplier of the biometrics and switching technology, was paid US$20 million upfront and on a commission basis of US$3 per card. This does not, of course, include all of the costs of implementing the program, but with a hypothetical number of 7 million accounts (for a population of 22 million) the payment would have come to US$41 million. In 2009, Ghana's public sector wage bill was one of the highest in Africa relative to GDP, at 11.3 percent or US$1.67 billion (World Bank, 2011). Annual savings of only 1 percent from the elimination of ghost workers—far less than the savings made in other cases which used biometric identification to trim bloated payrolls (Gelb & Decker, 2011)—would mean a payback period of three months for the E-Zwich system.

Some applications have been able to draw on existing national registers. Pakistan's Watan smartcard program, for example, provided reconstruction grants to families severely affected by flooding based on the National Database and Registration Authority (NADRA) database. An assessment of Phase 1 of the program by Hunt et al. (2011) concluded that the payment mechanism was a success. Over 1.5 million families had received the grant. Leakage was minimal and recipients were easily able to withdraw their benefits with a travel cost equivalent to only 1.4 percent of the grant amount. Most recipients also expressed a desire to transform their Watan card account into a permanent bank account. The assessment found that, due to the special registration effort made by NADRA, few people were excluded due to non-possession of a national ID card. Still, it also found that a substantial number of potentially eligible beneficiaries were excluded for a variety of other reasons, including failure to update relevant demographic and social data such as head-of-household status in the NADRA database. The review also noted the slowness of the grievance-resolution process. Still, the Watan example offers a lesson on the utility of a strong biometric national registration system for managing major transfer programs, particularly considering the potential loss of paper documents in natural disasters. However, the database must be continuously updated if it is used for emergency transfers.

Identification alone may not include the details needed for program targeting, such as income or assets. However, it can link an individual to information held in another database, such as Pakistan's National Economic and Social Registry (for details, see BISP, 2011) and ensure that registered individuals are unique. The system of civil registration is also central to databases used in many Latin American countries to administer social grants.[44]

Other applications have needed to conduct registration from scratch. Malawi's Dowa Emergency Cash Transfer (DECT) program provided drought relief to rural farming families and took fingerprints for both initial registration and verification for payments. The system appears to have worked smoothly and been welcomed by recipients, and the program was extended for a period to accommodate the desire of many to own regular bank accounts. Yet due to the small size and limited scope of the program, the use of biometrics was not considered cost-effective (Pearson & Kilfoil, 2007). A review by Devereux (2007), however, noted that one of the objectives was to help develop longer-term social protection programming and that biometrics would probably be cost-effective in that context: this was not likely to be the last drought in Malawi.

---

[44] For example, civil registry numbers are not required to enroll in the Dominican Republic's unique beneficiary system (SIUBEN, used to manage access to the system of social protection), but are needed to be eligible for benefits. These include electronic debit cards to cover food purchases, and health benefits. Registration facilities include several mobile registry offices. The ID card (*cédula*) is also a voter registration card. The registration process included a role for NGOs, to monitor the issue of IDs and assist enrollees to gather the necessary background information to register (World Bank, 2007). South Africa is also introducing a new social security card, to cover a range of transfers (see www.services.gov.za/services/content/Home/ServicesForPeople/Socialbenefits/Grantpaymentsystem/en_ZA)

In many of these cases, biometric technology has been combined with electronic payments mechanisms. Some programs have used "pull" payment systems, with recipients paid at a special facility at a particular time. Others have used "push" approaches, providing them the flexibility to access their grants at a wide range of point-of-service facilities, merchants, and financial institutions. Especially in cases where the recipient population is highly dispersed, the overhead cost of providing payment points, including through dedicated mobile ATMs, can be high. This has spurred a trend towards pull-type mechanisms, for example, in the delivery of social grants in South Africa. Originally disbursed through off-line card-based systems and mobile biometric ATMs, grants are increasingly channeled through recipients' bank accounts.

If the potential push service network is very sparse and cash-short, special pull arrangements may still be needed. In the Democratic Republic of Congo (DRC), for example, a program to deliver demobilization grants to ex-combatants initially relied on a push approach, but was later forced to shift towards mobile ATMs because there was so little cash in parts of the rural economy. As noted above, biometric authentication appears not yet to have been widely integrated into cell-phone-based transfer systems but it can still underpin program registration (for more details, see Gelb & Decker, 2011).

An additional application that has been suggested for biometrics has been to verify conditionality, such as school attendance and health clinic visits, in the case of CCT programs. However, there appear to be few applications where biometric authentication is currently used in these programs.[45] One exception is a randomized controlled trial (RCT) run by the Abdul Latif Jameel Poverty Action Lab (J-PAL) in Morocco that tested the effectiveness of fingerprint authentication in monitor children's school attendance.[46]

Civil service reform

A small but growing number of developing country governments have applied biometric technology in the management of public sector employees over the past decade. The principal motivation in these cases has generally been to reduce fraud and save money, although improvements in these areas hopefully also have benefits for service quality and coverage. These cases can be divided into two clear groups based on how they use biometrics: culling payrolls and monitoring attendance.

In the first group, we have found at least seven cases where countries have implemented large-scale projects to biometrically enroll civil servants in order to de-duplicate personnel

---

[45] Biometric compliance monitoring was proposed in the submission of the Philippines' *Pantawid Pamilyang Pilipino Program* (4Ps) to the Millennium Challenge Corporation (MCC) for funding support (MCC, 2009), but to our knowledge has not yet been implemented. See also an example from Mexico in the health applications section below.

[46] At the time of publication, the J-PAL evaluation results were not yet available. See www.povertyactionlab.org/evaluation/conditional-cash-transfers-education-morocco.

files and weed out so-called "ghost workers" and "double-dippers."[47] This can have positive effects both for fighting corruption and reducing the public wage bill. Nigeria's Integrated Personnel and Payroll Information System, for example, claims to have saved N12 billion in the first phase alone, and had eliminated over 43,000 ghost workers as of July 2011 (Gabriel, 2011). More recently, 17,000 fraudulent workers were eliminated from the Power Holding Company of Nigeria payroll alone (Okafor, 2012). Guinea-Bissau carried out a biometric census of civil servants in 2009 that reportedly cut 4,000 workers from the public wage bill (IMF, 2011).

This category of projects has potential not only to improve public management, but also as a gateway for other developmental applications. If a country is successful in establishing a clean, secure civil service payroll, this same system can be expanded to include pension payments and other social grants. Liberia has implemented a system similar to Nigeria's — called Employee Biometric Identification & Records System (EBIRS)—which has thus far reduced payroll by 10-15 percent. This project, which began with core ministries, has been gradually rolled-out to other public sector workers over time. Liberian government has reportedly considered expanding the system into a national ID project that will cover all citizens (Muhula, 2011). An advantage of this path toward national ID is that early applications can generate savings to help fund the expansion of the system.

Nearly all of these cases involve substantial donor support. At least three in various states of completion—including the projects in Liberia and Nigeria—have received assistance from the World Bank as part of larger civil service modernization programs. Not all have been successful. Beginning in 2000, the World Bank began funding a civil service modernization project in Yemen that included a biometric information system (BIS), among other components. The project experienced extensive delays—not surprising given the country's political and security climate—and as of 2010, around 170,000 state employees (mostly military and security services) had not yet been enrolled. Though the project successfully captured data for over 97 percent of civil sector and judiciary worker—at a cost of US$23.4 million for the BIS alone—only 3,792 double dippers had been removed from the database out of an estimated 60,000. The current status of the project and its future are uncertain (World Bank, 2010b).

A second group of cases aimed at reducing public corruption and poor service focuses not on identification, but on workplace authentication. Particularly in the last few years, as the price of biometric equipment has come down, some local and state governments have begun monitoring employee attendance with fingerprint readers. The technology has been particularly popular in India, where a diverse group of states and cities is using biometrics to reduce teacher absenteeism and to avoid paying municipal workers who fail to show up for

[47] Employees that do not exist (and someone else collects their wages) or are receiving multiple salaries, respectively. Another option is Ghana's previously-mentioned E-Zwich system, which can clean the payroll through the banking system (rather than personnel management system) by ensuring that each account holder receives only one payment.

work. This has the potential to decrease payroll fraud, although not all cases have so far been successful (for an example, see Botekar, 2012). Unlike payroll de-duplication—which has an indirect impact on service improvement through reduced leakage—attendance monitoring would ideally have a direct impact by ensuring that civil servants are at least present at their posts. [48]

Health

Biometric identification has become a cornerstone of many health programs in developing countries.[49] Our survey identified 19 such cases, many of which are small-scale projects often run by NGOs that serve between 100 and 10,000. There are also a handful of large-scale programs run both by governments and insurance companies. Nearly all have received financial or technical support from donors such as the World Bank, the International Finance Corporation (IFC), US Agency for International Development (USAID), and the Bill and Melinda Gates Foundation, among others. In health, biometrics are primarily used to verify insurance coverage or benefits, maintain electronic health records (EHRs), and link data and records.

Around half of the cases use biometrics to authenticate program eligibility including for insurance coverage, most using fingerprints in combination with a smartcard. Gabon (through the CNAMGS) and India (through *Rashtriya Swasthya Bima Yojna* or RSBY) are implementing national health insurance plans that include authenticating beneficiaries with fingerprints and smartcards at the point of service (Mbeng Mendou, 2012; Palacios, Das, & Sun, 2011; World Bank, 2010a). Smaller programs—such as the HOPE project to provide basic care to poor mothers and children in Cross River State, Nigeria—also use biometric smartcards, as have certain private insurance providers like Uganda's Microcare.[50] Chile's I-Med insurance company, for example, allows patients to pay their copays electronically using a fingerprint at the doctor's office. (Cross River State, 2010; Southbridge S.A., 2012; United Nations, 2008).

In these applications, fingerprints allow individuals to securely authenticate themselves and ensure that benefits cannot be stolen, sold or shared with unauthorized individuals. By limiting fraud, insurers can save money and provide better services to actual clients.

---

[48] Programs to monitor attendance must be introduced with sensitivity. Unlike payroll de-duplication, which is clearly directed against fraud, their more personal nature can be interpreted as a lack of trust between management and workers. In West Bengal, for example, the introduction of biometric monitoring of health personnel is first used with the highest-grade employees—administrative heads and medical officers—before being extended to lower grade positions (TNN, 2012). Attendance monitoring is not a strictly biometrics issue (requiring punch cards could seem equally punitive to employees), but the technology leaves little room for discretion. As another example, the Filipino parliament is reported to have adopted a Biometric Electronic Voting System (BEVS) for its plenary session to improve administrative efficiency and encourage lawmakers to attend proceedings and participate in votes (Diaz, 2011).

[49] For a broader discussion of ICTs in healthcare, see Lewis et al (2012).

[50] Microcare was bought out in 2009. Its successor, International Hospital Kampala, announced plans to begin issuing biometric smartcards to patients and clinicians in early 2012, see Talemwa (2012) .

Biometrics are less frequently used to ensure the uniqueness of individuals at enrollment; multiple enrollments are often a less pressing concern in health programs compared with inclusion and authentication. In RSBY, for example, fingerprint records are used only to authenticate identity at the point of service, but are not de-duplicated to ensure that each individual can only receive one card (Palacios, et al., 2011). [51]

Biometrics are also incorporated into systems for storing patient data, tracking hospital visits, etc. This includes most of the large-scale health insurance schemes provided by governments such as RSBY. Some smaller projects also use biometric verification to record patient data; for example a 2009 study used fingerprint authentication to monitor how often sex workers visited certain women's health clinics in Bangalore (Paik et al., 2010; Palacios, et al., 2011). In Vietnam, fingerprints were used to identify participants in a cholera vaccine trial (SonLa Study Group, 2007). Generally, EHRs can improve administrative efficiency, data collection, and the quality of care. Linking fingerprints to EHRs can further eliminate the need to carry identification, reduce errors in record-keeping, and decrease processing time, among other benefits. Additionally, biometrics can provide anonymity for patients; identifying someone via their fingerprint reduces the need for them to confirm personal details. Requiring health care providers to authenticate their transactions (prescriptions, treatments, etc.) can also help reduce fraud and improve accountability to both clinics and patients.

Within the group of cases that use biometrics for EHRs, there is a particular sub-set worth mentioning: those that use the technology to track specific courses of treatment. Here, the motivation for EHRs and biometric authentication is specifically to enable the collection and rapid analysis of real-time data that allows quick responses to patient needs. For example, Operation ASHA runs a tuberculosis (TB) treatment program in South Delhi using fingerprints to track adherence to treatment regimes.[52] Patient visits are logged using fingerprint scanners attached to a netbook, and sent to a central server at the end of each day via SMS; clinicians receive a text if any patients have missed their appointment and are able to follow-up within 48 hours to ensure they stay on course (Paik, et al., 2010). ASHA employees also received a monthly bonus for limiting the number of patients who default; biometrics made this easier to track. Fingerprint-enabled patient logs have also been used to track adherence to antiretroviral (ARV) treatment in South Africa and Malawi, by VaxTrac to record vaccinations in Benin, and by researchers to monitor participants in a cholera vaccine trial in Vietnam. The use of biometrics in such programs appears to have improved treatment and program administration (DELIVER, 2007; Paik, et al., 2010; VaxTrac, 2010).

A final group of programs uses fingerprints to link medical records or visit logs with other data. In Kenya, South Africa and Ghana, for example, various health and demographic surveillance system (HDSS) areas have attempted to use fingerprints to link survey records

---

[51] Strong incentives for multiple enrollments could cause a market-based service system to fail unless there is also de-duplication. Transitioning the base for RSBY to UID would address this issue.

[52] This was initially part of the same experiment that monitored sex workers in Bangalore, one of the few that evaluated the effectiveness of the biometric technology itself (Paik, et al., 2010).

with records of clinic visits. As Serwaa-Bonsu et al (2010) describe, the ability to link these records would allow for a deeper understanding of a health trends and behavior by providing both a "numerator" (clinic visits) and a "denominator" for the public health equation (HDSS survey data). Without a unique identifier (like an ID number or a fingerprint), records are sometimes linked based on probabilities of shared demographic data (names, gender, address, age, etc.). Evidence from the Africa Centre surveillance site in South Africa indicates that biometric linking, while not perfect, has the ability to outperform probabilistic linking.[53] In Chad, researchers used fingerprints to collect demographic and health information of migratory populations without having to rely on identity documents (Weibel et al., 2008).

In a somewhat different example, The Mexican National Commission of Social Protection in Health (CNPSS) is currently enrolling *Seguro Popular* (the national health plan) beneficiaries in a new biometric database called *Sistema Nominal en Salud* (SINOS). In addition to serving as the basis for EHRs and providing data for better preventative care, the CNPSS plans to eventually link SINOS via fingerprint to *Oportunidades* (Mexico's CCT program) in order to verify that beneficiaries are complying with health care requirements (Government of Aguascalientes, 2011; Government of Mexico, 2010).

Elections

Some of the largest biometrics applications in the developing world have been in elections. At least 34 low-to-middle income countries[54] have incorporated, or are planning to use, biometric technology into their electoral processes. We estimate that nearly 400 million people have had their biometrics captured as a part of one of these exercises. In all cases, the primary motivation for using biometrics has been to limit fraud. At the registration stage, the goal has been to ensure that individuals can only register once, through de-duplication. On Election Day, biometric authentication at polling stations can be used to authenticate voters.

Implementing biometric-based voter rolls has been supported by donors seeking to aid democratic consolidation, and urged by opposition parties or civil society advocates that allege corruption, mismanagement, or voter exclusion. In some circles, biometric registers are considered to be the gold standard in election management. As expected, these are large projects implemented by national governments frequently with substantial donor assistance, particularly from the United Nations Development Program (UNDP), the European Union (EU), the Organization of American States (OAS) and the Inter-American Development Bank (IDB). A few countries have also issued biometric voter ID cards as part of their registration exercises; this can have positive developmental effects beyond the election,

---

[53] The benefits seem to have involved saving time as well as (sometimes) improving accuracy. The KEMTRI/CDC HDSS in Kenya found that the success rate of using fingerprints collected during a survey to "re-identify" individuals when they attended a clinic was about the same as matching records based on demographics (68 percent), but that biometrics were much more efficient in producing the matching (Serwaa-Bonsu, et al., 2010; Were et al., 2011).

[54] See Appendix 2 for a full list of examples, we will discuss only a few here for the sake of brevity.

particularly in countries with no formal national ID. In Benin and the DRC, for example, cards issued as part of biometric registration were the first official IDs for many individuals, which they were able to use for wider purposes (Evrensel, 2010; UNDP, 2011).[55]

Biometric authentication is less common at polling stations in developing countries (and also in rich ones). This is partly a resource issue. Large-scale registration exercises that are carried out on a rolling basis can be accomplished with a relatively low equipment/citizen ratio—in Angola, for example, 2,030 agents staffing 164 stations enrolled 8.4 million voters in approximately 12 months (Angola Press Association, 2011). Elections themselves, however, entail a mass, simultaneous mobilization of staff and citizens within a short time period, and would thus require a widespread distribution of technology and connectivity. Additionally, there are cheaper, low- tech ways to prevent multiple voting. Checking photos and cards against voter lists and using indelible ink to mark voters may be good enough in many scenarios. Both Bolivia and Bangladesh, for example, used voter lists with the photos captured during registration to identify voters on Election Day (IFES, 2008; The Carter Center, 2009).

However, there are a few notable cases of biometric voter authentication. The Brazilian and Colombian government have each gradually distributed fingerprint readers to a limited number of polling stations, with the eventual goal of 100 per cent coverage. This iterative rollout helps to cope with cost and allows for adaptation and integration with other systems, avoiding many of the pitfalls seen with hasty voter registration exercises. Venezuela—which has used biometrics in elections since 2004—broke new ground in October 2012 by using biometric voter authentication with electronic voting for the first time (Mayhew, 2012). Still, the voter authentication is resource-intensive: Brazil had to deploy over 200,000 biometric readers to polling stations to cover some 7.5 million people, a fraction of its population (de Sainte Croix, 2010; RNEC, 2011).

The ability of biometric technology to ensure uniqueness and detect duplicates seems inherently suited to elections. They are high-stake events, where instances of fraud and exclusion—or ever the perception of them—can have immediate consequences for democratic outcomes, stability and governability. The 2009 Bolivian voter roll, for example, was widely seen as a national unity cause and conferred legitimacy on the elections (The Carter Center, 2009). Using a fingerprint or other biometric seems an ideal way to authenticate each voter's identity (is this woman who she claims to be, or is she stealing another person's vote?), eligibility (is she registered in the district?) and uniqueness (has she already voted?). Nevertheless, the cases surveyed indicate that exercises often do not use biometric technology to its potential, resulting in voter rolls that are no more accurate (and

[55] Fiji has also begun a biometric voter registration project that will issue ID cards. This will be the country's first national-scale ID, and the government has already declared that it will constitute valid ID for most official transactions (Tokalau, 2012). Mexico's voting card has also served as perhaps the most widely-used ID card in the country.

sometimes worse) than traditional lists. In some instances, costly biometric registration initiatives have been cosmetic rather than functional.[56]

The reasons for failure often involve logistics,[57] time constraints and the use of sub-standard technology. Unlike most social transfers or health insurance, elections involve full population coverage and strict schedules. Although electoral support is popular among donors, it often comes in waves close to important elections, with little lead time or resources for long-range planning. As a result, many countries start registration (biometric or otherwise) less than a year, or even a few months, before an election. This allows little time for training or adaptation, a particular problem for new, highly technical biometric systems that are seen as "black boxes," a potential weakness relative to the potential credibility of open human processes that are monitored by all political parties. Hasty procurement can also mean that countries get locked in to proprietary systems with unfavorable features.

Afghanistan, for example planned a high-tech, iris-enabled voter registration project for its 2009 elections with the support of UNDP. The "ELECT" program was eventually scaled back; iris scans were dropped in favor of taking inked fingerprints and manually scanning them to later de-duplicate with AFIS. Numerous technical and logistical problems delayed processing, and de-duplication could not be completed before the election despite widespread reports of underage, double, and fake registrations (ACE Electoral Knowledge Network, 2008; UNDP, 2009).

Somaliland also used a biometric voter roll in its presidential election held on 26 June 2010. The exercise was run in conjunction with a "citizenship confirmation" process that was intended to create a civil registry and national ID system in addition to issuing voter cards. In the end, the register contained some 1.2 million records and was used for a relatively successful election. However, up to 30 percent of these records are estimated to be duplicates, and the registration process was fraught with numerous technical and political challenges. Ultimately, the roll and current biometric system have been deemed un-usable for future elections, and the status of the national ID project is unclear (Mathieson & Wager, 2010).

Although the Bolivian case was considered successful in political terms and was certainly inclusive – the electoral roll was increased from 3 million to 5 million through the enrolment

---

[56] There may be something to be said for the signaling power of even cosmetic biometric registration. Even if rolls are not de-duplicated in time for the election, the knowledge or belief that they could be might reduce fraud. The deployment of technology on a large scale—3,000 mobile and fixed stations in Bolivia for example, can also signal the importance of the election and help to mobilize voters. These arguments seem hardly enough, however, to justify the cost. Moreover, technology can also be a negative if invoked to convey a veneer of legitimacy to a badly flawed process.

[57] In Bangladesh, for example, election workers canvassed peoples' homes directly to distribute and complete paper voter registration form, rather than completing them at an official center. This likely led to many more multiple registrations, most of which would have been caught by de-duplication, but needlessly burdened the process (IRI, 2009).

of numerous undocumented citizens, often from indigenous communities — a short registration timeline (six weeks) and an understaffed electoral administration meant there was little capacity to correct or reconcile records, or to deal with logistical and inclusion issues that arose (The Carter Center, 2009). As in some other relatively successful exercises such as Bangladesh, only local de-duplication was possible because of limitations of connectivity.

Even if biometric voter rolls are well-executed and even fully de-duplicated, they are often one-off, fiscally unsustainable activities. Of the 30-some registration exercises we are aware of, only a handful (e.g. Bangladesh and Benin) have led to permanent voter registries. Yet most come with a hefty price tag. Voter registration projects cost US$102 million (US$21 per person) in Afghanistan, US$580 million (nearly US$9 per person) in Nigeria, and $75 million ($15 per person) in Bolivia. The benefits of periodic biometric voter registration may not always be worth the cost. Chile offers a different model, where a permanent, biometric civil registry is used to generate the electoral roll.[58]

Other functional cases

Biometric technology is popping up in a number of other sectors related to development. For migration, UNHCR incorporates fingerprints into its "proGres" system to identify and track refugees in countries like Burundi, Ethiopia, Kenya, Malaysia, Tanzania and Thailand (UNHCR, 2008). UNHCR assisted NADRA in registering around 3 million Afghans refugees living in Pakistan. These individuals had their fingerprints and photos taken and de-duplicated in order to receive a proof of registration card, ensuring legal recognition (UNHCR & Pakistan, 2007).

Biometric applications have been less common in education than in other social sectors, though they are beginning to be used for monitoring teacher and student attendance (as described in previous sections on civil service reform and social transfers). Nigeria is also using fingerprints to certify identity for standardized test takers. Other public services have also relied on biometrics in recent years. Ethiopia—with assistance from the World Bank—has implemented a project to create a secure tax identification number, later linked to student loan repayment, credit bureaus and other systems (Tesfaye, 2009).

Cases that emphasize security and fraud reduction are less developmental but still worth mentioning. Nigeria, for example, has mandated biometric registration of SIM cards for mobile phone users in order to cut down on illicit activities. Over 78 million SIMs have been registered at a cost of US$39 million (N6.1 billion) (JACITAD, 2012). [59] India and the

---

[58] In 2012, Chile changed from voluntary to automatic voter registration based on the civil registry's list of voting-aged adults. This increased its electorate from 8.1 million to 13.4 million (out of a total population of 17 million), but caused problems when people who had disappeared under the Pinochet regime (but had not officially been recognized as dead) resurfaced on the roll. And with voting no longer mandatory, many also stayed home (Associated Press, 2012; Long, 2012).

[59] The exercise has not been without problems; see Malakata (2012).

Philippines[60] plan to issue biometric ID cards to fisherman and seamen, respectively, in order to protect their rights and prevent fraud (ROP, 2012; The Hindu, 2012). Also in India, the New Delhi government is registering taxicab drivers, while the Pune bar association is registering lawyers, both to deter scams by non-professionals (Jadhav, 2011). Biometric drivers' licenses have been linked to vehicle registration in El Salvador, and there are similar projects in Mexico and Bangladesh (Azad, 2011; Gemalto, 2010).

3.3. Foundational Applications

Over 40 developing countries use (or have begun employing) biometrics for "foundational" applications; identity services created for the purpose of providing general or multi-purposed identification. This includes national identity systems and "core" or "breeder" identification that proves a persons' identity and existence, and that enables her to obtain other IDs (Harbitz & Molina, 2010). Over the past decade, increased recognition of the role of formal identification has focused some attention and funding on under-documentation. Many countries have thus sought to build or overhaul their national identity regimes from the top down in order to ensure that all citizens (and in some cases, all residents) have an official form of documentation that can be used to verify their unique identity. [61]

In many cases, this involves biometric registration. These efforts often include providing a national ID card or other unique identifier (like India's Aadhaar number), building civil registries and issuing birth certificates. While a detailed description of each of these 40-plus cases is beyond the scope of this paper, there is less variation in implementation than among the functional applications and it is therefore possible to discuss general trends.

Latin America has advanced furthest along this path. Nearly all Central and South American countries have incorporated biometrics into national population databases of one kind or another, as have a number of Caribbean countries. As mentioned above, many of these countries have long histories of collecting fingerprint data as part of their civil registries and national IDs. In these first generation applications, biometrics were used mainly used for authentication. In recent years, however, there has been a growing trend toward collecting multiple fingerprints with sufficient data for de-duplication (Mexico and El Salvador are examples). Regional organizations, including the OAS, support civil identity programs, and

---

[60] The Filipino case is in compliance with the International Labor Organization (ILO) Seafarers' Identity Documents Convention of 2003, which required biometric identification of all seafarers to improve security and ensure the uniform implementation of workers' rights. According to the ILO, biometrics were the preferred form of identification among the seafarers themselves (for details see http://www.ilo.org/global/about-the-ilo/press-and-media-centre/news/WCMS_005139/lang--fr/index.htm).

[61] In their 2007 survey, Bennett and Lyon note 68 low and middle-income countries with national ID cards. Of these, 29 included a biometric, normally a single fingerprint; 12 were in Latin America. The picture has changed from then, with more countries having or developing biometric national IDs.

registries cooperate to share best practice.[62] Many Latin American systems have successfully consolidated, and enjoy some level of citizen confidence. In a 2007 IDB survey, for example, Peruvians expressed more faith in the national civil registry and identification authority (*Registro Nacional de Identificación y Estado Civil*, or RENIEC) than in the Catholic Church (Harbitz & Boekle-Giuffrida, 2009).

The second cluster of national-level identity programs is in Africa. This includes national ID projects in Ghana, Nigeria, Rwanda, and South Africa, to name a few. Most are recent endeavors, and many are still in the implementation stage. These second generation systems have included biometrics since inception with the purpose of establishing uniqueness. An exception is South Africa, which has a long history of biometric identification63 and a number of national-scale identity projects, such as the Home Affairs National Identification System (HANIS) (which went digital in 1998) and the Social Security Agency (SASSA) pension and cash transfer system (digitized in 1990) (Breckenridge, 2005).

A number of newer initiatives—often in countries without pre-existing population registries—have combined national civil registration and voter registration exercises. Rwanda, for example, simultaneously conducted a general census, a civil registration exercise, and a voter registration drive in 2007. Over 9.2 million people had their biometrics collected for the civil registry, which is used to periodically update the permanent electoral roll, and there are now plays to use the ID card for banking services (Evrensel, 2010; Gahamanyi, 2012).

Many other foundational identification cases in Africa have been less successful. Projects have stalled or run into serious implementation problems, sometimes because of highly irregular technology procurement. Uganda, for example, began a national ID project in 2010 that has been fraught with scandal[64] and, though 51 million Euros have already been paid to the supplier, cards have yet to be issued. Ghana began a registration drive for its National Identification System (NIS) in 2008, but stalled in 2009 due to budgetary and leadership issues. As of 2010, only an approximate 5 million people (out of a projected 24 million) had been enrolled (Breckenridge, 2010). Delays in national identification have often also compromised other systems.

---

[62] The Organization of American States (OAS), for example, started its Universal Civil Identity Program in the Americas (PUICA) in 2007. PUICA, along with UNICEF, IDB and Plan International, have made birth registration a priority in Latin America and the Caribbean. A region-wide pledge by governments to universalize registration by 2015 was renewed in 2011 with the motto "*regístrame, hazme visible*" ("register me, make me visible"). The region even boasts an international civil registry organization (*Consejo Latinoamericano y del Caribe de Registro Civil, Identidad y Estadísticas Vitales*, or CLARCIEV) intended to share best practices and information. See http://www.oas.org/en/spa/depm/puica.asp and http://www.clarciev.com/ for more.

[63] South Africa has collected fingerprints for over 80 years. Notably, millions of paper records were collected under apartheid for racial segregation purposes (Breckenridge, 2005).

[64] In 2012, several former ministers were accused of violating procurement laws (Mubiri, 2012). Reports also cite stolen and damaged equipment. As of July 2012, only 400 ID cards had been produced in the two years since the signing of the contract (Tash Lumu & Kakaire, 2012).

One common factor in many of these delays (in addition to procurement problems) is that governments are often trying to implement multiple, large-scale identification projects simultaneously (often all biometric). In the absence of robust identification, the incentive to create full national ID systems is strong. However, these projects are labor and cost intensive and can take many years to complete. Functional applications (like voter registration, pension payments, etc.) may require identification more urgently, and thus multiple systems develop. This has been the case in Nigeria, Ghana and Uganda, for example, each of which have attempted to complete multiple large-scale projects in the span of 2-3 years.

A third group of identity-driven projects is in Asia. These cases are fewer in number but diverse in terms of their architecture and implementation. As already mentioned, India and Pakistan have taken two different approaches to their identity systems (discussed further in the following section). Indonesia and Thailand have also adopted biometric national ID cards, and Bangladesh is in the process of attempting to convert its biometric voter roll into a general purpose identity system (as is Nepal). Malaysia's MyKad card is also unique; it serves as a national ID, but its smart chip has the (largely untapped) potential to store up to 256 additional services and applications, such as drivers licenses, bank accounts, health insurance information, etc. [65]

The institutional arrangements for the programs vary across country. One model, followed by countries, like Pakistan and Peru, is to implement the program through a specialized and autonomous "technical" agency, such as NADRA or RENIEC. At least part of the funding for these agencies comes from charging for ID-related services, though initial basic documentation is provided free of charge. In other cases, depending on history, the provision of national identification may be the responsibility of the Ministry of the Interior, or a body reporting to the Ministry of Justice, or an Election Commission.

These arrangements can have implications for the incentives to promote universal registration. Some agencies will be more stringent than others with verifying the credentials of applicants, including (where relevant) citizenship claims. Election Commissions, for example, tend to take a more conservative approach than social ministries, which consider their programs to have a substantial public good component. To reduce the prospect of inter-agency competition, it can be useful to empower a coalition of government bodies when an identity system is extended. The Dominican Republic, for example, created a "social cabinet" to oversee the expansion of its national registration system to poor,

[65] Which also includes the MyKid (children 0-12), MyPR (permanent resident), MyTentera (military), and MyPolis (police) cards. For more information, see www.jpn.com.my/docs/MyKad.htm.

unregistered citizens, though the Central Electoral Council played a lead implementing role.[66] Mexico has a similar body with representative from the different government stakeholders.[67]

Especially for countries with low birth certificate coverage, the criteria for registration and nationality can be contentious, especially as different options often have political or social significance through the groups they include or exclude. With the goal of social inclusion, a program in 2006 in the Dominican Republic aimed to register 400,000 poor citizens to include them in the social safety system which provided benefits of about US$30 per month, including through smartcard linked bank accounts. To deal with undocumented citizens, it instituted a "birth amnesty" for eligible children 16 and under," granting them exemptions from the normal requirements (World Bank, 2007). At the same time, however, the government began the retrospective application of a 2004 law on nationality that severely curtailed the previously liberal interpretation of the right to citizenship embodied in the constitution. This has had the effect of stripping *de facto* citizenship rights from many residents of Haitian extraction. While it was suggested that these could use their new documentation to apply for Haitian nationality, many of those affected were not eligible for Haitian citizenship because their parents had been born outside the country. These unfortunate individuals are now stateless, and the Dominican Republic is accused of violating the right to nationality embodied in the Convention on Human Rights (OSI & CEJIL, 2012).[68]

Building on birth registration campaigns may be a cost and time-effective way of building a national identity system, but there is the limitation that fingerprints are not easily collected from young children. Thus — at least until DNA-enabled birth registration becomes common — a truly robust biometric-enabled registration system must have multiple points of contact with individuals throughout their life; at birth in order to endure official (non-biometric) documentation, followed by updates to enroll adolescents.

3.4. Pathways to a National Identity System

Issuing national ID cards is perhaps the most obvious approach towards establishing a robust national identity regime with wide coverage, but identity systems can evolve in different ways. They can start with "demand" for specific functional applications and then possibly expand to cover other functions or even grow into foundational identification.

---

[66] The Social Council is headed by the Vice President and includes representatives from Education, Health, Labor, Sports, Women, Youth, Culture and Higher Education (World Bank 2007).

[67] In the Mexican case, it appears that the slow-moving progress of their national ID roll out is partly due to the unwieldy nature of this 60-member body (Brodersohn, 2012).

[68] There has also been concern in Mauritania that formalizing nationality will lead to exclusion for some groups (see http://www.opensocietyfoundations.org/voices/fear-and-statelessness-mauritania).

Other countries begin by supplying general-purpose identification and then moving toward various functional applications. There is precedent for both pathways from rich countries. [69]

The cases described above offer several examples of countries on the "demand-led" path. One example is Ghana's E-zwich system, which now performs some of the functions of a unique ID system for those on the public payroll and some in the formal sector. The same system could be extended to social transfers and grants, provided that all payments were made into E-Zwich-linked bank accounts. Many other examples of a function-to-foundation identity system come from the electoral sector. Some of these extensions have been an afterthought. Voter cards issued in the DRC's 2005 biometric registration exercise have become the country's *de facto* national ID. The cards covered around 90% of eligible voters and, in the absence of better identification are now used for myriad official transactions (Evrensel, 2010). Others have been intentional. In Bangladesh, the government is in the process of transitioning data captured during voter registration into a national ID (though this has not been a smooth process). If the project is completed, Fiji's new voter card will be considered acceptable identification for myriad official transactions (Tokalau, 2012).

Other examples come from the public administration sector. Ethiopia's unique tax ID number has already been scaled to link with multiple systems (e.g., credit reporting) and has the potential to scale to a national ID system. Liberia's EBIRS may also follow this path if the government does decide to expand enrollment to more sectors or to the population at large. Although none of the cases involved scaling up from social sector-related identification, the example of the US SSN shows that it is possible for a social program ID to assume wider identification functions.

The "demand-led" approach can be attractive, particularly for lower-income countries. Starting with civil service registration or a cash transfer program requires fewer resources up front than constructing (or re-constructing) an entire civil registry and birth documentation system. A smaller program can build on early success and increase scope and scale incrementally, with a more adaptive, iterative rollout process. It can offer quick returns to both government and affected citizens to maintain momentum. Program uptake will be faster when benefits are specific and tangible. To a citizen who lacks the identification necessary to receive a health subsidy, a health benefits card may be a more urgent priority than a national ID not associated with any specific gain. If phased appropriately, the program ought to be able to cover much or all of its costs from early savings.

---

[69] As one example, the scope and scale of the US SSN has expanded over time. Originally introduced in 1935 to track workers' incomes and benefits, it has gradually become the default (but not *de jure*) national identifier and is required for most official and many private transactions. Much of this expansion has been to reduce fraud. The 1986 Tax Reform Act required parents to report the SSN of children over five when claiming them as dependents (and getting a tax deduction)—effectively expanding its coverage to children. As a result, there were seven million fewer dependent claims in 1987, suggesting that these children were being claimed as dependents by non-custodial parents or were fictional (Liebman, 2000). See also http://www.ssa.gov/history/.

Pathway 1: Function to Foundation

Advantages	Disadvantages
▪ Potentially fewer overhead costs	▪ Fewer economies of scale and scope
▪ Adaptive learning	▪ Costly additional field visits to increase coverage
▪ Early cost savings and development returns	▪ Possible incompatible technology overlapping with other systems; integration requires long-term planning
▪ Incentives for citizen take-up	▪ Bureaucratic infighting, potential exclusion

Nevertheless, there are some pitfalls to application-driven identification. Overhead and personnel costs may be initially lower but efficiency is sacrificed and it will be harder to achieve economies of scale. The feasibility of building on an existing identity system also depends heavily on the quality, quantity and scope of data collected. Capturing only a thumbprint may be sufficient for a small transfer program, but will be insufficient for ensuring uniqueness in large populations. In Bangladesh, the data collected during voter registration was of mixed quality and coverage, making their transition to a national ID difficult (IRI, 2009). A patchwork approach to identification can also create an inefficient, overlapping network of incompatible systems that become increasingly chaotic, requiring citizens to register for identification many times over: Nigeria, India and South Africa offer examples. Some costly exercises, such as Bolivia's 2009 voter roll, which cost $15 per head, were never built into more permanent identity systems despite plans to do so.

Another problem with scaling functional identification is that different agencies may require different types of data, and have different standards for inclusion. An election commission (EC), for example, may place a high priority on ensuring its integrity; whereas a social ministry may prefer a more inclusive registry. Basing a national ID on a functional application that covers only a portion of the population also risks exclusion. The DRC voter card was issued only to those over 18, and ahead of elections. Those who were under 18 at election time have to wait some years before receiving a card (EC, UNDP, & International IDEA, 2010). Many of these difficulties can be avoided by employing long-term identity management systems, rather than developing a system card by card. However, a broader view is difficult when identification is viewed simply as a cost of delivering a particular service.

A second pathway is to focus on delivering foundational identification first. Especially in Latin America—but also in some other countries such as Malaysia and Pakistan—identification has followed the "top-down" approach, prioritizing the development of supply-driven national identification systems that can be used as a foundation for more

specific applications. In Latin America, Peru, Ecuador and most other countries have implemented birth and civil registration campaigns with the goal of reducing social and economic exclusion.[70] In this view, a national ID card is a basic necessity and gateway to rights and services. In 2008 Ecuadorian Constitution, for example, explicitly recognizes the right to a registered identity (article 66, number 28).

Most of these programs link the provisional of formal identification to national status. India's UID program is unusual in separating out the identity component from consideration of national status or eligibility for any particular program or service. It is designed to integrate and standardize identification for a range of disparate programs, most of which have been in operation for many years. This linkage, between identification and service delivery, is usually a staged process. In Pakistan, the NADRA database has served as a foundation for multiple transfer programs, including BISP, the Watan Card, and payments for internally-displaced persons (IDPs).[71] The National Socio Economic Registry's data sharing protocol sets out arrangements for sharing relevant sections of NADRA's data registry with other social programs (both government and NGO-managed). This database, like that of the *Sistema Único de Beneficiarios* (SIUBEN) in the Dominican Republic, includes more information than would normally be in collected for a national ID card because of the additional information needed for social services and transfers (for example, household asset data suitable for a proxy means test). As of 2012, NADRA is also in charge of preparing Pakistan's voter list in cooperation with the election commission (Ghauri, 2012). [72]

A different foundation-to-function option is to adopt national ID cards that serve as "one-stop-shops." In addition to satisfying identification requirements for a diverse range of government and private sector transactions, such cards also process and store transactions (e.g., an ID card which also holds a driver's license, links to a bank account, holds a transit pass, etc.). A small handful of countries—including Mauritius—have made plans for such multi-purposed ID cards, but few have come to fruition. The best active example is Malaysia's MyKad smartcard (see previous section).

The identity-driven path also has benefits and pitfalls. A robust national identifier or registry is an integral part of a modern state. It can serve as the basis for many applications, or tie existing systems together to improve efficiency and reduce corruption (for example, Argentina's linking of tax, benefit, and property registries). Although initial costs may be

---

[70] However, as outlined for the Dominican Republic, this approach can sometimes have the opposite result if it is implemented in a nationally exclusive way, even while being socially inclusive.

[71] While Pakistan is classified here as an example of centralized, supply-driven identification, NADRA was created in response to the specific imperative of security. In this sense, Pakistan's identity regime was also driven by a specific demand.

[72] For India, UID is still not widely required to access services, but this is changing. From January 1, 2013, residents of New Delhi are required to provide an Aadhaar number for a variety of programs. Even though enrollment was quite high in Delhi by the end of 2012—73 percent in one district—this has impelled a sudden rush to register and a degree of frustration (http://www.hindustantimes.com/India-news/NewDelhi/Delhiites-rush-to-get-UID-as-govt-makes-it-a-must/Article1-984635.aspx).

high, the total cost of a biometric civil registry or ID card will likely be less than the cost of creating multiple functional IDs. This seems especially true for voter registries, where donors have spent hundreds of millions of dollars on periodic biometric rolls that are often ineffective and used infrequently or discarded. A robust civil registry may cost the same as an electoral roll, but it can be used for many purposes—including creating voter lists by transparent, human-centered, processes (Section 3.2).

Pathway 2: Foundation to Function

Advantages	Disadvantages
▪ Many uses, adaptable	▪ Potentially higher initial costs
▪ Economies of scale, scope	▪ Slower development returns; possibly less active take-up
▪ Avoid redundancy, inefficiency, multiple registration	▪ Harder to maintain political will
▪ Potential linkage across applications	▪ Inter-ministerial coordination required
	▪ Formalized citizenship can exclude
	▪ Potential linkage across systems

Like the demand-led approach, the supply-led path also has some potential difficulties. The value of a national ID to a citizen is often less tangible or immediate than a voter card, drivers' license, or health insurance card. The possibility of unenthusiastic or even skeptical citizens necessitates more proactive public education and information campaigns.[73] Without sustained popular and political support—or without incentivized intergovernmental cooperation—the identity system may stall or fail to consolidate, precluding developmental benefits. If not impelled by a specific need, implementation may also be more vulnerable to diversion by corrupt procurement. And, while the ability to easily link databases can be a plus, it also has risks, including the loss of privacy (Section 2.3).

A final concern is the problem of exclusion on the basis of citizenship. In an informal or weak identity system, there are normally many *wrongfully excluded* individuals; those who are entitled to a service or benefit but do not have access due to under-documentation. A robust identity system should include these people, assuming enrollment campaigns successfully reach them. However, it will also exclude people that were *wrongfully included* to begin with. Some of the newly-excluded will be people ineligible for benefits who are intentionally trying to defraud the system; ghost workers, double-dippers, etc. However, some of the excluded may be already marginalized and vulnerable groups, such as refugees or ethnic minorities,

[73] See, for example, Ghana's promotional video for its ID project: http://www.youtube.com/watch?v=CcpEPrYdJVg

that have limited claims to inclusion elsewhere (for example in, the Dominican Republic). This is an identification management issue not specific to biometrics, but countries that choose a foundation-to-function identity management model will have to anticipate and confront such problems up front, when they may be less equipped to do so.

4. Emerging Trends and implications

As the identity gap is increasingly recognized as a constraint to inclusive development, identification-based development programs have proliferated across developing countries, many with support from donors. Some are national in scope, while others are one-off programs with a single functional purpose. Biometric identification technology is used in many of these programs, both to identify individuals uniquely (who are you?) and to enable them to authenticate themselves (are you who you claim to be?). In total, some 1 billion people are covered in the 160 cases surveyed in this paper, and the number is rising rapidly.

Has biometric identification been inclusive and effective in these programs? Do the benefits outweigh the risks? Few studies include rigorous cost-benefit analyses of the use of the new technologies against a counterfactual, or separate out the identification component from other applications of ICT, but many programs report at least some information, from administrative data or monitoring/tracking studies, including surveys, that bear on these questions.[74] Recognizing that many applications are in an early stage and that there is an urgent need for more rigorous assessment, this section synthesizes some of the trends and lessons that have emerged from the applications described above.

4.1. Successes

While more data is needed, existing applications of biometric identification suggest success in some areas, including potentially large gains in efficiency and inclusion—even in less-developed and fragile states. Effective identification opens up new ways of doing things, especially when linked to other ICT.

Rationalization of programs

As elaborated in Gelb and Decker (2011), many developing countries can benefit from robust identification to eliminate ghost workers and rationalize public transfers, subsidy programs and payrolls.[75] For example, expenditure tracking surveys in Africa show leakages of 30 percent and higher for public spending, especially in programs that transfer resources between different levels of government. A number of the cases described above illustrate that biometric de-duplication and authentication can indeed be successful in slimming down payrolls and transfers. When Botswana transferred its pension and social grants registration to biometric enrolment, the numbers reportedly fell by 25 percent through cutting out duplicates, ghosts and the deceased (Smit, 2010).In Nigeria, biometric audits reduced the

[74] Rigorous evaluations include the experiments in Malawi (rural farmers), New Delhi (TB patients) and Bangalore (sex workers).

[75] Biometric identification has also been proposed as a measure to reduce fraud in the delivery of benefits for rich countries. The benefits of the technology, relative to costs, depend on the level of fraud involving duplicates and other ghost beneficiaries. Loss estimates are typically lower (1-2 percent for US food stamps for example) but some assessments have nevertheless considered biometrics as cost-effective (GAO, 1995).

number of federal pensioners by almost 40 percent (African Press Agency, 2011).[76] Other cases include civil service reform in Liberia and Guinea-Bissau. De-duplication can take place at several points, including at the point of payment through the banking system (E-Zwich in Ghana). Assessments of Pakistan's Watan Card program, which featured the use of biometric smartcards, found that payments reached their intended destination with little deviation, and that the costs to the recipient of realizing the payments were very small. Even though not successfully completed, the case of Andhra Pradesh (pre-UID) also showed the potential for biometric de-duplication to reduce costly fraud associated with multiple claims for a wide variety of subsidies (Zelazny, 2012, Annex). With the pre-UID process about 60 percent complete, potential savings from eliminating multiple registrations were estimated at $6 million per month on ration cards, US$1.6 million per month on pensions and a one-time $5 million in housing grants. At a cost of $10 million for the backend software, the system would pay for itself within a month. Drawing on an assessment of the costs and benefits of branchless banking transfer payments relative to cash-based payments by Pickens et al (2009), Gelb and Decker (2011) assess the implications of adding biometric registration and verification to a program delivering US$240 million in 12 monthly installments to 1 million people. The payback period, assuming the elimination of only 5 percent losses, was about one year with savings cumulating to US$64 million over five years. A recent cost-benefit analysis of the UID scheme estimates an internal rate of return to the Indian Government of over 50 percent (NIPFP, 2012)

Inclusion

Cases also show the potential for inclusion. Reducing fraud and diversion is itself inclusive since it liberates resources that can go towards the intended beneficiaries, but there can be more direct effects also. Johnson (2008) analyzed the impact on beneficiaries of using biometric smartcards to deliver payments in Andhra Pradesh. He found that this reduced fraud at the back end, and resulted in greater convenience and empowerment for recipients. Waiting time and collection costs were reduced. The use of biometric smartcards ensured that payments to female beneficiaries were delivered directly to them, rather than to their husbands or brothers as had been common under the previous system. Technology also assisted the extension of the social safety net to poor citizens in the Dominican Republic. Several cases show the potential for inclusion in the area of access to financial services, including through the use of biometric ATMs (Bolivia, Nepal) and by providing identification acceptable for banking KYC requirements. Some cases also show the potential for political inclusion, as in Bolivia's expansion of its electoral roll to include large numbers of previously undocumented citizens.

[76] Though this project has more recently run into problems with corruption allegations: www.businessdayonline.com/NG/index.php/news/76-hot-topic/37779-no-sufficient-data-in-respect-of-estacode-dta-paid-for-biometric-exercise-13

Improved service delivery and accountability

Stronger identification and authentication of individuals can improve service delivery. Rigorously researched examples that show gains from biometric technology include experiments in Malawi (reinforcing incentives for rural farmers to repay loans) and New Delhi (improved monitoring of TB patients through their course of treatment, enabling incentives to health workers to discourage drop-outs). Stronger identity systems can facilitate market-based service delivery, and output-based incentives to extend programs without fear that numbers will be inflated by multiple enrollments. One example (RSBY) is the per capita payment to insurance companies in India based on the number of households enrolled; another is the per capita payment of $5 per head for each new individual registered (Dominican Republic). With strong authentication at the point of delivery, flows or services can be audited more precisely than otherwise possible. This opens up new possibilities for monitoring public service delivery and increasing public accountability (Watan cards in Pakistan).

Leapfrogging in fragile states

Although certain applications have struggled with a mismatch between advanced technology and a difficult political and logistical environment (Angola and Yemen, as well as some of the applications for elections noted below) biometric identification has assisted a number of less developed and conflict-ridden countries in leapfrogging past traditional service delivery mechanisms. When appropriately implemented, it appears to have worked reasonably even in conditions of limited capacity, poor connectivity, and rough terrain (DRC and Chad)—provided that these factors have been taken into account in design and that the programs have adapted in response to prevailing conditions. As an example, even though transfer programs tend to evolve from pull mechanisms of payment to push mechanisms as connectivity increases, the DRC demobilization program went the other way (towards mobile ATMs linked to iris-scanners) once it became clear that there was not a dense enough network of cash service points in part of the sparsely-settled region.

4.2. Failures and risks

Projects can be too ambitious and hasty (elections) or too small and fragmented with an excessive focus on individual applications rather than working towards a coherent, cost-effective, multi-purpose national ID strategy. Even socially inclusive identification programs can be nationally exclusive; not all programs explicitly provide for failure-to-enroll errors, and cost.

Failure to deliver

*S*ome costly voter registration drives, undertaken in difficult country conditions and subject to compressed timeframes, have failed to fully realize the benefits of biometric technology (Afghanistan) as well as being unsustainable without continuing donor support. In some cases, voter cards or an improved roll have provided *de facto* ID (DRC), but often there has been no follow-through to strengthening the country's permanent identification system. Biometric technology has sometimes been cosmetic in these exercises: it has neither

succeeded in de-duplicating the voter registry, or has de-duplicated only locally because of connectivity problems (Bolivia and Somaliland). Hastily procured "black box" technology does not always enhance credibility; in some views it detracts from open human processes, including more transparent, low-tech alternatives such as marking voters' fingers with indelible ink. Rarely are biometrics used to authenticate voters at the polls though examples are increasing.

Poorly executed projects are not limited to elections. Other cases have suffered from inadequate technology, including poor procurement, insufficient quality or quantity of data collected, and the scalability of the back-end processes needed to manage data and de-duplicate registrations (national IDs in Yemen, PDS in Andhra Pradesh). This often results from trying to do too much too fast, or getting locked-in to proprietary contracts. Long-term coherent planning is required, as well as a sound grasp of performance standards. Governments that attempt to introduce an all-encompassing identity system but lack capacity and resources may be overwhelmed, and the project may stall and ultimately fail.

Fragmentation and proliferation

A second problem is the fragmentation of identification efforts and their proliferation across programs. In some instances, projects have been too small for savings to cover the costs of setting up the system (DECT in Malawi). More generally, there are inefficiencies in setting up a different system of identification for every program and, if disparate systems cannot be linked, this also prevents providing services in a client-centered way. Some people might be covered by several different identification programs while others fall through the cracks. In addition to requiring individuals to register and re-register multiple times, proliferation raises the specter of chaotic proliferation of databases which can compromise data security.

In Nigeria, for example, a report by the Committee on Harmonisation of National Identity Cards (Government of Nigeria, 2006) identified 12 ongoing ID card projects—of which 8 included biometrics—and called for a shift from cards to nationwide identity management.[77] This is not to say that every country should go the Malaysian route of mandating a single national identification to cover all purposes. One alternative is to develop a common database to cover a range of social programs (as Pakistan and South Africa have done). If multiple IDs are necessary, the ability to coordinate between them is key.

Exclusion

If identification is to be inclusive, countries must break the cycle of under-documentation. This can involve allowing substitute documentation, like communal records from local civil

[77] In a recent article, Rajshekhar (2012) noted at least seven state-led biometric applications in India, in addition to those launched by banks. Pakistan has moved to head off data base proliferation by developing data sharing protocols for the National Socio Economic Registry managed by the Benazir Income Support Program, a partnership between the Ministry of Finance, NADRA (the National Identification Authority) and Pakistan Post. These enable essential variables from the centralized database to be shared with other social programs which, in turn, are expected to enrich the database with any additional information they collect.

or religious leaders, to provide a birth registration "amnesty" (national ID cards in the Dominican Republic and Pakistan[78]), or decoupling formal identification from citizenship (Aadhaar). The latter helps inclusion but issuing numbers without including considerations of citizenship at the same time may simply shift the documentation burden from the initial enrollment to later applications (voting or entitlements) where national status is a criterion of eligibility. Although its birth amnesty helped to include some undocumented nationals, the Dominican identification project implemented citizenship legislation that excluded many individuals of Haitian descent, leaving some in a stateless limbo. NGOs can play a useful role, monitoring rollout for inclusiveness and helping applicants through the sometimes time-consuming process of securing credentials. Countries where this issue is most pressing—especially those with large migratory or nomadic populations—will possibly find it easier to link identification system to some specific applications rather than start off with an exclusive focus on the contentious question of citizenship, but any identification-based strategy will need to anticipate the nationality issue and plan to address it.

National exclusion is a policy issue: for biometrics, the concerns are failure-to-enroll and errors.[79] Some programs make provisions for such failures—which can be minimized through the use of multi-modal biometrics (like Aadhaar)—but few are explicit on performance standards, including for rectifying errors. These are critical even if non-biometric approaches to identification may involve more errors; since biometric errors are rarer and systems are often billed as "infallible", individuals may have a more difficult time in cases of mistaken identity.[80] There is also the ongoing issue of how to include very young children for whom it is difficult to capture quality fingerprints or iris scans. Since birth registration is not complete without documenting family relationships, any measures to relax requirements for children must provide similar arrangements for parents. The alternative is a growing cycle of exclusion, as unidentified parents beget unidentified children.

Privacy

The taking of fingerprints seems to be generally accepted in developing countries, perhaps because people already associate it with banking and social programs. Many—including

---

[78] NADRA has recently allowed undocumented orphans to get national ID cards, despite their unconfirmed citizenship and parentage, see http://www.pakistantoday.com.pk/2012/11/08/city/karachi/cnics-to-be-issued-to-orphans/.

[7979] Failure-to-enroll rates can be substantial. In Chad 10 percent of fingerprints from women over 25 showed visible damage and were difficult to capture (Weibel, et al., 2008). In Malawi, fingerprint scanners were cleaned after each impression, and loan applicants washed their fingers before each impression to reduce errors. Nevertheless, researchers report that around 2 percent of borrowers had difficultly scanning their rights fingerprints (worn out due to tobacco planting), and that left thumbprints were taken in these cases (Giné, et al., 2010). Rates appear to be lower for iris (UIDAI, 2012b).

[80] This halo effect is also important to consider. In many cases, the technical nature of biometric data can instill an aura of credibility and integrity whether this exists or not—this can be good or bad. In India, Operation Asha found that patients were more likely to visit clinics using biometric health records because the "technology demonstrated that the program was committed to high quality treatment" (Paik, et al., 2010). In the Bolivian case, the biometric voter roll, though flawed, was considered a relatively popular success and national unity cause. Still, a false sense of credibility that obscures bad data may also prolong corrupt or exclusive systems.

participants in the vaccine trial in Vietnam—report that using biometrics *enhanced* privacy by enabling individuals to authenticate themselves without providing substantive information on gender, race, health status, etc. There has been some concern regarding taking women's biometrics in conservative populations, particularly photos and iris scans of Muslim women who wear the veil. In most cases, however, this has been a minor or a non-issue (for example, Bangladesh voter registration and refugee identification in Pakistan).[81]

Some applications of biometric identification have not required any database (e.g., Afghan refugee resettlement grants) but these are the exception. Most programs require that biometrics authenticate an individual to a stored record in a data set. The difficult question is when to allow individual records to be linked across data sets using a common identifier. Some linkages may be reasonably motivated by a desire to prevent tax evasion or benefit fraud (SINTyS in Argentina). National ID databases can link to program databases in order to improve targeting, including in emergency programs (Watan card).[82] Others linkages threaten privacy and could expose subjects and their families to personal risk (a particular concern for refugees), although we have not seen evidence of that in any of these cases. Countries need a framework for data protection that covers such questions, including for exceptional, security-related, access. Many developing countries do not have such a framework. In the shorter-run, agreed protections on personal data within a project can provide a band-aid but this is not a longer-term solution.

4.3. Strategy

There is no perfect approach towards a developmental identity system; some are "supply-driven" others build from demand. The most appropriate strategy is one that takes national context and capacity into account and recognizes the value of incentives to adopt the new technology and for institutional coordination. Data quality and quantity are paramount; technology is maturing rapidly and costs are plummeting.

Identification regimes evolve in different ways in different countries. Some have followed a top-down supply-driven process to create a more robust multi-purpose or national ID that can then be applied to a variety of programs (Latin America, Aadhaar). Others have followed a demand-driven approach, creating purpose-specific identification—such as payroll, taxes, or voter registration—that can then be extended to other uses. Identification may then be more immediately useful and motivate registration, anchor the system in development, and provide savings from more efficient programs that can be used to support the further extension of the system. But it also risks losing economies of scope and scale, especially if

[81] The UNHCR program to issue identification to Afghans living in Pakistan gave women the option of not having their photographs taken and relying only on fingerprints. They report that over 66 percent of women still opted to have their photos taken (UNHCR & Pakistan, 2007). Similarly, the IRI reports no major objection from Muslim women to being photographed during Bangladesh's biometric voter registration effort, which they attribute to an effective outreach campaign with community and religious leaders (IRI, 2009).

[82] However, this will likely only be beneficial if the databases are frequently updated (e.g., if addresses are incorrect, the right people may not get disaster relief payments).

the identification technology is seen as simply a cost of implementing a particular program rather than sufficiently accurate and scalable to underpin future uses.

Pilot programs and iterative development or rolling out programs by area (such as voter registration in Afghanistan, Brazil, Benin, etc.) may improve implementation. But some disruption is probably inevitable at the intersection of supply and demand, especially at moments when an ID first becomes mandatory for accessing an important service, leading to frustrated recipients and at least some temporary exclusion. Countries will need to plan for this, providing adequate notice and phasing-in requirements with incentives to minimize a sudden crush of applications.

In the longer-run, while the public seems to accept identification and the use of biometrics, especially when they improve services, new technology confronts the political economy of winners and losers, including those who lose scope for bureaucratic discretion. Successful applications require continuity of support and perhaps some influential champions to maintain momentum. Extending programs too quickly to sensitive groups—for example, to include security forces in payroll reform during a period of instability (Yemen)—can lead to abandonment.

Even without clear losers, institutional coordination may be problematic. Identity services are typically managed or used by agents with diverging mandates: ministries, electoral commissions, regulatory bodies, central banks, etc. Achieving economies of scope requires some mechanism of institutional coordination. This can take various forms, such as the creation of a "social cabinet" (Dominican Republic). Not all players need be included, especially if the intention is not to have one single identifier, but coverage should be sufficient to bring together a critical mass of applications and to demonstrate a national interest in pursuing a coordinated strategy for robust identification. Over the longer run, we can expect that "better" identification diffuses to cover a range of applications (US SSN and driver's licenses), but bureaucratic entrenchment can extend competing systems for a very long time.

India's UID program has profound implications for other countries, even though it is only beginning to be used in service delivery. Its standards-based approach enables competition in hardware and software markets, reducing costs. It has also set high standards for technology and data accuracy, which others can and should consider adapting for their own purposes. The use of several biometrics—such as fingerprints, iris, digital photo—increases both inclusion and precision (Aadhaar); it is better to do it once correctly than several times. Relative to the overall logistical costs of mounting a registration effort, the additional technology costs of including a wider range of biometrics is now modest: the old practice of including just one or two fingerprints is obsolete. Data quality is also important: quantity and quality should be adequate to enable enrollments to be de-duplicated, to ensure uniqueness. Unless sufficient data is collected at the beginning of an exercise, citizens may have to undergo repeated mass registrations as individual programs are expanded or taken over by national systems (PDS in Andhra Pradesh).

4.4. Role of donors

Donors can play critical roles in facilitating a strategic approach to identity management. They fund identification exercises (including by output-based aid), and play a demand-side role through programs. They should help to ensure that the poor do not face cost barriers to identification, that the technology is robust, and that the identity system provides public goods in the form of economies of scope and scale.

Donors have actively participated in the diffusion of identification technology to developing countries. They have supported about half of the applications surveyed in this paper; they can disseminate best practices, and offer technical and legal support. They also play a demand-side role, by funding of many applications, including transfer and health programs, as well as elections, which use identification services. They should not support systems that are likely to be financially unsustainable and to raise barriers to inclusion. They should resist the temptation to try and lend legitimacy to flawed processes by supporting ineffective technology that will clearly be unable to deliver its promised benefits.

Unique identification can be particularly useful for donors, because it opens the way to output-based financing: programs can be rolled out based on incentive payment for each successful delivery. This type of financing requires that the beneficiary roll is de-duplicated, since it creates incentives to create fake individuals, or to deliver services to the same people several times. With effective de-duplication, output-based financing can be used to roll out the registration program itself, by providing a payment for each successful enrolment (Dominican Republic ID).

Donors can also play a special role, helping resolve the collective action problems that limit the public good aspect of identification. They can strengthen incentives for ministries to develop a common identity-based approach, supporting them as they re-tool their operations to take advantage of a new joint system (SINTyS in Argentina) or otherwise encourage cooperation (elections in Benin). However, avoiding fragmentation will require donors to take a wider view of identification within the context of development than has often been the case in the past. Identification should be seen as part of a country development strategy rather than just a cost component of one particular program.

5. Conclusion

Low-income countries still face a large identity gap relative to rich ones; their official identification systems often have limited coverage and low accuracy. Within countries, there is a similar "identity gap" between rich and poor; the latter are far less likely to have strong birth certificates or other official identification. States cannot engage effectively with un-identified citizens. Without robust identification, individuals are excluded in many ways. They cannot authenticate themselves to claim rights, including services, voting, or participation in the formal economy.

The "identity gap" is increasingly recognized as not only a symptom of underdevelopment but a contributing factor. Programs are increasing, both to provide official identity and to strengthen identification as an instrument in development-related areas, including banking and finance, public payroll management, social transfers and pensions, health-care and health insurance and voter rolls. Many of these programs have begun to use biometric identification technology, so that the sales of the industry are growing more even more rapidly in poor countries than in rich ones.

National identification is a contentious topic, as is biometric technology, perhaps because of its association with surveillance and security—still, these concerns are still more pronounced in rich countries than in poor ones. This paper has considered developmental applications, drawing on information from 160 programs across low and middle-income countries, and distinguishing as far as possible between identification in general and biometric technology in particular. Some programs have emphasized foundational national ID, and its extension to a range of programs; others have been purpose-driven, building from an application to a broader purposed identity system. Countries differ in many ways, and there is no unique path towards developmental identification.

The paper argues that to be successful from a development perspective, applications have to be both inclusive and efficiency-enhancing. While the area cries out for more rigorous assessment, some of the cases appear to pass these tests and represent significant innovations in the developmental use of technology. But others fail to improve inclusion or efficiency (or both), pointing to the importance of context and implementation in the application of technology. These conclusions draw on available information. We recognize the need for more empirical evaluation, as well as more open performance data on the inclusion and accuracy of the identification systems themselves.

Where do we go from here? One lesson from the cases is the value of adopting a strategic developmental approach to identification, rather than seeing it simply program-by-program as a cost and adopting *ad hoc* approaches. This is also an issue for donors, who have supported at least half of the cases included in this paper. Especially with the maturation of the technology, countries should assess their identity management situation, review their needs, and formulate a strategy—together with donors—that can be rolled out in a way that integrates robust identification with a range of development programs. The alternative is a

project-by-project approach, with waste, inconvenience to citizens, and possible failure to reap the benefits of the technology.

A number of countries, including Pakistan, India, and various Latin American countries, offer good examples for South-South learning. By sharing and framing key lessons and tradeoffs, countries and donors can learn to strengthen identification systems, including through the application of biometrics when advantageous, and the use of alternative technology it is not. This requires greater partnerships both *between* and *within* countries that have undertaken identity projects, agencies that frequently use or fund biometric and identification technology—the World Bank, OAS, IDB, UNICEF, UNDP, bilateral agencies—and technical experts. When applied smartly, the biometric revolution can indeed be harnessed for development.

References

ACE Electoral Knowledge Network. (2008). Voter Registration in Afghanistan, from aceproject.org/today/feature-articles/voter-registration-in-afganistan

Adajania, K. E. (2012, August 14). Did You Know: Aadhaar can be used as proof address in KYC?, *livemint.com*. Retrieved from http://www.livemint.com/2012/08/14213635/Did-You-Know--Aadhaar-can-be.html

African Press Agency. (2011, February 1). 37,000 Ghost Pensioners Discovered in Nigeria, *NetNewsPublisher*. Retrieved from http://www.netnewspublisher.com/37000-ghost-pensioners-discovered-in-nigeria/

Alston, P., & Robinson, M. (Eds.). (2005). *Human Rights and Development: Towards Mutual Reinforcement* Oxford: Oxford University Press.

Angola Press Association. (2011, August 1). Angola: Voter Registration Update to Engage Angolans in Democracy, *All Africa Online*. Retrieved from allafrica.com/stories/201108011850.html

Associated Press. (2012). Salvador Allende's granddaughter in Chile election win, *The Guardian Online*. Retrieved from http://www.guardian.co.uk/world/2012/oct/29/allende-granddaughter-chile-election-win

Atick, J. (2012). *On the Future of Identity?* Paper presented at the From Biometrics To Augmented Human Recognition, Rome, May 10, 2012.

Azad, M. A. K. (2011, October 5). Hi-tech driving licence on cards, *The Daily Star Online*. Retrieved from www.thedailystar.net/newDesign/news-details.php?nid=205259

BBC. (2009, July 2). Q&A: Identity cards, *BBC News Online*. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/3127696.stm

BBC. (2012, May 15). Biometric data: Schools will need parents' approval, *BBC News Online*. Retrieved from http://www.bbc.co.uk/news/education-18073988

Bennett, C. J., & Lyon, D. (2008). Playing the ID Card: Understanding the significance of identity card systems. In C. J. Bennett & D. Lyon (Eds.), *Playing the Identity Card: surveillance, security and identification in global perspective*. New York: Routledge.

BISP. (2011). National Socio Economic Registry for the Social Protection Sector in Pakistan, BISP Data Sharing Protocol: Benazir Income Support Programme.

Botekar, A. (2012, August 17). Snags delay biometric attendance, *The Times of India Online*. Retrieved from http://articles.timesofindia.indiatimes.com/2012-08-17/nashik/33248461_1_ashram-schools-biometric-devices-sim-cards

Bowyer, K. W., Baker, S. E., Hentz, A., Hollingsworth, K., Peters, T., & Flynn, P. J. (2009). Factors That Degrade the Match Distribution In Iris Biometrics. *Identity in the Information Society, 2*(3), 327-343.

Bowyer, K. W., & Fenker, S. P. (2012). *Analysis of Template Aging in Iris Biometrics*. Paper presented at the IEEE Computer Society Biometrics Workshop, June 17, 2012. http://www.nd.edu/~kwb/FenkerBowyerCVPRW_2012.pdf

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. (2010). The World's First Biometric Money: Ghana's E-Zwich and the Contemporary Influence of South African Biometrics. *Africa, 80*(4).

Brodersohn, E. (2012). Experiences and Challenges on Unique Identification. Innovating applications, a Mexican case *International Conference on Implementing Social Programs: Better Processes, Better Technology, Better Results*. September 4-6, 2012, Bangalore, India.

Casselman, A. (2008, April 3). Identical Twins' Genes Are Not Identical, *Scientific American Online*. Retrieved from http://www.scientificamerican.com/article.cfm?id=identical-twins-genes-are-not-identical

Cross River State. (2010). Project HOPE - Free Healthcare for pregnant women and children under five, 23 May 2012, from http://www.mswcd.crs.gov.ng/index.php?option=com_content&view=section&layout=blog&id=5&Itemid=2

de Sainte Croix, S. (2010, March 30). Brazil's Most Secure Voting Ever, *The Rio Times*. Retrieved from http://riotimesonline.com/brazil-news/front-page/brazils-most-secure-voting-ever/#

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

Devereux, S. (2007). Innovations in the Design and Delivery of Social Transfers: Lessons Learned from Malawi: Institute of Development Studies and Concern Worldwide.

Diaz, J. (2011, October 26). House to expand e-voting *Philippine Star Online*. Retrieved from http://www.philstar.com/Article.aspx?articleId=741354&publicationSubCategoryId=

Dror, I. E., Charlton, D., & Peron, A. E. (2006). Contextual information renders experts vulnerable to making erroneous identifications. *Forensic Science International, 156*, 74/78.

E-Health Reporter. (2012, May 16). Six Months On, How is SIBIOS Working? Retrieved from http://www.ehealthreporter.com/en/noticia/verNoticia/1165/six-months-on-how-is-sibios-working

EC, UNDP, & International IDEA. (2010). Procurement Aspects of Introducing ICT Solutions in Electoral Processes: The Specific Case of Voter Registration. Brussels: EC-UNDP Task Force on Electoral Assistance,.

ePractice.eu. (2012). eGovernment Factsheet - Estonia - National Infrastructure Retrieved 23 August, 2012, from http://www.epractice.eu/en/document/288219

Evrensel, A. (Ed.). (2010). *Voter Registration in Africa - A Comparative Analysis*. Johannesburg: EISA.

Freishtat, S. (2012, July 26). Just a face in a crowd? Scans pick up ID, personal data, *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2012/jul/26/just-a-face-in-a-crowd-scans-pick-up-id-personal-d/?page=all

Froomkin, M., & Weinberg, J. (2012). Hard to Believe: The High Cost of a Biometric Identity Card. Research Brief: The Chief Justice Earl Warren Institute on Law and Social Policy, University of California Berkeley, School of Law.

Gabriel, O. (2011, 11 July). 36 MDAs had 43,000 ghost workers – Aganga, *Vanguard*. Retrieved from http://www.vanguardngr.com/2011/07/36-mdas-had-43000-ghost-workers-aganga/

Gahamanyi, J. (2012, August 11). Rwandans to use national ID cards for shopping, *The New Times Online*. Retrieved from http://www.newtimes.co.rw/news/index.php?i=15081&a=8835

Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., & Ortega-Garcia, J. (2012). *From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems*. Paper presented at the Black Hat USA, Las Vegas, 2012. https://media.blackhat.com/bh-us-12/Briefings/Galbally/BH_US_12_Galbally_Iris_Reconstruction_WP.pdf

GAO. (1995). Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program *Report to the Honorable Kenneth E. Bentsen, Jr., House of Representatives*: United States Government Accountability Office.

Gelb, A., & Decker, C. (2011). Cash at Your Fingertips: Biometric Technology for Transfers in Resource-Rich Countries *Working Paper 253*: Center for Global Development.

Gelb, A. and Clark J. (2013) Performance Lessons from UID. Center for Glopbal Development, forthcoming.

Gemalto. (2010). New driver's licenses: Identification and accountability for better road safety. Public Sector Case Study.

Ghauri, I. (2012, July 9). NADRA study shows voter numbers rise in Punjab, *The Express Tribune Online*. Retrieved from http://tribune.com.pk/story/405622/nadra-study-shows-voter-numbers-rise-in-punjab/

Giné, X., Goldberg, J., & Yang, D. (2010). Identification Strategy: A Field Experiment on Dynamic Incentives in Rural Credit Markets.

Government of Aguascalientes. (2011). *Sistema Nominal en Salud (SINOS)*. Aguascalientes: Retrieved from http://www.isea.gob.mx/formatos/InfoSinos.pdf.

Government of Mexico. (2010). Primera Consulta, Consulta Segura. *México Sano, 3*(19).

Government of Nigeria. (2006). Final Report of the Committee on Harmonisation of National Identity Cards.

Guidorizzi, R. (2012). *Active Authentication: Moving Beyond Passwords*. Paper presented at the TABULA RASA. Spoofing and Anti-Spoofing: the Wider Human Context, Rome, May 10-11, 2012.

Harbitz, M., & Boekle-Giuffrida, B. (2009). Democratic Governance, Citizenship, and Legal Identity: Linking Theoretical Discussion and Operational Reality *Institutional Capacity and Finance Sector Working Paper*. Washington, DC: Institutional Capacity and Finance Sector, Inter-American Development Bank.

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

Hernandez, R., & Mugica, Y. (2003). What Works: PRODEM FFP's Multilingual Smart ATMs for Microfinance. Innovative solutions for delivering financial services to rural Bolivia: World Resources Institute.

Higgs, E. (2011). *Identifying the English: a History of Personal Identification 1500 to the Present* London: Continuum.

Hosein, G. (2011, August 26). Why we work on refugee privacy. Retrieved from https://www.privacyinternational.org/blog/why-we-work-on-refugee-privacy

Hunt, S., O'Leary, S., Newton-Lewis, T., & Ali, D. Z. (2011). Evaluating implementation of Pakistan's citizens damage compensation programme (phase 1). Final Report: Oxford Policy Management.

IFES. (2008). Assessment of the Photo Voter List in Bangladesh. Final Report: International Foundation for Electoral Systems.

IMF. (2011). Guinea-Bissau: Second Poverty Reduction Strategy Paper, IMF Country Report No. 11/353. Washington, DC: International Monetary Fund.

INEC. (2009). Ecuador: Historia de la Estadística en el País: Instituto Nacional de Estadística y Censos.

IRI. (2009). Bangladesh Parliamentary Elections. Election Observation Mission Final Report. Washington, DC: International Republican Institute.

JACITAD. (2012). Nigeria SIM Registration Survey, Status Report: Joint Action for ICT Awareness and Development.

Jadhav, A. (2011, October 6). Pune Bar Association to get biometric cards to vet fake lawyers, *Daily News and Analysis Online*. Retrieved from http://www.dnaindia.com/mumbai/report_pune-bar-association-to-get-biometric-cards-to-vet-fake-lawyers_1595634

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1).

Johnson, D. (2008). Case Study on the Use of Smartcards to Deliver Government Benefits in Andhra Pradesh, India: Institute for Financial Management and Research.

Leland, J. (2006, September 4). "Immigrants stealing U.S. Social Security numbers for jobs, not profits - Americas - International Herald Tribune", *New York Times*. Retrieved from http://www.nytimes.com/2006/09/04/world/americas/04iht-id.2688618.html?_r=1&pagewanted=allexpand

Lewis, T., Synowiec, C., Lagomarsino, G., & Schweitzer, J. (2012). E-health in low- and middle-income countries: findings from the Center for Health Market Innovations. *Bulletin of the World Health Organization, 90*, 332–340.

Liebman, J. B. (2000). Who are the Ineligible EITC Recipients? *National Tax Journal, 53*, 1165-1186.

Long, G. (2012, October 26th). Chile's military rule 'disappeared' on electoral roll, *BBC News Online*. Retrieved from http://www.bbc.co.uk/news/world-latin-america-20078323#

Malakata, M. (2012, May 25). Multiple problems thwart Nigeria SIM card registration, *PC Advisor*. Retrieved from http://www.pcadvisor.co.uk/news/mobile-phone/3360184/multiple-problems-thwart-nigeria-sim-card-registration/

Mathieson, D., & Wager, R. (2010). Somaliland National Election Commission: Report on the Preparation of the Voter Register January to June, 2010 (Vol. Version 1.2): ERIS.

Mayhew, S. (2012, 10 October). Smartmatic assists Venezuela [to] conduct national election, *BiometricUpdate.com*. Retrieved from www.biometricupdate.com/201210/smartmatic-assists-venezuela-conduct-national-election/

Mbeng Mendou, J.-P. (2012). *Financing innotative (sic) of health care in Gabon*. Paper presented at the Prince Mahidol Award Conference 2012, January 24-28, Bangkok, Thailand.

http://www.pmaconference.mahidol.ac.th/index.php?option=com_docman&task=doc_download&gid=554

MCC. (2009). 4Ps Concept Paper for MCC: Millennium Challenge Corporation.

Mubiri, R. (2012, July 5). MPs want implicated officials to refund ID project money, *Uganda Radio Network Online*. Retrieved from http://ugandaradionetwork.com/a/story.php?s=43450&PHPSESSID=e8c335e745dee53a4805c7899a4d5ba7

Muhula, R. (2011, August 31). [Telephone conversation with Alan Gelb and Julia Clark].

Narayan, D. (1999) Voices of the Poor, Volume 1 *Can Anyone Hear Us? Voices From 47 Countries*: World Bank, Poverty Group, PREM.

NIPFP. (2012). A cost-benefit analysis of Aadhaar: National Institute of Public Finance and Policy.

Okafor, C. (2012, May 29). EFCC, SSS Others to Uncover Ghost Workers, *This Day Live*. Retrieved from http://www.thisdaylive.com/articles/efcc-sss-others-to-uncover-ghost-workers/116818/

OSI, & CEJIL. (2012). Submission to the United Nations Human Rights Committee: Review of the Dominican Republic: Open Society Justice Initiative and the Center for Justice and International Law.

Paik, M., Samdaria, N., Gupta, A., Weber, J., Bhatnagar, N., Batra, S., . . . Thies, W. (2010). *A Biometric Attendance Terminal and its Application to Health Programs in India*. Paper presented at the 4th AMC Workshop on Networked Systems for Developing Regions, 15 June 2010, San Francisco, CA. http://www.dritte.org/nsdr10/files/nsdr10_paper04.pdf

Palacios, R., Das, J., & 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.

Pearson, R. V., & Kilfoil, C. (2007). Dowa Emergency Cash Transfer (DECT) Wider Opportunities, Evaluation and Recommendations: Solid Lessons and a Promising Vision *DECT Wider Opportunities Report-Final-v01.doc*: Concern Worldwide.

Pessino, C., & Fenochietto, R. (2007). *How to implement a National Coordinated System for the Identification of Individuals and Information Exchange to Improve Fiscal and Social Equity. Lessons from LACs*. Paper presented at the 1st International Conference on Theory and Practice of Electronic Governance, ICEGOV 2007.

Pickens, M., Porteous, D., & Rotman, S. (2009). Banking the Poor via G2P Payments *Focus Note 58*. Washington, DC: CGAP, World Bank.

Piron, L.-H., & O'Neil, T. (2005). Integrating Human Rights into Development: A synthesis of donor approaches and experiences *Prepared for the OECD DAC Network on Governance (GOVNET)*. London: Overseas Development Institute (ODI).

Post, P. (2012, July 26). Uganda Taking Team to Little League World Series, *New York Times*. Retrieved from http://www.nytimes.com/2012/07/27/sports/uganda-to-field-1st-african-little-league-world-series-team.html?pagewanted=print

Rajshekhar, M. (2012, June 24). Are Your Biometrics Stacked Against You?, *The Economic Times*. Retrieved from http://articles.economictimes.indiatimes.com/2012-06-24/news/32382928_1_biometrics-uidai-national-population-register

RNEC. (2011). Pruebas Piloto de Voto Electronico, 2006 a 2011 *Documento de Trabajo para la Modernizacion de la Gestion Electoral*: Secretaria Technica, Registraduria Nacional del Estado Civil.

Roop, L. (2012, June 21). IDair's new fingerprint reader captures prints from 6 meters away, *The Huntsville Times*. Retrieved from http://blog.al.com/breaking/2012/06/idairs_new_fingerprint_reader.html

ROP. (2012). PH submits ILO C185 ratification instrument to ILO Retrieved 26 August, 2012, from http://www.dole.gov.ph/secondpage.php?id=2665

Serwaa-Bonsu, A., Herbst, A. J., Reniers, G., Ijaa, W., Clark, B., Kabudula, C., & Sankoh, O. (2010). First experiences in the implementation of biometric technology to link data from Health and Demographic Surveillance Systems with health facility data. *Global Health Action, 3*.

Smit, T. (2010). Telephone converstaion with Alab Gelb and Caroline Decker, 9 July 2010.

SonLa Study Group. (2007). Lessons from the field: Using a fingerprint recognition system in a vaccine trial to avoid misclassification. *Bulletin of the World Health Organization, 85*(1), 64-67.

Southbridge S.A. (2012). Health in Chile - Market Profile, February 2012. In New Zealand Trade & Enterprise (Ed.), *Exporter Guide*.

Steiner, C. (2010, April 20). The Identity Thief Killer, *Forbes Online*. Retrieved from http://www.forbes.com/forbes/2010/0412/investing-identify-theft-iris-scanner-big-brother-we-see-you.html

Talemwa, M. (2012, March 27). IHK introduces patient smart cards, *The Observer Online*. Retrieved from http://www.observer.ug/index.php?option=com_content&view=article&id=17896%3Aihk-introduces-patient-smart-cards&catid=58%3Ahealth-living&Itemid=89

Tash Lumu, D., & Kakaire, S. (2012, July 13). IDs: Museveni explains role, *The Observer Online*. Retrieved from www.observer.ug/index.php?option=com_content&task=view&id=19820&Itemid=114

TechNavio. (2012). Biometrics Market in India 2010–2014.

Tesfaye, M. (2009, July 15). Ethiopia: The Revenue and Customs Authority to collect fingerprints, *Ethiopian Review*. Retrieved from http://www.ethiopianreview.com/articles/14032/print/

The Carter Center. (2009). Observation Mission of the Bolivia Voter Registration 2009. Final Report. Atlanta, GA: The Carter Center.

The Hindu. (2012, August 11). Kerala scores a first, issues biometric ID cards for fishermen, *The Hindu Online*. Retrieved from http://www.samachar.com/Kerala-scores-a-first-issues-biometric-ID-cards-for-fishermen-mildK6bbfbi.html

TNN. (2012, August 18). Fingerprint attendance for health dept officers, *Times of India*. Retrieved from http://timesofindia.indiatimes.com/city/kolkata/Fingerprint-attendance-for-health-dept-officers/articleshow/15539934.cms

Tokalau, T. (2012, August 19). Ministry to accept voter cards as valid ID, *The Fiji Times Online*. Retrieved from http://www.fijitimes.com/story.aspx?id=209538

UIDAI. (2012a). Role of Biometric Technology in Aadhaar Authentication. Authentication Accuracy Report.: Unique Identification Authority of India

UIDAI. (2012b). Role of Biometric Technology in Aadhaar Authentication. IRIS Authentication Accuracy - PoC Report: Unique Identification Authority of India

UIDAI. (2012c). Role of Biometric Technology in Aadhaar Enrollment: Unique Identification Authority of India

UNDP. (2009). Enhancing Legal & Electoral Capacity for Tomorrow (ELECT), Annual Progress Report – 2009: United Nations Development Programme, Afghanistan.

UNDP. (2011). Benin: Election Support Retrieved 22 June, 2012, from http://www.undp.org/content/undp/en/home/ourwork/democraticgovernance/global_programmes/global_programmeforelectoralcyclesupport/highlights/benin_success_story/

UNHCR. (2007). Pakistan: Operational highlights *UNHCR Global Report*.

UNHCR. (2008). Applying ICT to Support Refugees *UNHCR & Microsoft Partnership Profile*: United Nations High Commissioner for Refugees

UNHCR. (2012). UNHCR Global Trends 2011: A Year of Crises. New York: United Nations High Commissioner for Refugees.

UNHCR, & Pakistan, G. o. (2007). Registration of Afghans in Pakistan, 2007: Ministry of States & Frontier Regions Government of Pakistan, National Database & Registration Authority (NADRA), United Nations High Commissioner for Refugees.

UNICEF. (2005). The 'Rights' Start to Life: A Statistical Analysis of Birth Registration. New York: The United Nations Children's Fund (UNICEF).

UNICEF Innocenti Research Centre. (2002). 'Birth Registration: Right from the Start'. *Innocenti Digest No. 9, UNICEF Florence*.

United Nations. (2008). Innovation for Sustainable Development: Local Case Studies from Africa: Department of Economic and Social Affairs.

VaxTrac. (2010, May 12). Tech Update! Retrieved from http://vaxtrac.com/blog/2010/11/tech-update/

Wade, W. (2012). Identity 101 *International Conference on Implementing Social Programs: Better Processes, Better Technology, Better Results*. September 4-6, 2012, Bangalore, India.

Washington Post. (2012, May 1). A Md. court's bizarre ban against collecting DNA samples, *Washington Post*. Retrieved from http://www.washingtonpost.com/opinions/a-md-courts-bizarre-ban-against-collecting-dna-samples/2012/05/01/gIQAgAkAvT_story.html

Weibel, D., Schelling, E., Bonfoh, B., Utzinger, J., Hattendorf, J., Abdoulaye, M., . . . Zinsstag, J. (2008). Demographic and health surveillance of mobile pastoralists in Chad: integration of biometric fingerprint identification into a geographical information system. *Geospatial Health, 3*(1), 113-124.

Were, V., Ijaa, W., Amek, N., Chiteri, E., Obor, D., Onyango, E., . . . Laserson, K. (2011). *Fingerprinting Individuals in the KEMRI/CDC Health and Demographic Surveillance System (HDSS), Western Kenya, 2010*. Paper presented at the 11th INDEPTH Scientific Conference (ISC), October 24-27, 2011, Maputo, Mozambique. http://www.indepth-network.org/ISC%202011/presentations/Tuesday/HDSS%20FINGERPRINTING%20PRESENTATION_Victor%20Were.pdf

Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics: Identity Assurance in the Information Age*: McGraw-Hill Osborne Media.

World Bank. (2007). Project Appraisal Document on a Proposed Loan in the Amount of US$19.4 Million to the Dominican Republic for a Social Protection investment Project. Washington, DC: World Bank.

World Bank. (2010a). Project Appraisal Document on a Proposed IDA Grant...to the Republic of Benin for a Health System Performance Project. Washington DC.

World Bank. (2010b). Public Financial Management Reform in the Middle East and North Africa: An Overview of Regional Experience, Part I, Overview and Summary. Washington, DC: Middle East and North Africa Vice Presidency, World Bank.

World Bank. (2011). Wage Bill and Pay Compression Summary Note. Washington, DC: World Bank, PREM Public Sector & Governance unit.

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.

Appendix 1: Key Concepts in Biometrics

Biometric basics[83]

Using biometrics for identification means assessing an individual's identity based on a unique physical or behavioral trait; something that they *are*. This is, of course, not the only means of identification. For millennia, individuals have also been identified based on something they *have* (a card, birth certificate or token), or something they *know* (a PIN or a password). Still, digitized biometrics, have several advantages over physical tokens and numerical codes, as they

- Are unique to every individual
- Cannot be misplaced or forgotten, and are very difficult to fake or steal
- Do not require literacy
- Can help to create an auditable trail for transactions
- Increase anonymity when used in place of personal details (names, addresses, etc.)

Fingerprints have historically been the most commonly used biometric, but iris recognition is becoming more prevalent in development applications, along with face prints. Such biometrics can help answer the question "is this person who they say they are?" When linked with other data, such as age, residency etc., they can also determine whether or not the individual is eligible for certain rights or benefits (voting, welfare, driving, etc.). They are often combined in order to increase security—for example, many chip-based ID cards store both fingerprint and PIN data. Still, biometrics cannot be a substitute for all documentation. In order to prove nationality, for example, one must have a birth certificate or other official document.

Increasingly, projects are using multimodal biometrics: that is, they use fingerprints along with iris scans and/or face prints. More data means higher accuracy, wider population coverage (if someone has damage to their fingers, you can get by with their iris scan), and increased efficiency. For example, iris scans are ideal for one-to-many (1:N) matching because they offer the most data points, while fingerprints are faster and cheaper to process and thus favored for one-to-one (1:1) comparisons, such as checking if a person matches the data stored on their national ID card.

The process for biometric identification differs based on technology choices and context. However, most cases generally involve some combination of the following steps:

1. **Capture (enrollment)**. Biometric data is collected using scanners, cameras or other devices (e.g. microphones for voice recognition). The devices record distinctive

[83] For a more comprehensive overview of biometrics, see Jain et al. (2004).

characteristics, such as fingerprint minutiae (key points). These details can either be stored as images (e.g., photos) or templates. With the exception of face prints, biometrics are most commonly stored as templates (often encrypted) rather than actual images (e.g., a picture of a fingerprint). This saves storage space and increases security; if someone were to hack your file, it would be very difficult to recreate your fingerprint.

2. **Identification (de-duplication).** Once the biometric has been recorded and stored, it can then be compared with other templates to ensure that it is unique. In this 1:N comparison, the computer checks the enrolled biometric template against each previously-enrolled template to see if there are any matches. This process is often used to de-duplicate records in order to reduce fraud—for example, ensuring that each civil servant is on the payroll only once. In certain cases, 1:N identification will be conducted in real time during enrollment; in others data is captured and stored to be de-duplicated at a later date. However, de-duplication is not always necessary or undertaken; many programs have captured biometric data not for its ability to ensure uniqueness, but rather for its authentication uses.
3. **Authentication (verification).** Like identification, verification involves comparing a stored biometric template against a stored template. In this case however, the comparison is used not to ensure that an individual's identity is unique, but rather to verify that an individual is who they claim to be—a 1:1 comparison. For example, an individual may authenticate her fingerprint against a template stored on a smartcard, or one stored in a computer profile that is called up by entering her name or ID number.

Both identification and authentication require comparisons between an enrolled biometric and one or more stored templates. Most large-scale, national identification systems, such as civil registries or voter rolls, rely on a centralized database for storage. Data can be routed from the point of capture (e.g., field offices) to the central database in order to de-duplicate. If the system is fully online, data could be compared instantaneously. If the system is offline, captured data must be uploaded to the central database in batches.

Similarly, online systems allow for authentication in real time with a fingerprint. Offline systems will likely require a smartcard. Smartcards include a computer chip that can store biometric templates, transactions, and other data. They can be used offline and then synched with a database periodically (e.g., a microcredit recipient uses her card at a local shop to receive payment, a record of payment is stored on the card and terminal, and synched later that evening). Technically, biometric-enabled smartcards can be used without a database, however this is uncommon.

However, data need not be stored in a centralized database or a smartcard; sometime, it is stored locally on a point-of-service (POS) terminal. One example is the UNHCR project that used biometrics to prevent Afghani refugees returning from Pakistan from claiming multiple re-settlement allowances. Upon crossing, each refugee was identified using iris scans to make

sure they had not passed through before; all biometric data was stored on the scanning unit and no other personal details were recorded.

Accuracy and Error Rates

Statistically speaking, biometrics are by far the most accurate method of identification. Still, the software and hardware used to capture and analyze biometric data is not infallible. Three types of errors can occur when individuals enroll their biometrics and during the process of matching an individual's biometric against a one stored on a card or in a database:

- **Fail to capture (failure to enroll):** the enrollment hardware (e.g., fingerprint scanner, camera) cannot capture an image of high enough quality.
- **False positive:** the system erroneously finds a match between the captured biometric and the stored template (e.g., you scan your fingerprint while opening a bank account and it says you have already registered—but you haven't!).
- **False negative:** the system erroneously finds *no* match between the captured biometric and the stored template (e.g., you scan your fingerprint at the ATM and it does not recognize you as having an account—but you do!).

Failure to capture biometric data can be the result of technical issues—such as low-quality scanners, dirt on the equipment, sweaty or dirty fingers, direct sunlight, poor lighting (for iris scans), etc.—or of injured or non-existent body parts, such as missing fingers and eyes, or damage from accidents or manual labor (see above table). It is also difficult to capture fingerprints of children and the often the elderly. In these cases, alternate processes (such as multimodal biometrics or waiving biometric requirements) must be in place to ensure inclusion.

False positive and false negative errors have different consequences depending on whether they occur in a 1:1 match or a 1:N match. In a de-duplication (1:N) process, for example, a false positive means that an individual is identified as already existing in the system when they do not, leading to a false rejection (you are not unique!). A false negative means that no match is found when it should be, and the individual is falsely accepted into the system as unique. The opposite is true for 1:1 matching (like verification). A false positive means that an individual's print is incorrectly identified as a match with the stored template, and they will be erroneously accepted or authenticated. If there is a false negative error, their authentication will be falsely rejected.

- **False acceptance rate (FAR):** the rate at which unauthorized individuals are allowed enrollment/access.
- **False rejection rate (FRR):** the rate at which authorized individuals are denied enrollment/access.

	False Negatives	False Positives
1:N	FAR	FRR
1:1	FRR	FAR

There is a tradeoff between FAR and FRR; algorithms that have a low tolerance for FARs will by definition have higher FRRs. Thus, each program must balance these needs: is it more important to ensure uniqueness (at the risk of falsely rejecting eligible individuals), or is it more important to be inclusive (at the risk of falsely accepting ineligibly individuals)? The answer will depend on the type of application. It is (hopefully) essential to exclude unauthorized individuals from accessing a nuclear facility, but important to ensure that the maximum number of individuals are included in a health program.

It is also important to recognize the limits to biometric technology and ongoing questions about its security. Particularly relevant to authentication applications, some biometrics may not be as stable as originally believed (Bowyer & Fenker, 2012). Spoofing—faking biometric measurements —is possible, though it increasingly requires more sophisticated technology. This can be made more difficult by alert operators, but collusion between subject and operator should not be ruled out, and in any event future applications are likely to emphasize remote authentication. The relative security of biometrics may also be compromised when combined with other technology, like offline card-based systems, which have shown as vulnerable to hacking and cloning. Some initiatives, such as India's UID program, have thus forsaken cards in favor of a strongly guarded centralized database but this too is not immune from errors, hacking and accidental exposure.

Industry Growth

The biometric industry has boomed over the last decade. Much of this growth has been in poorer countries:

Estimated growth rate of biometrics industry by region, USD millions

Region	Sales, 2005	Sales, 2010	% of Global Sales, 2005	% of Global Sales, 2010	Growth per Year
South America	137.0	515.8	9%	10%	30%
Middle East / India	160.0	715.9	10%	14%	35%
Africa	87.7	415.8	6%	8%	37%
Developing countries	*384.7*	*1647.5*	*25%*	*31%*	*34%*
Asia-Pacific Rim	372.4	1158.0	24%	22%	25%
Europe / Australia	257.0	821.1	17%	16%	26%
North America	524.8	1637.0	34%	31%	26%
Industrialized countries	*1154.2*	*3616.1*	*75%*	*69%*	*26%*
World	1538.9	5263.6	100%	100%	28%

Source: authors' calculations based on yearly revenue figures from the International Biometrics Group (IBG), http://www.wenturedigital.com/component/content/article/35-latest-headlines/46-fingerprint-biometric-market-growth.html

Appendix 2: Referenced Cases

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Afghanistan	"electronic Tazkera" (ID)	"Enhancing Legal & Electoral Capacity for Tomorrow (ELECT)"					
Albania	"Letërnjoftimi" (ID)						
Angola	"B.I." (ID)	voter registration	-				
Argentina	▪ RENAPER (civil registry & ID) ▪ "SIBIOS"						"Clave Única de Identificación Tributaria" (tax ID)
Armenia	national ID						
Bangladesh	"Preparation of Electoral Roll with Photographs (PERP)" and national ID						
Benin		"Liste Electorale Permanente Informatisee" (LEPI)			▪ "e-Health card" (insurance) ▪ "VaxTrac" (vaccinations)		
Bolivia	"Registro Unico de Identificacion" (ID)	biometric census				PRODEM FFP (smart card bank accounts)	
Botswana	"Omang" (ID)		"SmartSwitch" (banking, transfers)				

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Brazil	"Registro de Identidade Civil (RIC)" card (ID)	"Cadastro Biométrico" (voter ID, authentication)					
Burundi			demobilization payments	▪ military/police census ▪ civil servant registration			UNHCR proGres (refugee tracking)
Cape Verde		"Cadastro Eleitoral"					
Chad					"Pastoral Production System" (population tracking)		
China	national ID						
Chile	civil registry, ID				"Bono Electrónico (I-Med)" (copays)		
Colombia	National Registry of Civil Status, ID	"Plena Identidad" (voter authentication)					
Comoros		voter registration					
Costa Rica	"Gobierno Digital" (voter card, serves as main ID)						

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Cote d'Ivoire		voter registration					
Dominican Republic	"Cedula de Identidad y Electoral" (ID)						
Democratic Republic of Congo		voter ID	"PNDDR" (demobilization payments)				
Ecuador	DGRCIC "cédula de identidad" (civil registry, ID)						
El Salvador	RNPN "Documento Único de Identidad" (civil registry, ID)						drivers' license/vehicle registration
Ethiopia							UNHCR proGres (refugee tracking) NIN (taxes)
Fiji		"Electronic Voter Register" (voter ID)					
Gabon	national ID				"CNAMGS Carte d'Assurance Maladie" (insurance)		
Gambia	"GAMBIS" (ID)	"Biometric Voter Registration System"					

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Ghana	"National Identification System (NIS)", ghanacard (ID)	voter registration				▪ E-Zwich banking ▪ Opportunity International banking	
Guatemala	civil registry, national ID						
Guinea		voter registration					
Guinea-Bissau				biometric census of civil servants			
Guyana		voter registration					
Haiti	voter registration, issued ID cards						
Honduras	national ID						
India	▪ "UID/aadhaar" (ID) ▪ "National Population Census"		▪ MNREGA & NOAPS (Andhra Pradesh) ▪ PDS (Andhra Pradesh, Orissa, Karnataka)	▪ Teacher attendance (Maharashtra, Delhi) ▪ BMC employee attendance (Mumbai)	▪ RSBY insurance ▪ TB medication delivery (Delhi) ▪ sex worker clinic visits (Bangalore)	▪ biometric ATMs (Kerala) ▪ ICICI Bank/FINO smartcards	"National Coastal Security Program" (ID for fisherman)

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Indonesia	E-KTPs (ID)		"Cash Grants for Livelihood Recovery" (relief payments)			PT Bank Danamon	
Iraq				civil service reform			
Jamaica		voter registration					
Kenya		"Electronic Voter Registration"	"Hunger Safety Net Program"		▪ KEMRI/CDC HDSS ▪ "CliniPAK" (EHRs)		UNHCR proGres (refugee tracking)
Lesotho	national ID						
Liberia				Employee Biometric Identification & Records System (EBIRS)			
Malawi		voter registration	Dowa Emergency Cash Transfer (DECT)		FPIS (Fingerprint Identification System, treatment monitoring)	▪ MALSWITCH ▪ OIBM ▪ Credit market experiment	
Malaysia	MyKad (ID)						UNHCR proGres (refugee tracking)
Mauritania	"Biometric Census" (civil registry & ID)						

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Mexico	CEDI (ID) & "Registro de Menores de Edad"	voter registration	"Diconsa/ Oportunidades" payments		"Sistema Nominal en Salud" (SINOS)		drivers' license/vehicle registration
Morocco	national ID		J-PAL Education CCT				
Mozambique		voter registration				"Banco Oportunidade de Moçambique" (BOM)	
Namibia			▪ "Basic Income Grant" ▪ "Universal Pension Scheme"				
Nepal		voter registration				Sajilo Banking Sewa (banking, transfers)	
Nicaragua	national ID						
Nigeria	▪ NIN/GMPC (ID) ▪ MySmartCity Card (Cross River State)	voter registration	▪ National Pension ▪ "Project Comfort" (Cross River State)	IPPIS (payroll & pensions)	"Project HOPE" (Cross River State)		▪ standardized testing (exams) ▪ "National SIM Card Registration Project"

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Pakistan	NADRA, CNIC (civil registry, ID)		▪ BISP* ▪ Watan Card* ▪ IDP assistance* ▪ Repatriation grants (UNHCR) *draw from NADRA				▪ Refugee Proof of Registration, ID ▪ UNHCR proGres (refugee tracking)
Panama	cédula de identidad (ID, voter card)						
Paraguay	New Identification System (NIS)						
Peru	RENIEC (civil registry, ID)						
Philippines		voter registration	UMID (social transfers) 4Ps (payments)	Biometric Electronic Voting System (BEVS) for parliamentarians			
Rwanda	"e-Rwanda", "Indangamuntu" (joint distribution for ID and voter card)					Opportunity International Savings Card	
Senegal		voter registration					ID cards for refugees
Sierra Leone		voter registration					

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Somaliland		voter registration					
South Africa	HANIS (ID)		KZN Joint Municipal Provident Fund/ SASSA pensions & transfers		▪ AHDSS (EHRs) ▪ PCIS (EHRs) ▪ STAT (treatment monitoring)		
Sudan	national ID						
Tanzania	national ID						UNHCR proGres (refugee tracking)
Thailand	national ID						UNHCR proGres (refugee tracking)
Togo		voter registration					
Uganda	National Security Information System (NSIS) (ID)	"National Photo-Bearing Voters' Register (NVR)"			"Microcare Medical Acess Treatment Card (MTAC)"	MAP International banking/credit report	
Uruguay	national ID						
Venezuela		"Pon tu Huella" voter registration, authentication					
Vietnam					SonLa RCT (vaccine trial)		

Country	Foundational	Elections	Transfers	Civil Service	Health	Financial	Other
Yemen	civil registry modernization project, ID			"Biometric Information System (BIS)"	"Queen of Sheba Safe Motherhood Project" (health insurance)		
Zambia		voter registration					